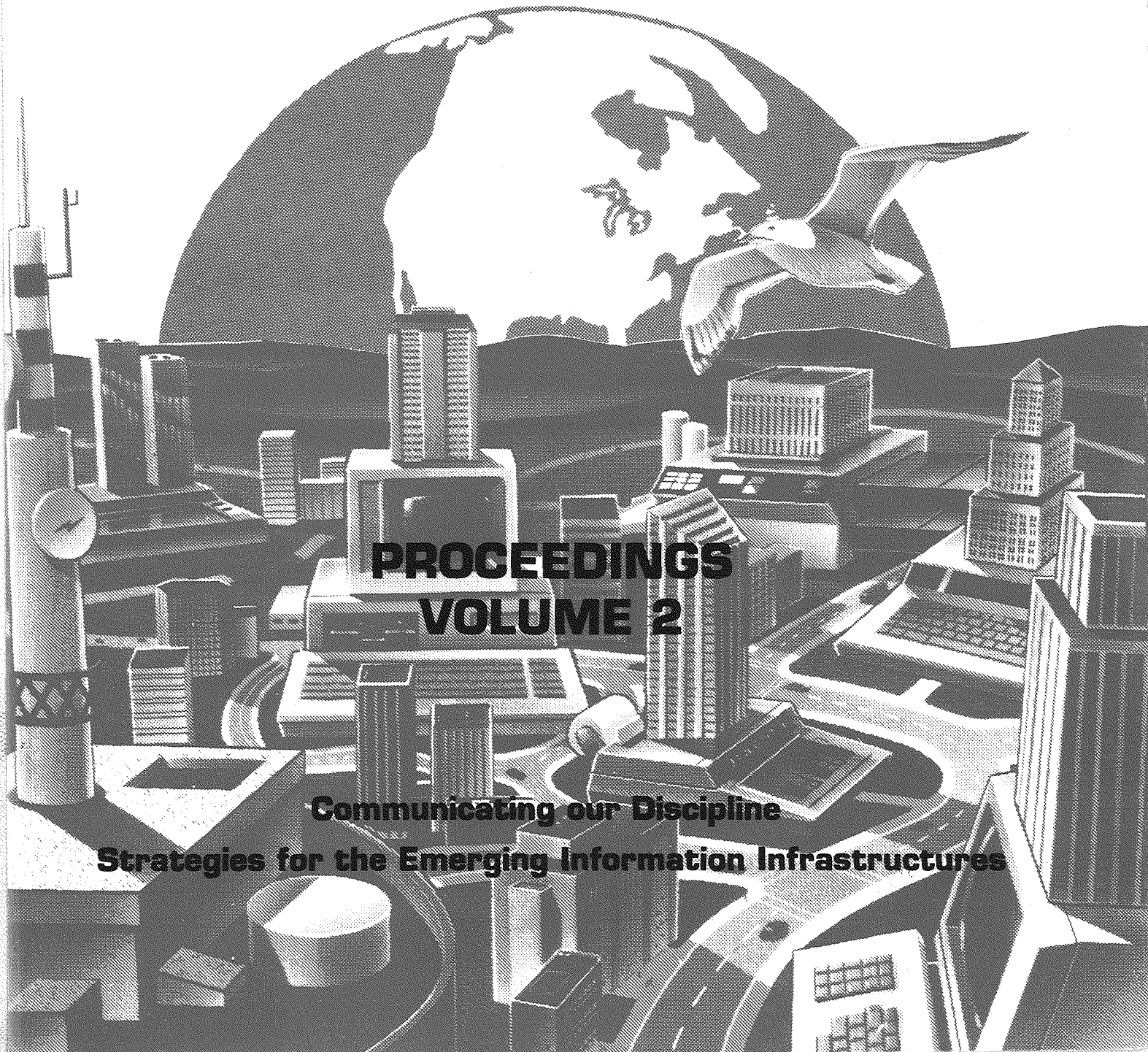


*NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY/  
NATIONAL COMPUTER SECURITY CENTER*

# **17th NATIONAL COMPUTER SECURITY CONFERENCE**

**October 11-14, 1994  
Baltimore Convention Center  
Baltimore, Maryland**



## **PROCEEDINGS VOLUME 2**

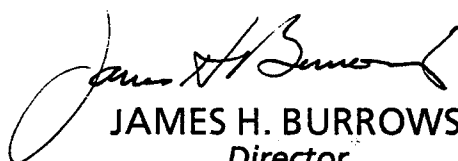
**Communicating our Discipline  
Strategies for the Emerging Information Infrastructures**

**Welcome!**

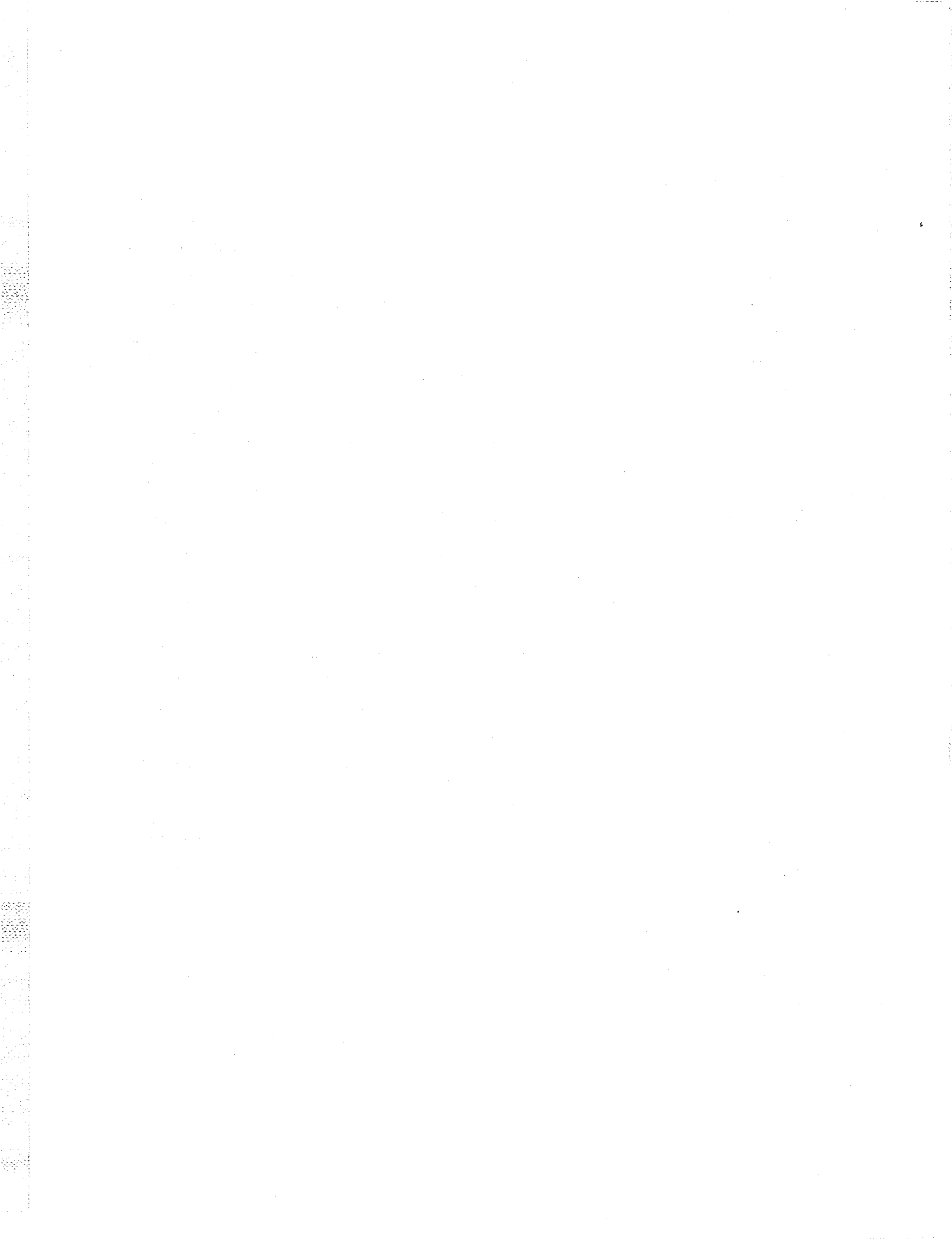
*The National Computer Security Center (NCSC) and the Computer Systems Laboratory (CSL) are pleased to welcome you to the Seventeenth Annual National Computer Security Conference. There is a new sense of urgency in the U.S. and abroad to achieve protection for the rapidly evolving information infrastructures. This year's program is designed to provide you information on the exciting new opportunities and the latest security technology. We believe the conference will stimulate a copious exchange of information and promote a solid understanding of today's information security issues and solutions.*

*The program tracks have been established to serve a wide range of interests from highly technical R&D projects to user oriented management and administration topics. Clearly, network security is a high priority topic. The opening and closing plenary sessions will highlight various dimensions of the security challenges in emerging information infrastructures. Papers and panel sessions will address a broad spectrum of network security subjects including: security architecture, internet security, firewalls, multilevel security (MLS) products, MLS system certification and accreditation, and security management. There will be a report on the progress and status of the Common Criteria and efforts for international harmonization. Risk management is a topic of increasing interest in today's difficult economic environment. As in the past, a number of tutorials will be given to introduce attendees to various information security topics and product areas.*

*We hope the networking conducted at the conference, the presentations and these proceedings will provide you with insights and ideas you can apply to your own information security endeavors. We encourage you to share the ideas and information acquired this week with your peers, your management, and your customers. Through this process we will enhance the security of our information systems and networks and build a strong foundation to meet tomorrow's challenges.*

  
**JAMES H. BURROWS**  
Director  
Computer Systems Laboratory

  
**PATRICK R. GALLAGHER, JR.**  
Director  
National Computer Security Center



# Conference

**Dr. Marshall Abrams**  
**Rowland Albert**  
**James P. Anderson**  
**Keith D. Anthony**  
**William Arbaugh**  
**James Arnold**  
**Alfred Arsenault**  
**Victoria Ashby**  
**David Balenson**  
**Jay W. Birch**  
**W. Earl Boebert**  
**Dr. Martha Branstad**  
**John S. Brofka**  
**Dr. Blaine Burnham**  
**Dr. John Campbell**  
**Lisa Carnahan**  
**Dr. Deborah Cooper**  
**Dr. Dorothy Denning**  
**Donna Dodson**  
**Ellen Flahavin**  
**Daniel W. Gambel**  
**William Geer**  
**Virgil Gibson**  
**Dennis Gilbert**  
**Irene Gilbert-Perry**  
**James K. Goldston**  
**Dr. Joshua Guttman**  
**Dr. Grace Hammonds**  
**Douglas Hardie**  
**Ronda Henning**  
**Dr. Harold Highland, FICS**  
**Jack Holleran**  
**Hilary H. Hosmer**  
**Howard Israel**

*The MITRE Corporation*  
*National Security Agency*  
*J.P. Anderson Company*  
*United States Air Force*  
*Department of Defense*  
*National Security Agency*  
*National Security Agency*  
*The MITRE Corporation*  
*Trusted Information Systems, Inc.*  
*I-NET, Inc.*  
*Secure Computing Technology Corporation*  
*Trusted Information Systems, Inc.*  
*HQ USTRANSCOM/J2S*  
*National Security Agency*  
*National Security Agency*  
*National Institute of Standards and Technology*  
*Unisys*  
*Georgetown University*  
*National Institute of Standards and Technology*  
*National Institute of Standards and Technology*  
*Grumman Data Systems*  
*Air Force Information Warfare Center*  
*Grumann Data Systems*  
*National Institute of Standards and Technology*  
*National Institute of Standards and Technology*  
*Integrated Computer Systems*  
*The MITRE Corporation*  
*AGCS, Inc.*  
*Unisys*  
*Harris Information Systems*  
*Computers & Security*  
*National Security Agency*  
*Data Security, Inc.*  
*AT&T Bell Laboratories*

# Referees

**Professor Sushil Jajodia**

**Dr. Steven Kent**

**Leslee LaFountain**

**Steven LaFountain**

**Paul A. Lambert**

**Dr. Carl Landwehr**

**Dr. Theodore M.P. Lee**

**Steven B. Lipner**

**Teresa Lunt**

**Frank Mayer**

**Dr. Catherine Meadows**

**William H. Murray**

**Dr. Peter Neumann**

**Steven Padilla**

**Marybeth Panock**

**Nick Pantiuk**

**Donn Parker**

**Dr. Gopal Ramanathan**

**Philip M. Roney**

**Dr. Ravi Sandhu**

**Marvin Schaefer**

**Daniel Schnackenberg**

**Steven Skolochenko**

**Bill Smith, CISSP**

**Dr. Stuart G. Stubblebine**

**Patricia Toth**

**Captain Charles Tracey, USAF**

**Dr. Chii-Ren Tsai**

**Kenneth R. VanWyk**

**John Wack**

**Grant Wagner**

**Major Glenn Watt, USAF**

**Howard Weiss**

**Roy Wood**

**Thomas E. Zmudzinski**

*George Mason University*

*Bolt, Barenok & Newmann*

*National Security Agency*

*National Security Agency*

*Motorola Incorporated*

*Naval Research Laboratory*

*Independent Consultant*

*Trusted Information Systems*

*SRI International*

*The AEROSPACE Corporation*

*Naval Research Laboratory*

*Deloitte & Touche*

*SRI International*

*SPARTA, Inc.*

*The MITRE Corporation*

*Grumman Data Systems*

*SRI International*

*The MITRE Corporation*

*Computer Sciences Corporation*

*George Mason University*

*ARCA Systems*

*Boeing Defense and Space Group*

*U.S. Department of Justice*

*Defense Information Systems Agency*

*USC Information Sciences Institute*

*National Institute of Standards and Technology*

*Joint Staff, Pentagon*

*Citicorp Global Information*

*Defense Information Systems Agency*

*National Institute of Standards and Technology*

*National Security Agency*

*U.S. STRATCOM*

*SPARTA, Inc.*

*National Security Agency*

*Defense Information Systems Agency*

# Awards Ceremony

6:00 p.m. Thursday, October 13  
Convention Center, Room 317

A joint awards ceremony will be held at which the National Institute of Standards and Technology (NIST) and the National Computer Security Center (NCSC) will honor the vendors who have successfully developed products meeting the standards of the respective organizations.

The NCSC recognizes vendors who contribute to the availability of trusted products and thus expand the range of solutions from which customers may select to secure their data. The products are placed on the Evaluated Products List (EPL) following a successful evaluation against the *Trusted Computer Systems Evaluation Criteria* including its interpretations: *Trusted Database Interpretation, Trusted Network Interpretation, and Trusted Subsystem Interpretation*. Vendors who have completed the evaluation process will receive a formal certificate of completion from the Director, NCSC marking the addition to the EPL. In addition, vendors will receive honorable mention for being in the final stages of an evaluation as evidenced by transition into the Formal Evaluation phase or for placing a new release of a trusted product on the EPL by participation in the Ratings Maintenance Program. The success of the Trusted Product Evaluation Program is made possible by the commitment of the vendor community.

The Computer Security Division at NIST provides validation services to test vendor implementations for conformance to security standards. NIST currently maintains validation services for three Federal Information Processing Standards (FIPS): FIPS 46-2, Data Encryption Standard (DES); FIPS 113, Computer Data Authentication; and FIPS 171, Key Management Using ANSI X9.17. During this award ceremony, NIST presents "Certificate of Appreciation" awards to those vendors who have successfully validated their implementation of these standards.

With the reaffirmation of the Data Encryption Standard as FIPS 46-2 in 1993, DES can now be implemented in software, as well as hardware and firmware. To successfully validate an implementation for conformance to FIPS 46-2, a vendor must run the Monte Carlo test as described in NBS (NIST) Special Publication 500-20. The Monte Carlo test consists of performing eight million encryptions and four million decryptions, with two encryptions and one decryption making a single test.

Vendors test their implementations for conformance to FIPS 113 and its American National Standards Institute (ANSI) counterpart, ANSI X9.9, Financial Institution Message Authentication (Wholesale). This is done using an electronic bulletin board system. Interactive validation requirements are specified in NBS (NIST) Special Publication 500-156, Message Authentication Code (MAC) Validation System: Requirements and Procedures. The test suite is composed of a series of challenges and responses in which the vendor is requested to either compute or verify a MAC on given data using a specified key which was randomly generated.

Conformance to FIPS 171 is also tested using an interactive electronic bulletin board testing suite. FIPS 171 adopts ANSI X9.17, Financial Institution Key Management (Wholesale). ANSI X9.17 is a key management standard for DES-based applications. The tests are defined in a document entitled NIST Key Management Validation System Point-to-Point (PTP) Requirements. The test suite consists of a sequence of scenarios in which protocol messages are exchanged under specified conditions.

**We congratulate all who have earned these awards.**

# 17th National Computer Security Conference

## *Table of Contents*

### *Refereed Papers*

#### RESEARCH AND DEVELOPMENT, TRACK A

Testing Intrusion Detection Systems: Design Methodologies and Results from an Early Prototype .....	1
Nicholas Puketza, Biswanath Mukherjee, Ronald A. Olsson, Kui Zhang, University of California, Davis	
A Pattern Matching Model for Misuse Intrusion Detection .....	11
Sandeep Kumar, Eugene H. Spafford, Purdue University	
Artificial Intelligence and Intrusion Detection: Current and Future Directions .....	22
Jeremy Frank, University of California, Davis	
A Three Tier Architecture for Role-Based Access Control .....	34
Ravi S. Sandhu, Hal Feinstein, SETA Corporation	
Using THETA to Implement Access Controls for Separation of Duties .....	47
Rita Pascale, Joseph R. McEnerney, Odyssey Research Associates	
Implementing Role Based, Clark-Wilson Enforcement Rules in a B1 On-Line Transaction Processing System .....	56
Barbara Smith-Thomas, AT&T Bell Laboratories; Wang Chao-Yeuh, Wu Yung-Sheng, Institute for Information Industry, Taiwan	
Virtual View Model to Design a Secure Object-Oriented Database .....	66
N. Boulahia-Cuppens, F. Cuppens, A. Gabillon, K. Yazdanian, ONERA/CERT, France	
Achieving Database Security Through Data Replication: The SINTRA Prototype .....	77
Myong H. Kang, Judith N. Froscher, John McDermott, Oliver Costich, Rodney Peyton, Naval Research Laboratory	
The Sea View Prototype: Project Summary .....	88
Teresa F Lunt, Peter K. Boucher, SRI International	
Towards a Formal Verification of a Secure and Distributed System and its Applications .....	103
Cui Zhang, Rob Shaw, Mark R. Heckman, Gregory D. Benson, Myla Archer, Karl Levitt, Ronald A. Olsson, University of California, Davis	
Making Secure Dependencies over a LAN Architecture for Security Needs .....	114
Bruno d'Ausbourg, CERT/ONERA, France	

## ***Refereed Papers (Cont'd)***

Automatic Generation of High Assurance Security Guard Filters .....	123
Vipin Swarup, The MITRE Corporation	
Belief in Correctness .....	132
Marshall D. Abrams, The MITRE Corporation; Marvin V. Zelkowitz, University of Maryland, College Park	
Towards a Privacy-Friendly Design and Use of IT-Security Mechanisms .....	142
Simone Fischer-Hübner, University of Hamburg	
Using a Semiformal Security Policy Model 2C a C2 Better .....	153
Marvin Schaefer, ARCA Systems, Inc.; Gary R. Grossman, Jeremy J. Epstein, Cordant, Inc.	
<b>ARCHITECTURE AND STANDARDS, TRACK B</b>	
A Taxonomy for Security Standards .....	165
Wayne A. Jansen, NIST	
The Graphical Display of a Domain Model of Information Systems Security (INFOSEC) Through Semantic Networks: A Description of the INFOSEC Semantic Network for Information Systems Security Engineers .....	175
Teresa T. Smith, Kathleen V. Dolan, National Security Agency	
A New Attack on Random Pronounceable Password Generators .....	184
Ravi Ganesan, Chris Davies, Bell Atlantic	
Development History for Procurement Guidance Using the Trusted Computer System Evaluation Criteria .....	198
Major Melvin L. DeVilbiss, USA, National Security Agency	
Exporting Evaluation: an analysis of US and Canadian criteria for trust .....	206
Paul A. Olson	
What Color is Your Assurance? .....	215
David R. Wichers, Joel E. Sachs, Douglas J. Landoll, ARCA Systems, Inc.	
BFE Applicability to LAN Environments .....	227
Tom Benkart, ACC Network Systems; Dave Bitzer, National Security Agency	
The Architecture of Triad: A Distributed, Real-Time, Trusted System .....	237
E John Sebes, Nancy Kelem, Terry C. Vickers Benzel, Mary Bernstein, Eve Cohen, Jeff Jones, Jon King, Trusted Information Systems, Inc.; Michael Barnett, David M. Gallon, Roman Zacjew, Locus Computing Corporation	
Constructing a High Assurance Mail Guard .....	247
Richard E. Smith, Secure Computing Corporation	



## ***Refereed Papers (Cont'd)***

### **APPLICATIONS AND INTEGRATION, TRACK C**

Controlled Execution UNIX .....	254
Lee Badger, Homayoon Tajalli, David Dalva, Daniel Sterne, Trusted Information Systems, Inc.	
Architectures for C2 DOS/Windows-Based Personal Computers, Securing an "Unsecurable" Operating System .....	264
Jeremy Epstein, Gary Grossman, Frederick Maxwell, Noble Veirs III, Albert Donaldson, Cornelius Haley, Cordant, Inc.	
A Practical Hardware Device for System and Data Integrity as well as Malicious Code Protection .....	274
T.E. Elliott, Department of National Defence, Canada	
Partitioning the Security Analysis of Complex Systems .....	283
Howard Holm, National Security Agency	
The Composition Problem: An Analysis .....	292
Guy King, Computer Sciences Corporation	
Making Do With What You've Got .....	299
Janis W. Berryman, The Boeing Company; Bruce F. Kennedy, Cubic Applications, Inc.	
Modern Multilevel Security (MLS): Practical Approaches for Integration, Certification, and Accreditation .....	309
Bill Neugent, Mike Burgoon, Jeanne Firey, Mindy Rudell, The MITRE Corporation	
Applying COMPUSEC to the Battlefield .....	318
Diane M. Bishop, Stephen R. Arkley, Computer Sciences Corporation	
Security Requirements for Customer Network Management in Telecommunications .....	327
Vijay Varadharajan, Hewlett-Packard Labs, UK	
Support for Security in Distributed Systems Using MESSIAHS .....	339
Steve J. Chapin, Kent State University Eugene H. Spafford, Purdue University	
A Technical Approach for Determining the Importance of Information in Computerized Alarm Systems .....	348
David S. Fortney, Lawrence Livermore National Laboratory, Judy J. Lim, Lim and Orzechowski Associates	

## ***Refereed Papers (Cont'd)***

- ASAM: A Security Certification and Accreditation Support Tool for DoD  
Automated Information Systems ..... 358  
Loreto Remorca, Jr., William Barr, Secure Solutions, Inc.;  
Robert Zomback, U.S. Army CECOM, Space and Terrestrial Communications  
Directorate; V. Michael Caputo, MICON Services Company
- A Financial Management Approach for Selecting Optimal, Cost-Effective  
Safeguards Upgrades for Computer- and Information-Security Risk  
Management ..... 370  
Suzanne T. Smith, Barranca Inc.; Stephen Gale, William J. Malampy,  
University of Pennsylvania
- MANAGEMENT AND ADMINISTRATION, TRACK D
- The Electronic Intrusion Threat to National Security & Emergency  
Preparedness Telecommunications: An Awareness Document ..... 378  
Dr. Joseph Frizzel, National Communications System;  
Ted Phillips, Traigh Groover, Booz Allen & Hamilton, Inc.
- Using Application Profiles to Detect Computer Misuse ..... 400  
Nancy L Kelem, Daniel F. Sterne, David I. Dalva, Kenneth M. Walker, Trusted  
Information Systems, Inc., Debra Anderson, Harold Javitz, Alfonso Valdes, SRI  
International, Linda L. Lanekwicz, Glenn Bell, Spring Hill College
- Can Computer Crime be Deterred? ..... 412  
Sanford Sherizen, Ph.D., Data Security Systems, Inc.
- Demonstrating the Elements of Information Security with Threats ..... 421  
Donn B. Parker, SRI International
- The Aerospace Risk Evaluation System (ARiES): Implementation of a  
Quantitative Risk Analysis Methodology for Critical Systems ..... 431  
Charles H. Lavine, Anne M. Lindell, Sergio B. Guarro,  
The Aerospace Corporation
- The Security-Specific Eight Stage Risk Assessment Methodology ..... 441  
David L. Drake, Katherine L. Morse, Science Applications International  
Corporation
- Security Awareness and the Persuasion of Managers ..... 451  
Dennis F. Poindexter, Center for Information Systems Security
- The Network Memorandum of Agreement (MOA) Process: Lessons Learned .. 459  
William C. Barker, Lisa M. Jaworski, Geroge R. Mundy, Trusted  
Information Systems, Inc.
- Independent Validation and Verification of Automated Information  
Systems in the Department of Energy ..... 468  
William J. Hunteman, Los Alamos National Laboratory;  
Robert Caldwell, Department of Energy

## *Panel Summaries*

### RESEARCH AND DEVELOPMENT, TRACK A

Fuzzy Security: Formalizing Security as Risk Management .....	478
Security is Risk Management .....	480
Ruth Nelson, Chair, Information System Security	
Fuzzy Policies .....	482
Hilary H. Hosmer, Data Security, Inc.	
Assurance, Risk Assessment, and Fuzzy Logic .....	483
John McLean, Naval Research Laboratory	
Using Fuzzy Logic in Formal Security Models .....	486
Sergei Ovchinnikov, San Francisco State University	
Role Based Access Control, Its Structure, Mechanisms and Environment .....	488
Hal Feinstein, Chair, SETA Corporation	
Role-Based Access Control Position Paper .....	491
Marshall D. Abrams, The MITRE Corporation	
Role-Based Access Control, A Position Statement .....	492
Ravi S. Sandhu, George Mason University	
Role-Based Access Control, Position Statement .....	493
David Ferraiolo, NIST	
Inference Problem in Secure Database Systems .....	494
Bhavani Thuraisingham, Chair, The MITRE Corporation	
An Inference Paradigm <sup>1</sup> .....	497
Donald G. Marks, Department of Defense	
The Inference Problem: A Practical Solution .....	507
Teresa F. Lunt, SRI International	
Security-Oriented Database Inference Detection .....	510
Thomas H. Hinke, Harry S. Delugach, University of Alabama	
Key Escrowing: Today and Tomorrow .....	514
Miles E. Smid, Chair, NIST	
The Target System .....	514
Jan Manning, National Security Agency	
Procedures for Lawful Interception of Telecommunications .....	514
Mike Glimore, Federal Bureau of Investigation	
Future Considerations for Key Escrowing .....	514
Dr. Dorothy Denning, Georgetown University	
The Security Association Management Protocol Panel .....	515
Major Terry Hewitt, USAF, Chair, National Security Agency	
Position Paper .....	517
James Leppek, Harris Corporation	
Position Paper .....	518
Dave Wheeler, Motorola	

1. *Refereed paper*

## *Panel Summaries*

Highlights of the New Security Paradigms '94 Workshop .....	519
Eric Leighninger, chair	
Formal Semantics of Confidentiality in Multilevel Logic Databases .....	520
Adrian Spalka, University of Bonn, Germany	
Healthcare Information Architecture: Elements of a New Paradigm .....	532
Daniel J. Essin, University of Southern California; Thomas L. Lincoln, The RAND Corporation	
Communication, Information Security and Value .....	554
John Dobson, University of Newcastle, UK	
Fuzzy Patterns in Data--Anomaly Detection .....	566
T. Y. Lin, San Jose State University	

### ARCHITECTURE AND STANDARDS, TRACK B

The Development of Generally Accepted System Security Principles (GSSP), NIST's Approach .....	581
Marianne Swanson, Chair, NIST	
Viewpoint .....	581
Will Ozier, ISSA GSSP Committee Chair	
Viewpoint .....	581
Marianne Swanson, NIST	
Viewpoint .....	581
Ed Roback, NIST	
Viewpoint .....	581
Barbara Guttman, NIST	
Product and System Certification in Europe .....	582
Klaus J. Keus, Chair, BSI, Germany	
Status of European Certification Schemes and Mutual Recognition .....	582
Angelika C. Jennen, BSI, Germany	
Certification Maintenance under ITSEC .....	583
Jeremy Wilde, Logica, UK	
Security Evaluations in the Netherlands--An evaluators view on globalization of evaluations .....	583
Dr. Paul L. Overbeek, TNO Physics and Electronics Laboratory, The Netherlands	
Effectiveness in French Evaluations .....	583
Laurent Borowski, CR2A, France	
The relation between Correctness and Effectiveness in System Composition .....	584
Mats Ohlin, Electronic Systems Directorate, Sweden	
Evaluation of Platform Independence .....	584
Peter Cambell-Burns, Admiral Management Services Limited, UK	
Vendor Assurance vs. 3rd Party Evaluation: A Constructive Approach ..	585
Dr. Heinrich Kersten, BSI, Germany	

## *Panel Summaries (Cont'd)*

New Concepts in Assurance Panel .....	586
Pat Toth, Chair, NIST	
Viewpoint .....	586
Lynne Ambuel, National Security Agency	
Viewpoint .....	586
Deitra Kimpton, CSE, Canada	
Viewpoint .....	586
Ken Rochon, National Security Agency	
Viewpoint .....	586
Karen Ferraiolo, ARCA Systems	
New Challenges for C&A: The Price of Interconnectivity and Interoperability .....	587
Ellen Flahavin, Co-chair, NIST	
Joel Sachs, Co-chair, ARCA	
The Department of Defense Goal Security Architecture (DGSA) .....	588
W. Timothy Polk, Chair, NIST	
The Department of Defense Goal Security Architecture .....	588
Richard McAllister, National Security Agency	
The DGSA Overall Transition Strategy .....	588
Carl Deutsch, National Security Agency	
Security Standards for DGSA-based Architectures .....	588
Janice Schafer, Defense Information Systems Agency	
DGSA's Applicability to non-DoD Environments .....	588
Jim Coyle, Booz-Allen & Hamilton	
Multilevel Security--Current Applications and Future Directions .....	589
Colonel J. Sheldon, USA, Chair, DISA/CISS	
Viewpoint .....	589
John Wiand, USSOCOM	
Viewpoint .....	589
Russ Myers, USACOM	
Viewpoint .....	589
Emily Klutz, USACOM	
Viewpoint .....	589
Lieutenant Colonel Tom Surface, USPACOM	
Viewpoint .....	589
Major Kevin Newland, USSPACECOM	
Viewpoint .....	590
Mr. Paul Woodie, National Security Agency	
Viewpoint .....	590
Mr. Charles West, DISA	

## *Panel Summaries (Cont'd)*

Prominent Industry-Sponsored Security Architectures Currently Under Development .....	592
Michael McChesney, Chair, Secure Ware, EGSA	
Viewpoint .....	596
Roger Schell, Novell	
Viewpoint .....	598
Bill Dwyer, Hewlett-Packard	
 APPLICATIONS AND INTEGRATION, TRACK C	
Can Your Net Work Securely? .....	599
Peter G. Neumann, Chair, SRI International	
How to Trust a Distributed System .....	600
B. Clifford Neuman, USC, Information Sciences Institute	
Internet Firewalls .....	602
John Wack, Chair, NIST	
Proven Detection Tools for Intrusion Prevention .....	603
Michael Higgins, chair, Defense Information Systems Agency	
MLS System Solutions - A Continuing Debate Among The Critical Players ....	604
Joel E. Sachs, ARCA Systems, Inc.	
Trusted Systems Interoperability Group	
Stan Wisseman, Chair, ARCA Systems, Inc. ....	607
Historical Perspective .....	610
Paul Cummings, Digital Equipment Corporation	
Common Internet Protocol Security Option .....	613
Ron Sharp, AT&T Bell Laboratories	
Trusted Security Information Exchange for Restricted Environments ....	614
Charlie Watt, SecureWare	
Trusted Administration Working Group .....	616
Jeff Edelheit, The MITRE Corporation	
Trusted Applications Working Group .....	618
Stan Wisseman, ARCA Systems, Inc.	
Government Perspective .....	619
George Mitchell, NCSC	

## *Panel Summaries (Cont'd)*

NSA Concurrent Systems Security Engineering Support to the MLS TECHNET Program .....	620
Bradley Hildreth, Chair, National Security Agency	
Viewpoint .....	624
Mary Mayonado, Eagan, McAllister Associates, Inc	
Viewpoint .....	626
Teresa Acevedo, Pulse Engineering, Inc.	
Viewpoint .....	628
Jenny Himes, National Security Agency	
Viewpoint .....	629
Gregory Wessel, National Security Agency	
Viewpoint .....	630
Randy Blair, National Security Agency	
Viewpoint .....	631
Richard White, Air Force Information Warfare Center	
Viewpoint .....	633
George Hurlburt, Naval Air Warfare Center	
Provisions to Improve Security on the Internet .....	635
Dr. Harold Highland, Chair, Computers & Security	
Viewpoint .....	636
Dr. Harold Highland, Computers & Security	
Viewpoint .....	639
Frederick Avolio, Trusted Information Systems, Inc.	
Viewpoint .....	641
Dr. Stephen Bellovin, AT&T Bell Laboratories	
Viewpoint .....	643
Matt Bishop, University of California, Davis	
Viewpoint .....	645
William R. Cheswick, AT&T Bell Laboratories	
Viewpoint .....	647
Dr. Jon David, The Fortress	
Viewpoint .....	650
Colonel Frederick A. Kolbrener, U.S. Army	
Viewpoint .....	652
A. Padgett Peterson, Martin-Marietta Information Group	

## ***Panel Summaries (Cont'd)***

### **MANAGEMENT AND ADMINISTRATION, TRACK D**

Model Information Security Programs .....	654
Richard W. Owen, Jr., Chair, Office of the Attorney General, Texas	
Viewpoint Academia .....	654
Stephen J. Green, University of Houston	
Viewpoint Commercial .....	655
Genevieve M. Burns, Monsanto Company	
Viewpoint Federal .....	655
Philip L. Sibert, U.S. Department of Energy	
Viewpoint State .....	656
Jan W. Wright, Information Resources Commission, Florida	
Interdisciplinary Perspectives on InfoSec: Bringing the Humanities into Cyberspace .....	657
Michel E. Kabay, Chair, National Computer Security Association and JINBU Corporation, Canada	
An Anthropological View: Totem and Taboo in Cyberspace <sup>2</sup> .....	658
Michel E. Kabay, National Computer Security Association and JINBU Corporation, Canada	
Philosophy of Law and InfoSec: Justifying Morality in Cyberspace .....	669
Virginia Black, Pace University	
Psychology and InfoSec: Improving Compliance with InfoSec Policies ...	675
Percy Black, Pace University	
Military Science and Information Security .....	681
James P. Craft, Systems Research and Applications Corporation	
Ethical Issues in the National Information Infrastructure .....	685
Jim Williams, Chair, The MITRE Corporation	
Medical Information Privacy, Current Legislative and Standards Activities ...	688
Marc Schwartz, Support Medical Systems, Inc., Chair	
Viewpoint .....	690
Robert Gellman, United States House of Representatives	
Viewpoint .....	692
Molla Donaldson, National Academy of Sciences	
Viewpoint .....	694
Dale Miller, Irongate, Inc.	
Viewpoint .....	695
C. Peter Waegemann, Medical Records Institute	
Viewpoint .....	696
Gerald S. Lang, The Harrison Avenue Corporation	
Privacy and the Handling of Patient Related Information in the Public Swedish Health Care System <sup>3</sup> .....	699
Torleif Olhede, Stockholm University, Sweden	

2. *Refereed paper*

3. *Refereed paper*



## *Panel Summaries (Cont'd)*

Computer Crime on the Internet .....	713
Christine Axsmith, Esq., Chair, ManTech Strategies Associates	
Viewpoint .....	714
Donn Parker, SRI International	
Viewpoint .....	714
Mark Pollitt, Federal Bureau of Investigation	
Viewpoint .....	714
Ted Chambers, Scientific Computer Support Team	
Viewpoint .....	715
Barbara Fraser, Carnegie Mellon	
Viewpoint .....	715
Martin Schoffstall, Performance Systems International	
Viewpoint .....	716
Mark Fedor, Performance Systems International	
Do You Have the Skills to be a Future INFOSEC Profession .....	717
Dr. William (Vic) Maconachy, Chair, Center for Information Systems Security	
Computers at Risk Recommendations: Are They Still Valid? .....	723
Hal Tipton, Chair, HFT Associates	
Viewpoint .....	724
Will Ozier, Ozier Peterse & Associates	
Viewpoint .....	724
Earl Boebert, Secure Computing Corporation	
Viewpoint .....	725
Steve Walker, Trusted Information Systems	
Objectives and Progress of the GSSP Committee .....	727

### TUTORIALS & PRESENTATIONS, TRACK E

Tutorial Series on Trusted Systems and Operational Security .....	731
R. Kenneth Bauer, Joel Sachs, Dr. Eugene Schultz, Dr. Gary Smith, Jeff Williams, ARCA Systems, Inc.; Chris Bressinger, DoD Security Institute; Dr. Charles Abzug, LtCdr Alan Liddle, National Defense University	
Security Information for the Asking: The Untapped Information Potential Awaiting the Security Practitioner .....	733
Viewpoint .....	733
Kathie Everhart, NIST	
Viewpoint .....	733
Marianne Swanson, NIST	
Viewpoint .....	734
Bob Lau, National Security Agency	
Viewpoint .....	734
Nickilyn Lynch, NIST	

## ***Panel Summaries (Cont'd)***

### **SPECIAL SESSIONS AND DEMONSTRATIONS**

International Harmonization: The Common Criteria--Progress and Status . . . .	735
Eugene Troy, Chair, NIST	
Security Requirements for Distributed Systems . . . . .	738
Robert Dobry, Chair, National Security Agency	
The Application of Electronic Groupware Tools to Address IT Security Challenges . . . . .	739
Dennis Gilbert, Demonstration Coordinator, NIST	
The Learning Track . . . . .	740
Training Challenges of the 90's . . . . .	740
Joan Pohly, FISSEA Chair	
Proposed New NIST Training Standards . . . . .	741
Dorothea deZafra, Public Health Service	
Computer Security Resources that Work . . . . .	741
Barbara Cuffie, Social Security Administration	
Effective Marketing of the Computer Security Program to Management .	741
Joan Hash, Social Security Administration	
Tools and Methodologies for Delivering Training . . . . .	741
Janet Jelen, Public Health Service	
Demonstrations on Computer Security Training Tools . . . . .	741
Anthony Stramella, National Cryptologic School	
Training Events on a Shoestring Budget . . . . .	741
Sadie Pitcher, Department of Commerce	
Adult Learning and Information Systems Security Training . . . . .	742
Dr. Eugene V. Martin, Organization and Education Consultant	
Information Systems Professionalism--Professional Development and Certification . . . . .	742
Richard Koenig, Harold Tipton, International Information Systems Security Certification Consortium	
Computer Ethics for Future Generations . . . . .	742
Richard Koenig, International Information Systems Security Certification Consortium	

## Authors and Panelists Cross Index

Abrams, Marshall D. ....	132, 491	Coyle, Jim .....	588
Abzug, Dr. Charles .....	731	Craft, James P. ....	681
Acevedo, Teresa .....	626	Cuffie, Barbara .....	741
Ambuel, Lynne .....	586	Cummings, Paul .....	610
Anderson, Debra .....	400	Cuppens, F. ....	66
Archer, Myla .....	103	Dalva, David I. ....	254, 400
Arkley, Stephen R. ....	318	d'Ausbourg, Bruno .....	114
Axsmith, Christine, Esq. ....	713	David, Jon .....	647
Avolio, Frederick .....	639	Davies, Chris .....	184
Badger, Lee .....	254	Delugach, Harry S. ....	510
Barker, William C. ....	459	Denning, Dr. Dorothy .....	514
Barnett, Michael .....	237	Deutsch, Carl .....	588
Barr, William .....	358	DeVilbiss, M. L., Major USA ..	198
Bauer, R. Kenneth .....	731	deZafra, Dorothea .....	741
Bell, Glenn .....	400	Dobry, Robert .....	738
Bellovin, Stephen .....	641	Dobson, John .....	554
Benkart, Tom .....	227	Dolan, Kathleen V. ....	175
Benson, Gregory D. ....	103	Donaldson, Albert .....	264
Vickers Benzel, Terry C. ....	237	Donaldson, Molla .....	692
Bernstein, Mary .....	237	Drake, David L. ....	441
Berryman, Janis W. ....	299	Dwyer, Bill .....	598
Bishop, Diane M. ....	318	Edelheit, Jeff .....	616
Bishop, Matt .....	643	Elliott, T. E. ....	274
Bitzer, Dave .....	227	Epstein, Jeremy .....	153, 264
Black, Percy .....	675	Essin, Daniel J. ....	532
Black, Virginia .....	669	Everhart, Kathie .....	733
Blair, Randy .....	630	Fedor, Mark .....	716
Boebert, Earl .....	725	Feinstein, Hal .....	34, 488
Borowski, Laurent .....	583	Ferraiolo, David .....	493
Boucher, Peter K. ....	88	Ferraiolo, Karen .....	586
Burns, Genevieve M. ....	655	Firey, Jeanne .....	309
Boulahia-Cuppens, N. ....	66	Fischer-Hübner, Simone .....	142
Bressinger, Chris .....	731	Flahavin, Ellen .....	587
Burgoon, Mike .....	309	Fortney, David S. ....	348
Caldwell, Robert .....	468	Frank, Jeremy .....	22
Cambell-Burns, Peter .....	584	Fraser, Barbara .....	715
Caputo, V. Michael .....	358	Frizzel, Dr. Joseph .....	378
Chambers, Ted .....	715	Froscher, Judith N. ....	77
Chao-Yeuh, Wang .....	56	Gabillon, A. ....	66
Chapin, Steve J. ....	339	Gale, Stephen .....	370
Cheswick, William R. ....	645	Gallon, David M. ....	237
Cohen, Eve .....	237	Ganesan, Ravi .....	184
Costich, Oliver .....	77	Gellman, Robert .....	690

## Authors and Panelists Cross Index

Gilbert, Dennis	739	Lavine, Charles H.	431
Glimore, Mike	514	Leighninger, Eric	519
Green, Stephen J.	654	Leppek, James	517
Groover, Traigh	378	Levitt, Karl	103
Grossman, Gary	153, 264	Liddle, Alan, LtCdr	731
Guarro, Sergio B.	431	Lim, Judy J.	348
Guttman, Barbara	581	Lin, T. Y.	566
Haley, Cornelius	264	Lincoln, Thomas L.	532
Hash, Joan	741	Lindell, Anne M.	431
Heckman, Mark R.	103	Lunt, Teresa F.	88, 507
Hewitt, Terry, Major USAF	515	Lynch, Nickilyn	734
Higgins, Michael	603	Maconachy, Dr. William (Vic)	717
Highland, Harold, FICS	635, 636	Malampy, William J.	370
Hildreth, Bradley	620	Manning, Jan	514
Himes, Jenny	628	Marks, Donald G.	497
Hinke, Thomas H.	510	Martin, Dr. Eugene V.	742
Holm, Howard	283	Mayonado, Mary	624
Hosmer, Hilary H.	482	Maxwell, Frederick	264
Hunteman, William J.	468	McAllister, Richard	588
Hurlburt, George	633	McChesney, Michael	592
Jansen, Wayne A.	165	McDermott, John	77
Javitz, Harold	400	McEnerney, Joseph R.	47
Jaworski, Lisa M.	459	McLean, John	483
Jelen, Janet	741	Miller, Dale	694
Jennen, Angelika C.	582	Mitchell, George	619
Jones, Jeff	237	Morse, Katherine L.	441
Kabay, Michel E	657, 658	Mukherjee, Biswanath	1
Kang, Myong H.	77	Mundy, Geroge R.	459
Kelem, Nancy	237, 400	Myers, Russ	589
Kennedy, Bruce F.	299	Nelson, Ruth	478, 480
Kersten, Dr. Heinrich	585	Neugent, Bill	309
Keus, Klaus J.	582	Neuman, B. Clifford	600
Kimpton, Deitra	586	Neumann, Peter G.	599
King, Guy	292	Newland, Major Kevin	589
King, Jon	237	Ohlin, Mats	584
Klutz, Emily	589	Olhede, Torleif	699
Koenig, Richard	742	Olson, Paul A.	206
Kolbrener, F. A., COL USA	650	Olsson, Ronald A.	1, 103
Kumar, Sandeep	11	Ovchinnikov, Sergei	486
Landoll, Douglas J.	215	Overbeek, Dr. Paul L.	583
Lang, Gerald S.	696	Owen, Jr., Richard W.	654
Lankewicz, Linda L.	400	Ozier, Will	581, 724
Lau, Bob	734	Parker, Donn	421, 714

## Authors and Panelists Cross Index

Pascale, Rita .....	47	Thuraisingham, Bhavani .....	494
Peterson, A. Padgett .....	652	Toth, Pat .....	586
Peyton, Rodney .....	77	Troy, Eugene .....	735
Phillips, Ted .....	378	Valdes, Alfonso .....	400
Pitcher, Sadie .....	741	Varadharajan, Vijay .....	327
Pohly, Joan .....	740	Veirs III, Noble .....	264
Poindexter, Dennis F. ....	451	Wack, John .....	602
Polk, W. Timothy .....	588	Waegemann, C. Peter .....	695
Pollitt, Mark .....	714	Walker, Kenneth M. ....	400
Puketza, Nicholas .....	1	Walker, Steve .....	727
Remorca, Jr., Loreto .....	358	Watt, Charlie .....	614
Roback, Ed .....	581	Wessel, Gregory .....	629
Rochon, Ken .....	586	West, Charles .....	590
Rudell, Mindy .....	309	Wheeler, Dave .....	518
Sachs, Joel E. ...	215, 587, 604, 731	White, Richard .....	631
Sandhu, Ravi S. ....	34, 492	Wiand, John .....	589
Schaefer, Marvin .....	153	Wichers, David R. ....	215
Schafer, Janice .....	588	Wilde, Jeremy .....	583
Schell, Roger .....	596	Williams, Jeff .....	731
Schoffstall, Martin .....	716	Williams, Jim .....	685
Schultz, Dr. Eugene .....	731	Wisseman, Stan .....	607, 618
Schwartz, Marc .....	688	Woodie, Paul .....	590
Sebes, E. John .....	237	Wright, Jan W. ....	656
Sharp, Ron .....	613	Yazdanian, K. ....	66
Shaw, Rob .....	103	Yung-Sheng, Wu .....	56
Sheldon, J., COL USA,, .....	589	Zacjew, Roman .....	237
Sherizen, Sanford Ph.D., .....	412	Zelkowitz, Marvin V. ....	132
Sibert, Philip L. ....	655	Zhang, Cui .....	103
Smid, Miles E. ....	514	Zhang, Kui .....	1
Smith, Dr. Gary .....	731	Zomback, Robert .....	358
Smith, Richard E. ....	247		
Smith, Suzanne T. ....	370		
Smith, Teresa T. ....	175		
Smith-Thomas, Barbara .....	56		
Spalka, Adrian .....	520		
Spafford, Eugene H. ....	11, 339		
Sterne, Daniel .....	254, 400		
Stramella, Anthony .....	741		
Surface, Tom, LTCOL, USA ...	589		
Swanson, Marianne .....	581, 734		
Swarup, Vipin .....	123		
Tajalli, Homayoon .....	254		
Tipton, Harold .....	723, 742		

# USING APPLICATION PROFILES TO DETECT COMPUTER MISUSE

Nancy L. Kelem

Daniel F. Sterne  
David I. Dalva  
Kenneth M. Walker

Debra Anderson  
Harold Javitz  
Alfonso Valdes

Linda L. Lankewicz  
Glenn Bell

Trusted Information Systems Inc.  
444 Castro Street, Suite 800  
Mountain View, CA 94041  
415/962-8885

Trusted Information Systems Inc.  
3060 Washington Road  
Glenwood, MD 01368  
301/854-6889

SRI International  
333 Ravenswood Ave.  
Menlo Park, CA 94025  
415/326-6200

Spring Hill College  
4000 Dauphin St.  
Mobile, AL 36608  
205/380-3473

## Abstract

This paper presents the results of a study that investigated the feasibility of determining whether a system is being used for its approved purposes by monitoring resource usage statistics captured in an audit log. The focus differed from traditional intrusion detection, which is concerned with the behavior associated with users. Instead, intrusion detection techniques were adapted to focus on characterizing the expected behavior of application programs. To test the utility of the profiles, audit records representing "masquerades" were compared with application profiles to see whether the masquerades could be detected.

*Keywords:* intrusion detection, resource usage, audit, computer misuse, program behavior, pattern recognition, export control. <sup>1</sup>

## 1 Introduction

### 1.1 Background — The Export Safeguards Demonstration Project

In recent years, the U.S. Government has been faced with the problem of controlling sales of high technology computer systems and applications to other countries without unnecessarily restricting sales for legitimate use. Potential overseas customers seek purchase of the most technologically advanced systems and in some cases can readily obtain these from other countries if not offered by U.S. firms.

The Export Safeguards Demonstration, funded by ARPA and carried out by Trusted Information Systems (TIS), has investigated and prototyped engineering technologies having potential to permit greater U.S. exports of high performance systems while discouraging their diversion for unauthorized use. These technologies may provide additional flexibility and export control options for the U.S. Government. In addition, they appear to be applicable to commercially available systems without major hardware or software modifications. This paper describes experimentation with one of these technologies, in which state-of-the-art intruder detection technology has been adapted to automate the analysis of audit records collected from Safeguards-protected systems; this analysis has been directed at determining whether misuse of an exported system can be detected via examination of the resource usage statistics associated with application programs.

### 1.2 Purpose

This paper describes experiments in which intruder detection technology was adapted for detecting misuse of computer systems, particularly systems subject to stringent export controls. In order to be approved, export licenses for high performance computer systems typically stipulate that the exported system must only be used for a specific purpose. For example, supercomputers might be approved for export for weather modeling or oil or gas exploration. Less powerful systems might be approved for inventory control or other commercial uses. Any use other than that for which an exported system has been approved would constitute misuse. It is not the purpose of this paper to describe the various difficulties that would be inherent in operational fielding of misuse detection systems. Instead, the focus is on whether the necessary misuse analysis is even feasible.

<sup>1</sup>This project was funded by Rome Laboratory under Contract No. F30602-91-C-0067

The work described herein explores the following conjecture: it may be possible to determine whether a system is being used for its approved purpose by monitoring resource usage statistics captured in an audit log. The basis of this conjecture is the notion that application program functionality and resource use are so strongly correlated that reliable resource usage profiles can be constructed for different kinds of applications, that is, for different kinds of system usage. By periodically comparing a system's resource usage with a previously established profile for a particular kind of authorized use (e.g., inventory control), misuse may be detectable. On the other hand, to be useful, an inventory control profile must be general enough that it matches the behavior of a wide variety of inventory control programs and versions thereof. Using an insufficiently general profile for monitoring purposes may lead to an unacceptable number of misuse detection false alarms. For example, it would not be acceptable for the inventory control program to cause an alarm merely because it had been revised or upgraded and therefore behaved differently from its profile.

### 1.3 Overview of the Study

Developing the capability for reliable misuse detection envisioned above is a long term research goal. As a first step, this project applied intruder detection technology to investigate the relationship between application program functionality and resource usage.

To perform the analyses for this task, TIS subcontracted with established intrusion detection researchers at SRI International in Menlo Park, California, and Spring Hill College (SHC) in Mobile, Alabama. TIS built the audit data collection software, supplied the subcontractors with data, and provided high-level guidance for the analyses. The subcontractors selected the analytical approaches, performed the analyses, and reported the results. Responsibility for determining the content and format of the audit data was shared by all.

#### 1.3.1 Definition of Misuse

The ability to detect misuse depends in large part on how precisely misuse can be defined. Misuse could be defined as any use that differs from a site's previously established usage profile. Or it could be defined as any use that differs from that for which a site was approved by some controlling body, e.g., an export control authority. Clearly, the more narrowly and accurately defined a site's usage is, the easier it is to determine if current usage fits that definition. As a first step toward this difficult goal, most of the effort on this task was devoted to applying intrusion detection technology to differentiating application programs based solely on the audited behavior of programs that were executed on specially instrumented computer systems. Some effort was also devoted to attempting to combine profiles of functionally similar programs into a group profile. Group profiles could be used to represent the general classes of programs, e.g., programs for accounting, weather predicting, etc., normally occurring at a site. The purpose of this work was to explore another way of characterizing acceptable system activity, other than in terms of individual application profiles.

Differentiating application program behavior is different from conventional intrusion detection. In conventional intrusion detection, data representing each user's usage of a computer is analyzed to see whether it seems consistent with what has previously been observed about that user's past usage. If a user's activity seems anomalous compared to past behavior, then some suspicion is warranted that the audited usage was caused by an intruder, i.e., a different, possibly unauthorized, user masquerading under the legitimate user's identifier. For this study, it wasn't important whether the behavior seemed normal for a user; the focus was on whether observed behavior seemed normal for a given application program. For example, suppose that in the past, each execution of the "ls" directory lister at some given computer facility never used more than three seconds of CPU time. If one day that installation's audit data included an "ls" record that used fifty seconds of CPU time, it might indicate that something other than "ls" was really executing.

The above example is an oversimplification, of course. This part of the Export Safeguards project was a high-risk feasibility study, primarily because little has been published on the topic of analyzing audit data to detect differences in program behavior. The project began with little information available about which aspects of behavior would be the best discriminators. The subcontractors did not have direct experience on which to build, but were able to adapt analytical techniques that had been developed for intruder detection.

### 1.3.2 Summary of the Results

Performing meaningful analysis potentially requires analyzing many aspects of application behavior. Although TIS's ability to instrument audit data collection in operational UNIX<sup>TM</sup> systems was somewhat limited (see Section 2.2 below), several of the collected fields turned out to be useful in telling applications apart.

The results of the audit data analyses were mixed. The analysts were able to compile profiles of application programs. The ability to differentiate applications was tested by comparing applications using only their profiles, without referring to the program names that identified the applications. Although some individual application profiles were quite "unforgiving" and could almost always be used to differentiate records from other "guest" applications, other profiles were too forgiving to be used reliably. The records of some applications were more "obtrusive" as guests than others, hence more easily detected. The obtrusiveness of an application was often unrelated to how forgiving it was.

Because the set of audit data fields that could be collected was relatively small, significantly better results might be achievable if it were possible to collect additional types of data. In general, the analyses were more useful with individual application profiles than with group profiles or overall system profiles. Grouping profiles on the basis of functional, rather than behavioral, characteristics produced vague profiles that are less useful for detection of programs other than those in the profiled group.

### 1.4 Organization of this Paper

An overview of the project's audit data collection goals, strategy, limitations, and implementation are described in the following section. The analytical approaches that were applied by the subcontractors and the results of the analyses are presented in Section 3. Section 4 summarizes what was learned.

## 2 Data Collection Overview

Data collection has always presented challenges for intrusion detection researchers. It is difficult to locate organizations that will permit auditing by an independent organization. It is also difficult to persuade users to permit their usage to be audited. While designing an audit record to provide many fields for analysis, consideration must be given to minimizing performance degradation on audited systems. This section describes the manner in which TIS collected the audit data used by the subcontractors for their analyses. In most respects, the challenges faced by this project were similar to those faced by most other intrusion detection researchers.

### 2.1 Goals of Data Collection

The Safeguards audit data collection facilities were designed to provide as much useful data as possible for the data analysis research without wasting processing and analysts' time by including audit features that were not likely to improve the ability to differentiate profiles. Because it was not known in advance which aspects of computational behavior were the best at distinguishing programs, it was necessary to weigh the expected usefulness of the data that could be collected against the costs of collection. The costs included:

- staff time for implementing collection mechanisms,
- impact on the audited users' system response time,
- subcontractors' time for analysis, and
- capacity of the subcontractors' analysis tools and systems.

Because the above resources were fairly limited, it was necessary to select a relatively small set of audit fields. Therefore, early in the project some effort was devoted to developing an "educated guess" about which aspects of behavior would be the best candidate discriminators. The fields selected for collection are shown in Figure 1.

---

UNIX is a registered trademark of UNIX System Laboratories, Inc.



## 2.2 Data Collection Issues

The first collection issue is common among intrusion detection researchers. This is the problem of locating organizations that will permit auditing of their operational sites. There are several concerns that may lead an organization's management to be reluctant about permitting an independent researcher to collect audit data from its sites. Some of these concerns are:

- The auditing software may degrade the system's performance,
- The auditing software may interfere with other software or reduce the system's reliability,
- Auditing could facilitate spying on employee and corporate activities or capturing sensitive information.

Not only must an organization's management be willing to permit auditing, but the organization must have a suitable population of computer users who are willing to risk a potential invasion of privacy. For this project, the most readily obtainable supply of audit data was from employees at TIS offices. Users of TIS systems include individuals who perform administrative and technical functions, including word processing, document preparation, system analysis, project management and planning, and software design, development, and testing.

Having found usable sources of computer usage, the next issue involved developing instrumentation to collect audit data. Initially, it had been planned to instrument a multiuser UNIX operating system at the kernel level. This would require obtaining the kernel source code for a UNIX system. Because of the difficulties in obtaining a source code license, this approach was not possible. Instead, auditing software was designed to extract information from the process state table. This software was based on public domain utilities and did not require kernel source. It was carefully tuned so that there was no noticeable impact on system reliability.

Feature selection was the final data collection issue. To use the project's collection and analysis resources in the most efficient way, a highly knowledgeable system administrator selected a relatively small set of auditable features, based on in-depth knowledge of the operating system. These choices were discussed with the subcontractors and their statisticians, whose suggestions were also considered. The result was a relatively small but potentially useful set of audit fields.

## 2.3 Implementation of Data Collection

After it had been decided that the audit records should contain information from the process state table, it was necessary to decide how often to sample each program. One approach taken was to create an audit record at the termination of each process. This is a common strategy because it provides cumulative measures of memory, CPU, and other resource usage. In fact, both subcontractors had indicated that this kind of "per-execution image" auditing was most suitable for their analytical approaches.

The other approach to auditing involved periodically taking a "snapshot" of the process table. The period might range from a fraction of a second to many seconds. Every active process on the system was included in this "periodic" audit, thus providing an arbitrarily fine-grained, hence more complete, trace of program behavior.

From an operational standpoint, both of these collection strategies are necessary to provide an accurate representation of system usage. Periodic collection alone does not provide sufficiently accurate information because this type of auditing can be circumvented by processes designed to begin and terminate within the collection intervals. Per-image auditing is not complete either because it can be circumvented by programs designed to run for extended periods of time or never exit.

An added benefit of periodic auditing is that for long-running processes, it provides the necessary information for building profiles of resource usage over time. Such auditing is especially well-suited to analysis of sequences of events. However, analysis of event sequences is currently a weakness of intrusion detection systems. It was decided that because infrequent periodic auditing incurs very little overhead, such data would be collected for future use, even though it was not clear whether either subcontractor would have the resources needed to analyze it.

### 2.3.1 Acquisition of Process Table Data

The biggest data collection constraint was the lack of kernel source code. Access to the source code would have allowed a fairly straightforward implementation of the collection procedures in the operating system. Instead, to implement the per-image auditing tool, the dynamic system service libraries were modified by adding code to the exit routine called by every dynamically linked process. The code sends the process ID number to an audit collection daemon and waits for a response. The audit daemon accepts the process ID number, uses a system call to access the process table to gather the process statistics for the identified process, and then responds to the process, allowing it to proceed. The audit daemon was optimized so that the impact on performance was unnoticeable. Unfortunately, only dynamically linked processes were audited on exit; all statically linked processes were bypassed. Some statically linked processes (i.e., emacs) were relinked using the modified exit code. Statically linked processes that were not relinked could not be audited. The periodic mechanism, however, collected statistics on all processes, both dynamically or statically linked.

### 2.3.2 User-Controlled Auditing

Volunteers for auditing were solicited at the three largest TIS offices. At each office, the system that had the most (multi-user) activity was identified. Volunteers who were willing to have all their usage on that system audited were instructed to make a simple change to their LD\_LIBRARY\_PATH environment variable. This enabled the audit data collection software.

Protecting the privacy of the audited users was a significant concern, especially because audit data about users would be transmitted off site. Some users did not want their use of particular programs to be audited. To address these concerns, multiple levels of auditing were implemented, and each user was permitted to determine his or her auditing level. The implemented levels included: no auditing, partial auditing (a core set of programs only), and full auditing (every dynamically linked program run by the user). Each user also had the ability to turn auditing on and off at any time. In addition, user IDs were collected but user names were not. Without the user table, there would be no way to associate the data with any particular individual.

## 2.4 Results of Data Collection

With regard to impact on system performance and reliability, the audit data collection software caused only minor problems after being installed at the three sites. On occasion, the data collection file grew so large that it used all available disk space. There were a few instances in which auditing was wrongly blamed for reliability problems that were actually caused by unrelated errors.

The TIS Glenwood, Maryland, office was the main source of audit data for the study. Because one of the experiments required data from more than one "environment," data was also collected at two other TIS offices. Although everyone at the TIS Bay Area office in Mountain View, California, volunteered for auditing, there were so few users that too little data was collected on the system to be very useful. The TIS Los Angeles, California, office was useful as a source of "different environment" comparison data.

Site	Per-Image Total Bytes	Periodic Total Bytes
TIS Glenwood	120,416,964	2,148,201,816
TIS Los Angeles	218,043,920	—
TIS Bay Area	4,886,784	—

Table 1: Amount of Audit Data Collected

Table 1 shows the amount of data collected at each TIS office. Although almost twice as much per-image data was ultimately collected from TIS Los Angeles as from TIS Glenwood, much of the Los Angeles data was collected in a time frame that was not useful to the analysts.

	SRI	SHC
	---	---
Process ID	+	+
Control terminal	+	+
Accumulated CPU time	+	+
Percent of CPU time used by this process (decayed over time)	+	+
Accumulated CPU time for this process and all its children	+	+
Current command name	+	+
Current command plus any arguments	+	+
Numeric user ID	+	+
Combined size of data and stack segments (in kbytes)	+	+
Real memory size of process	+	+
Percentage of real memory used by this process	+	+
Disk I/O - page ins	+	+
Session ID of process	+	+
Start time of process	+	+
Exit time of the process	+	+
Process current state flags: system proc, proc being traced, etc.	+	+
Process nice level	+	+
Process ID of root of the process group	+	+
Process's parent ID	+	+
Number of open files	+	
Number of major and minor page faults incurred	+	
Number of swaps incurred	+	
Integral of process's real memory usage over time (e.g.; 60K over 3 seconds, integral = 180)	+	
Seconds resident (for scheduling)	+	
Ticks of cpu time	+	
Virtual size of the text segment	+	
Characters read/written	+	
User time used	+	
System time used	+	
Messages sent	+	
Messages received	+	
Signals received	+	

Figure 1: Audit Variables Collected

Figure 1 shows the process statistics that were collected from the process table. Shortly before beginning data collection for SRI, TIS enhanced its audit collection software. This meant that the content of the audit records provided to SHC and SRI were different and TIS was able to provide SRI with a few more audit fields. Figure 1 shows which fields were provided in the per-process image data to each subcontractor.

### 3 Audit Data Analysis Overview

Although the goal of the Export Safeguards analysis is somewhat different from that of conventional intrusion detection, the project was able to take advantage of analytical techniques and approaches that have been developed for conventional intruder detection. Both subcontractors first undertook a "training" phase, in which a large number of records were analyzed to yield profiles of the applications represented in the data.

In order to ensure objectivity, the subcontractors were told nothing about the content of the data files used for training, other than the source of the data, the format of the records, and the fact that each

record represented an application image. In fact, with one exception this is also true for the files used as candidate representatives of misuse. One file of data from Glenwood included several records that were created as a result of running a few unusual, resource-intensive applications. Both subcontractors were told which file included the resource-intensive data, but neither was told anything beyond this. Apart from the resource-intensive records, there was no difference between the files used for profile training and those used for comparison testing with the profiles.

The following two sections describe the two independent sets of experiments. The two approaches were very different. SRI's New Intrusion Detection Expert System (NIDES)[4] was well-suited to completeness and depth of analysis. To complement this approach, the goal of the SHC work was breadth of analysis, exploring several analytical approaches related to pattern recognition.

### 3.1 Description of NIDES Tasks

NIDES<sup>2</sup> has been used for research in intrusion detection for several years. Compared to traditional intrusion detection, the Export Safeguards project required somewhat different analysis using a fairly unusual set of audited characteristics of application behavior. Therefore, it was necessary to design and implement "measures" of behavior that had not previously been used. Apart from that, it was fairly straightforward to adapt NIDES to profile applications instead of users. Because each record was identified by the name of a program and because the content of the record represented the execution of that program, it corresponded directly to the usual user ID/user behavior paradigm of conventional intrusion detection.

Only the NIDES statistical tool was used for this project. NIDES built a statistical profile for each subject — an application program, in this case — that was represented (a sufficient number of times) in a "training set" of audit data. NIDES uses profiles as baselines of acceptable behavior. Instances of recent behavior for each subject can then be compared to the subject's profile. NIDES compares groups of recent record(s) of activity for each subject with the established profile for the same subject name to see whether the recent records are anomalous. Recent activity that is anomalous compared to profiled activity for the same subject is labeled as "masquerader" data. That is, a "masquerader" is a record whose name indicates it represents a different application than it actually does.

For this project, because the subjects were applications instead of users, it was more important to learn whether *individual* non-training records were anomalous. User behavior is more appropriately interpreted based on activity that is represented in a collection of audit records, but it was expected that each invocation of an application would be as significant as any other.

Several files of raw, unadulterated data representing actual system usage were collected. At least one month's worth of data was needed for establishing the baseline profiles. A subsequent data file, although also including only unmodified, raw data, included five noteworthy records. These five records, although properly labeled with their true application names, had been intentionally included as a sanity check. The five records represented the execution of two unusually resource-intensive (RI) applications. One was a password checker and the other was a prime number generator. It was expected that these applications would produce audit records that were significantly different from those normally generated at the audited sites. These records were used in refining, or tuning, NIDES's ability to detect masqueraders. By changing the name of an application on an RI record, the record could be used to try to masquerade as any (or every) profiled application.

The most systematic and exhaustive experiment involved cross-profiling. Unadulterated non-training records were used as "masqueraders" by comparing each application's records against the profiles of every other application. This was an excellent way of simulating a large amount of candidate masquerader data because, in effect, each non-training record could have its name changed so that it could masquerade as every other profiled application. The RI data records were useful as a sanity check, but precisely because they were so unusual they did not serve well as a fair test of NIDES's ability to differentiate normal applications. Cross-profiling of normal application records was much more informative than detection of RI records.

---

<sup>2</sup>NIDES is a revised version of SRI's Intrusion Detection Expert System (IDES)

## 3.2 Approach and Findings

For NIDES, the parameters that control profile-building are tuned in three phases — concept, verification, and refinement. NIDES's ability to detect masquerading records improved throughout these phases. As mentioned above, the RI records were used in true-positive testing, in which it is seen how successful the application profiles are in detecting, among a stream of records, known masqueraders that were not contained in the training data set. False-positive testing, which determines whether the profiles erroneously indicate that known non-masqueraders are potential masqueraders, was also performed.

### 3.2.1 Cross-profiling Experiment

The most comprehensive experiment involved running each application's records against the profiles of every other application. Of all the experimentation performed by the subcontractors, the completeness of this experiment resulted in the most objective evaluation of the utility of statistical intrusion detection techniques and of the usage variables that were collected for the purpose of differentiating applications.

Many applications had profiles that were too forgiving to be used to reliably detect masqueraders. Some applications, though (e.g., "pwd"), had profiles that could be used very successfully to detect almost all other applications. Other applications, e.g., "latex" (but not "pwd") were highly detectable by other applications *and* had profiles that were very successful at detecting almost all other applications. Still others, e.g., "vi," were fairly easily detected by other applications yet had very forgiving profiles. Profiles of applications such as "gettfullnm" were unusually useful for detecting some applications but of little value for detecting others.

Overall true-positive detection percentages were computed for all applications. True-positive detections are those in which NIDES flagged a masquerade. A false-positive detection occurs when NIDES erroneously indicates that a record is a masquerader when in reality it is not. The most successful, least tolerant, profiles, i.e., those with the best overall true-positive percentages, belonged to "latex" (98.53%), "getfullnm" (98.24%), "stty" (95.43%), "fmt" (90.02%), "emacs" (86.23%), and "mymoreproc" (82.40%). The least successful, most tolerant, profiles belonged to "vi" (6.19%), "grep" (13.38%), "cp" (24.07%), "compile"<sup>3</sup> (24.71%), "ls" (32.84%), "rm" (34.81%), and "more" (35.06%).

### 3.2.2 Grouping Experiment

Another experiment investigated the feasibility of grouping together applications with similar functionality to see whether the combined group profile could effectively be used to discriminate applications that are *not* members of the group. It was hoped that application groups might realistically represent the activity of an organization that might benefit from the type of control envisioned in the Export Safeguards project. For example, if the set of programs that comprises an organization's accounting system could be characterized as a group, then it would be possible to detect when any non-accounting program was run, without raising an alarm unnecessarily when any individual accounting program is replaced by another accounting program, possibly an upgraded version of the original.

With respect to Export Safeguards operational scenarios, the results regarding group profiles for functionally related programs must be regarded as a strong negative. No evidence was found that functionally related programs may be grouped in such a way that their combined profile may be effectively used to detect programs outside the functional group. Three groupings were designed. Groups A and B were both designed by referring to NIDES statistical information that indicated they might show high within-group similarity and high out-of-group detection rates. Group C was chosen prior to the NIDES analysis, based only on intuition regarding functional similarity. Groups A and B contain fewer members than Group C and were designed specifically because it appeared that their profiles would combine in a useful manner.

In the majority of cases, Group C's profile is worse than those of Groups A and B for detecting programs that are not members of the group. For example, "ghostview" could be detected by Group C only 59%

---

<sup>3</sup>This is not a compiler or a standard UNIX utility. It is a tool that compiles a directory of telephone numbers into a format more suitable for searching

of the time at the "yellow"<sup>4</sup> level, compared with 64.4% for Group A and 82.7% for Group B. There are occasional instances in which Group C performed as well as one or the other group, but this is rare. This should not be interpreted as a failure in designing Group C with the "wrong" members. Rather, it indicates that group profiling based on apparent functional similarity is likely to be an extremely difficult approach to misuse detection in the Export Safeguards scenario.

### 3.2.3 Measure Averages

The analyses produced "measure averages" that indicate how useful each of the audit fields was in differentiating applications. Although measure averages were not produced for the cross-profiling experiment, they were produced for detection of the RI records with respect to all the application profiles. Of the twelve measures shown, one of the most consistently useful measures was MEMCMB (combined size of data and stack segments). SIGNAL (signals received) and TEXTSZ (virtual size of the text segment) were the least useful.

## 3.3 Description of Pattern Recognition Tasks

Spring Hill College was selected as the second subcontractor because of the staff's previous research on intrusion detection using non-parametric pattern recognition techniques [3]. It was felt that pattern recognition was the most promising approach to characterizing application behavior, because it had been used successfully in the past to help determine which behavior features are the most distinctive among a population of users. Instead of analyzing the behavior of a population of users, though, this project's goal was to analyze the characteristics of a population of application programs.

Nonparametric pattern recognition provides two potential benefits. First, it is intended to reduce the problem of erroneously flagging some behavior as anomalous (a false positive alarm). Because initially there was no information regarding the profiles of applications, it was expected that false positives would be a significant problem. A second benefit of the nonparametric approach is its ability to deal with large amounts of data in a relatively small amount of time. This means that this kind of analysis is suited to a real-time operational setting. Although for this Export Safeguards project an operational scenario included off-line analysis of audit data, the fact that this analysis could be performed in real time could be a significant advantage in other scenarios. For example, if audit data is being analyzed to detect the activation of a virus (see Section 4 below), then the ability to perform analysis in real time is beneficial.

First, a profile was developed for each application that appeared in the audit data. Although it turned out that only a few of the variables (audit fields) were useful discriminators, the subset of variables that *were* of use turned out to be good discriminators. don't have many different colors and numbers. The pattern recognition analysis discovered a three-variable cluster that was very useful in distinguishing the set of audited applications. Combined size of data and stack, real memory size, and cumulative number of disk I/O page ins were reliable discriminators among application programs. To see how good these three-variable profiles were, in the second phase of the study, candidate "misuse" records were compared against the profiles. To provide a source of "misuse" records, raw data files, similar to those used for profiling, were altered by changing the program names on 286 (one per cent) of the records. The bogus names were chosen randomly from the list of valid program names. In this way, records were created that represented potential misuse, i.e., a program "masquerading" as another program. Using three detection techniques, these switches could be detected about 97% of the time. Although reducing the rate of false positive detections was a goal of previous pattern recognition research, it was not a goal of the pattern recognition experiments to determine the false positive detection rates for the techniques.

Had resources permitted, it would have been useful to simulate a more subtle kind of spoofing. For example, instead of program names being chosen randomly, they could have been chosen expressly because the profile of the chosen application was similar to the profile of the application being spoofed. Following is a brief description of the approach and findings of the pattern recognition analyses.

---

<sup>4</sup>An audit record is flagged at the yellow level when the combined abnormality of all its measures of behavior exceeds the top 1% threshold value of the profile against which the record is being compared.

### 3.4 Approaches and Findings

In order to compensate for the handicap of the unavailability of kernel source code and the relative paucity of audit fields, it was decided to investigate a range of analytical approaches to identify distinguishing application characteristics. There were several primary approaches. A brief discussion of two of the approaches and the findings of the most significant experiments is presented below.

#### 3.4.1 Data Reduction by Binary and Ternary Breakpoints

The objective of data reduction is to make a large amount of data easier to analyze without suppressing so much detail that the analysis is not informative. Data reduction techniques typically replace actual observed data values by mapping them to a smaller set of values. There are several ways of doing this. For the Export Safeguards project, the set of observed values for each field was mapped into sets of only two or three values. This is similar to mapping an analog signal into zero or one — binary breakpoints — or mapping many shades of color into black or white or gray — ternary breakpoints. The goal is to identify the fewest number of breakpoint(s) without losing so much of the original detail that the data field no longer contributes to differentiating the record. The audit data was mapped to 0/1 and 0/1/2 breakpoints, according to percentiles. For 0/1 reduction, the lowest 50% of the values were mapped to zero and the highest 50% were mapped to 1. For 0/1/2 reduction, the values were categorized into the bottom, middle, and top thirds.

Because there were several data fields that were mapped to their category values, the string of category values for each record can be regarded as its “pattern.” Binary breakpoint reduction yielded an 8-bit bit-string pattern.<sup>5</sup>

Breakpoint data reduction facilitated several types of analysis. For example, when 286 samples out of 28,437 records had their program names changed as described above, 248 of the changes were detected by noting that the binary pattern represented by the data values on the records were inconsistent with the (altered) program name on the records.

Another use of breakpoint reduction was in characterizing overall system usage. The purpose was to learn whether the application profiles were transferable to other “environments.” A different environment might mean a different user population, system configuration, or machine architecture.

Table 2 shows performance characteristics for the three environments that were audited. All three were SPARCs processors configured as both hosts and file servers for a local network.

One way of learning about transferability would be to compare individual audit records from one machine against profiles generated on another machine. To shed light on this issue, overall profiles of system usage were compared. The intent was to determine whether profiles generated by breakpoint reduction on some system with some set of users could be used to detect other applications on a different system with a different set of users to quantify the significant (as defined for the purposes of this project) differences among the machines that were being audited. Were more resources available, it would be useful to formulate a “normalization vector,” i.e., a set of transformations that could be applied to application profiles generated on some machine in order to make them relevant to some other machine. This project’s analysis confirmed that such normalization would indeed be necessary for transferability.

Site	Proc Type	Speed	Users	RAM mb	Swap mb	SCSI mbs	MFLOPS	MIPS	Main Bus mbs
TIS Glenwood	Dual	33mhz	50	64	120	5	6.1(dual)	40	128
TIS Los Angeles	10/30	33mhz	10	48	150	5	10.6	86	>80
TIS Bay Area	SPARC2	40mhz	3	32	64	10	4.2	28.5	80

Table 2: Performance Characteristics of Audited Systems

<sup>5</sup>For comparison, the NIDES analysis used sixteen logarithmic category bins. This would correspond to fifteen breakpoints.

### 3.4.2 Data Reduction by Clustering

Clustering is somewhat similar to breakpoint data reduction in that raw data values are mapped to a smaller set of values. However, it has an advantage, because it is more sensitive to the potential importance of outlying values. Whereas binary breakpoint reduction arbitrarily maps all values above the median to the same category, [1] describes clustering as "finding natural groupings in a set of data." In a geometrical sense, if a set of data has  $n$  variables, then cluster analysis would identify the "clouds" of raw data observations in  $n$ -space that best represent the entire set of observations. Each cloud includes a subset of observations that are similar to each other, i.e., that have similar values for the same variables.

Of the 286 records whose application names were altered, detection by cluster membership was successful with 191 records — about two-thirds of the cases.

Probabilities of cluster membership for the different environment were, as expected, different from the profiles. This also points up the need for normalization of application profiles, including cluster membership, before they can be utilized in an environment other than that in which the profiles were created.

## 4 Conclusions and Further Work

In general, the results of the analyses were mixed. It was demonstrated that profiles of applications could be built using techniques that had been used for intruder detection. In most cases, though, these profiles were not highly reliable for use in detecting other applications. Given the relatively small set of audit variables available as candidate discriminators, the results should not be used to infer that intrusion detection techniques are not promising for application differentiation. However, the results of this project suggest that monitoring system usage to detect misuse remains a research topic. Moreover, there remains significant uncertainty that monitoring for this purpose will ever be able to achieve the degree of accuracy that would justify relying on it.

The negative results regarding grouping applications according to functionality cast doubt on the feasibility of inferring application functionality from audit data. Further thought and investigation will be required if this technique is to be successful. Although the statistically similar applications could be grouped with a small degree of success, this does not have a great deal of utility for the Export Safeguards operational scenario.

Based on this project's experience and results, it appears that there are several related areas that would benefit from further research. These are not meant to be strictly "follow-on" projects. Rather, they are aspects of audit data analysis, some fairly closely related to this project and some more tangential, that are deserving of some attention and effort by the intrusion detection community.

### 4.1 Efforts To Benefit Export Control Monitoring

As mentioned above, monitoring system usage to detect misuse remains a research topic. In the event that additional work will be undertaken in this area, below are listed suggested directions for that work.

#### 4.1.1 Audit Trail Standardization

An area of research that would indirectly benefit export control monitoring is audit trail standardization. Effort in this area was one of the recommendations of the System Design and Long-Term Issues group at a recent workshop [2]. Because standardization will constrain the types of detection that are possible, it is important that the needs of application monitoring be taken into account. For example, this project might have failed if the only data available were those features normally audited for intruder detection. Application differentiation depends less on user-controlled variables, such as login/logout time and session location, than does user differentiation. It depends more on variables that are not under the control of a user. Standardization efforts should take into account the various purposes of audit data analysis, so that as many uses as possible may be accommodated.



### 4.1.2 Transferability of Application Profiles

There was little success in the investigation of the detection power of functional groupings. The purpose of the experimentation was to characterize an entire organization's (or suborganization's) activity. This problem would also benefit from additional efforts to develop "normalization vectors." A first step in this direction was the attempt to profile the overall usage of the system configuration at TIS Glenwood. This first effort was not tightly controlled, so the specific numeric results are not very reliable. However, it did indicate that it might be possible to perform experiments, similar to system benchmarking, designed to yield a set of functions by which applications profiles built from audit data at a site could be useful in detecting masqueraders at a different site. To be reliable, all aspects of the audited sites would need to be known and preferably controllable. These include: characteristics of the user population (e.g., novice or expert), machine architecture, commonly run applications, peripheral characteristics, and system load.

## 4.2 Other Uses of Application Profiling

### 4.2.1 Detection of Virus Activation

Another potential use of application differentiation is the detection of virus activation. This differs from virus detection in which source or object code is analyzed to see whether any of a known set of virus infections is present. Instead, applications that are vulnerable to viruses could be profiled in a way similar to what was done for this project. A possible approach would be to characterize normal, uninfected behavior of these programs over time. Program executions that differ from normal profiles could indicate the presence of a virus. If the events to be audited over time require modifications to the kernel, then this type of detection would almost certainly require source code for the subject operating system.

### 4.2.2 Analysis of Sequential Activity

Another possible direction would be to pursue identification and subsequent recognition of sequences of events within audit data. Section 2.3 mentioned the potential use of "per-interval" audit data in analyzing sequences of actions. This area has barely begun to be researched by the intrusion detection community. Standard intrusion detection has primarily considered sequential activity only in terms of prespecified rule bases and hypothesized scenarios. It might be worthwhile to design a tool that could analyze periodic audit data, determine which sequential patterns exist, and incorporate this information into application profiles. This could be used, for example, in real-time detection of unknown viruses, by noting a disruption in the usual sequence of events for each application.

## References

1. Duda, Richard, and Hart, Peter, *Pattern Classification and Scene Analysis*, Wiley-Interscience, 1973.
2. Longstaff, Thomas A., Results of a Workshop on Research in Incident Handling, Special Report, CMU/SEI-93-SR-20, September, 1993.
3. Lankewicz, Linda, Real-Time Anomaly Detection Using a Non-Parametric Pattern Recognition Approach, TUTR 91-106, Dept. of Computer Science, Tulane Univ., May, 1991.
4. SRI, International, NIDES User Manual, Version 1 - Alpha Release, February 17, 1993.
5. Trusted Information Systems, Inc., Export Safeguards Demonstration Statement of Work, ARPA Contract DABT-63-92-C-0017 under HJ1500-2091-0563/DAR28687, 3 June 1992.
6. Trusted Information Systems, Inc., and Pulse Engineering, SAFEGUARD System Specification (Preliminary), ARPA Contract DABT-63-92-C-0017, 29 March 1993.
7. Trusted Information Systems, Inc., SRI, International, and Spring Hill College, Export Safeguards Audit Data Collection and Analysis Final Report, Rome Laboratory Contract No. F30602-91-C-0067, 31 January 1994.

# CAN COMPUTER CRIME BE DETERRED?

Sanford Sherizen, Ph.D.  
Data Security Systems, Inc.  
Natick, MA  
Phone: (508) 655-9888  
FAX: (508) 650-0088  
E-Mail: SSHERIZEN@MCIMAIL.COM

**Abstract:** Deterrence is an essential element in the control of criminal behaviors. The primary objective of deterrence is to secure compliance with the law by detecting violations, discovering the perpetrators, and appropriately penalizing them to inhibit future violations.

In this paper, deterrence is applied to information protection, based on the premise that deterrence should be considered as a central concern in addition to the existing technical and managerial approaches to computer crime prevention. There is a need for personnel security officials to determine how best to change the existing perceptions of employees and outsiders regarding the risks of getting caught in computer crime activities as well as the perceived payoffs from such activities.

Various concepts of deterrence are reviewed, followed by a discussion of what social science researchers know and don't know about the topic. Problems in applying the concept to computer crime are considered. The final section of the paper focuses on the particular types of computer crime and computer users appearing to have the most deterrence potential and the policy and program approaches needed in order to create deterrence within Governmental organizations.

An earlier version of this paper was presented at the Computer Crime: A Peopleware Problem Conference, sponsored by PERSEREC, Monterey, CA, 24 -25 Oct. 1993. My appreciation to Dr. Ted Sarbin for guiding me and for developing the conference.

© Copyright, Data Security Systems, Natick, MA 1993

## **Why is Deterrence Important for Computer Crime Prevention?**

Discussions about appropriate punishments for computer criminals often suggest that harsher punishments are needed to deter their behaviors. Yet, a review of the criminological literature suggests an uneven and often contradictory picture of the effectiveness of deterrence. The purpose of this paper is to explore whether deterrence can contribute to computer crime prevention and, if so, the conditions under which it can best be achieved.

At this time, deterrence is not considered as an important aspect of information security and computer crime prevention. This lack of consideration is less due to a conscious consideration that deterrence cannot work than for operational reasons. While legislators and attorneys may consider the issue in their deliberations, information security personnel are more concerned with the direct issues of prevention and detection rather than the broader issues of determining an ideal punishment scheme. Organizational lawyers and senior executives make deterrence-related decisions but they must weight reputation and other critical organizational concerns. If organizations choose not to press charges against an individual found committing a computer crime or abuse in order to protect the organization's reputation, that "letting someone get away with it", even when the person loses their job and is punished in other ways, sends a clear message to other employees. Thus, the current treatment of information protection problems may well run counter to deterrence.

It is important to consider how to place deterrence within computer crime prevention efforts. A deterrent perspective can help to guide national policy, particularly in making computer crime and related laws more effective in curbing computer crimes and abuses. Even limited success with deterrence can provide some protection from an increasing number of computer crimes and the growing seriousness of the problem.

## **What is Known About Deterrence?**

Deterrence is an essential element in the control of criminal behaviors. Its primary objective is to secure compliance with the law by detecting illegal activities, discovering the perpetrators, and appropriately penalizing them in order to inhibit future violations.

Deterrence offers a rational approach to limiting an individual's involvement or willingness to participate in illegal acts. Deterrence is built on the assumption that if the cost of an undesirable behavior can be increased, the behavior will decrease.

Classical deterrence models suggest that the effectiveness of the legal cost or threat is a function of how individuals perceive the certainty, severity, and celerity (swiftness) of punishment. This "rational-choice" behavioral model is based on the premise that humans are rational, hedonistic beings who know what is harmful to them, so that based upon a knowledge of laws and the fear of sanctions, they are able to choose and control their behaviors to avoid adverse consequences. Social control experts need only understand the correct "dosages" of rewards and punishments in order to lead individuals to behave properly.

Empirical research on deterrence, however, does not support this "rational-choice" model. Various empirical social science studies on crime lead to the conclusion that deterrence is much more complex than theory (and common sense) suggest. [24; 25] Criminals may not act as rationally as the theories assume, there are complicated rules affecting how an individual perceives risky situations, and many individual as well as organizational factors intervene between the threat of legal sanctions and behavioral outcomes. (A fuller analysis of the deterrence literature can be found in 18.)

Comparatively little agreement exists in the research literature about deterrence and its application to criminal behavior. [12; 3] In general, the little agreement that exists regarding deterrence is that the opportunity and reward components of the rational-choice model of crime appear to be operative under certain conditions while the risk or cost component, as measured by perceived risks of formal sanctions, does not appear to be operative. [12]

Clearly, the mechanistic approach to human behavior and control structures is simplistic, both for its limited understanding of the complexities of rational behavior as well as its emphasis only upon formal legal sanctions. The varieties of human behaviors, the complexities of human perceptions affecting behaviors, and the often inadequate functions of social control make this approach problematic.

The "rational potential criminal" may apply to limited cases. People who contemplate committing a crime often have incorrect or unrealistic perceptions of the probabilities of being sanctioned and of the severity of the sanction. Further, many people who commit crime act on impulse, either under the influence of drugs or alcohol or simply as the result of opportunity and need intersecting. [7]

More specifically, the research can be summarized by three conclusions. [Ibid, 102-103] First, research has failed to unearth a consistent deterrent influence of perceived severity of formal sanctions. Second, while most studies find a consistent but modest effect of perceived certainty of formal sanctions, others find that this effect is conditional, holding only for persons who are uncommitted to conventional morality. Third, the above results may be questionable because of methodological shortcomings of the studies from which they were generated.

Relatively little is known about risk perception and behaviors as it applies to crime decisions, although there is a large literature on risk perception and decision making applied to other topics, including gambling and health. [19] Studies of risk perception and deterrence have failed to recognize the complexity of the perceptual processes that intervene between the threat or experience of legal sanctions and the behavioral outcomes. There is a need to specifically examine computer criminal perceptions of punishment as well as risks [4].

There is a growing consensus on the importance of informal social controls in deterring criminal behaviors in place or in addition to the more formal legal controls. These informal sanctions, called extra-legal factors, create compliance with socially accepted behaviors. In a review of trust violations [11], the organizational literature reveals differing types of formal and informal controls over illegal behavior. Informal sanctions (co-worker reactions) can be even more effective than formal sanctions (corporate and criminal law). [13; 6] Conscience or internalized norms and attach-

ments to significant others, including friends, family, and colleagues/peers, can influence criminality by decreasing the expected gain or utility of crime. [14] Shame and embarrassment are informal threats of sanctions that are important predictors for some individuals on whether they will become involved with criminal behaviors. [5]

It is unclear from the research what strategies are most effective for increasing deterrence. There does tend to be agreement about the essential factors affecting an individual's decision to commit a crime. The most relevant include:

- (1) crime control factors- the certainty, swiftness, and/or severity of punishments, both formal legal sanctions as well as interpersonal sanctions by family, friends, and significant others
- (2) risk and profit factors-interactions of individual perceptions, objective cost-benefit realities, and behavioral activities
- (3) individual ("internal") factors-how conventional norms are accepted by individuals as moral reasoning and self-image concerns
- (4) crime opportunities- the protective safeguards in place, crime event decision-making, and the opportunity costs considerations

Yet, how much each of these contribute to the crime decision or how each of these can be changed in order to deter crime is not certain. At this time, there are no sure ways to know which social policies on deterrence are most effective or could be considered as an appropriate means to diminish crime.

### **Applying Deterrence to Computer Crime Prevention**

There is a need for information security officials to determine how best to change the existing perceptions of employees and outsiders regarding the risks of getting caught in computer crime activities as well as the perceived payoffs from such activities. That will not be easy but there are several applied social science options available.

As with other white collar criminals, computer criminals are often more easily dissuaded than are "less rational" criminals who commit illegal acts when opportunities occur rather than as a result of planning their crimes. Further, the extra-legal social stigma and negative affects on job opportunities can be powerful incentives to prevent certain middle-class persons from becoming involved with computer crime. In these ways, certain forms of computer crime and certain potential computer criminals are more deterrable than others.

Making deterrence part of computer crime prevention will not be a simple effort. As difficult as deterrence is to apply, computer crime makes an even more difficult target. The variety of computer crime activities tends to complicate the determination of what would be the best deterrence policy choices. What might work for teenaged hobbyists might not work for destructive hackers. Average users might be more affected than technically skilled users. Individuals might be deterred but managers who decide to use computers for organizational gain might not be. [1] Deterrence might work in one industry but not work in another industry. Further, computer use now involves a variety

of environments, including home, school, work, hobby, etc.. All of these have different controls (or lack of them) and an inconsistent and non-sequential ability to influence behaviors.

Partial answers about deterrence are possible, at least in terms of where deterrence emphases need to be placed. Legislative, law enforcement, and organizational changes need to be made in order for deterrence to be effective with computer crime.

### Legislative Changes

Deterring computer crime will require the public sector to pass improved legislation (2) and the private sector to study, develop, and implement appropriate security measures. Computer crime deterrence requires more apprehension and punishment in order to function. [15] Even though there are 49 state computer crime laws and a number of Federal computer crime laws, there have only been a handful of criminal prosecutions. [22] If the perception of the certainty and severity of punishment is a key variable in explaining deterrence, then the law has not been an effective force in controlling computer crime. [10] Deterrence of computer crime should focus on tailoring penalties to computer crime severity, with special attention being paid to key information processes, industries, and types of violations. As important, there is a need to consider revising wire and mail fraud laws so that they more directly cover new technological development. These fraud laws, as well as other laws, have often been used by prosecutors in place of the weak and outdated state and federal computer crime laws.

Changes are also necessary in terms of mandatory reporting. One federal prosecutor (private conversation) suggested that computer crime will not be controlled until organizations are required to report these crimes to law enforcement. Such a requirement would maximize opportunities for the authorities to determine which cases require legal attention rather than to await cases depending upon the willingness of organizations to press charges. Interestingly, the Federal Sentencing Guidelines [17], which emphasizes the reporting of crime (as well as detection and prevention) and recent SEC barring of Salomon executives from further Wall Street activities due to their lack of reporting of underling's illegal acts may serve as a warning shot to managers. The U.S. Sentencing Commission's consideration of computer-related crimes for inclusion under the Guidelines could increase organizational attention to this issue even further.

### Law Enforcement Changes

Legislation and regulation alone will not be sufficient, however. If deterrence is to become more of a computer crime prevention issue, law enforcement aspects of computer crime prevention, such as current resource limitations on investigation and prosecution of computer crimes, will also have to be addressed. In many ways, deterrence involves risk and "payoff" decisions by individuals [8]. For most individuals who commit computer crimes, detection and punishment are so infrequent that this would seem to be of little concern to them. Those few computer crime cases which have made it into the criminal justice system have not led to speedy or severe punishments. At times, cases are mishandled by law enforcement agencies [20], raising questions about the effectiveness of the law.

## Organizational Changes

Beyond formal laws and regulations, there are other possibilities for applying deterrence to computer crime. One possibility is to focus on countering the social influences that lead people to commit crimes. Researchers have found that controls over certain illegal behaviors were associated with moral commitment (internalization of legal norms), fear of social disapproval, and fear of legal punishment. [5] Relating that to computer crime, it is clear that organizations can attempt to influence perceptions of appropriate computer behaviors.

To a large degree, employees are influenced in their views about "normal" computer use and computer crime as a result of group interactions. Individuals make decisions, including risk decisions, as group members and are influenced by group norms. In that sense, an individual's perception of risk can be modified by the tendency of a group discussion to shift the preferences of members of the group toward more risky choices than they would have selected as individuals. [9]. On the other hand, if the group process can be influenced by deterrent messages, then this may be an effective means of swaying individual perceptions toward viewing increased risks of computer abuse activities.

Deterrence of computer crimes can take other behavioral forms. For some employees, minimizing their opportunities to legitimize or neutralize their crimes forces them to understand what are and what are not appropriate activities. Sykes and Matza [21] suggest that there are five major types of neutralization. These are (1) denial of responsibility, (2) denial of injury, (3) denial of the victim, (4) condemnation of the condemners, and (5) appeal to higher loyalties. Relating this to computerized activities, an organization can attempt to specifically counter these attempts to redefine crimes, forcing employees to understand that there are no justifications for what they are attempting.

This countering of justifications is particularly important for two reasons. First, computerized environments remove people from direct access to many of their work functions, with work "disappearing behind the screen". [25] Work consists of pushing keys, moving data files, and other abstract work that can remove the individual's feel of control and involvement as well as responsibility for his or her acts. Second, the downsizing of the Government and other economic threats that are striking the American labor force are causing anger and resentment among employees. [14] The result is a situation that easily allows individuals to view themselves as victims and to structure their criminal activities as something that is appropriate, allowable, and, in a word, a "non-crime".

Organizations can minimize these "non-crime" viewpoints by developing:

- (a) information security awareness training that directly stresses what is a crime, viewed legally as well as ethically
- (b) social control mechanisms that stress group norms and social embarrassment which stress that such activities let down colleagues and co-workers [13]

- (c) deterrence for employees using computer systems by finding and questioning work errors, providing prompt security warnings, and highlighting the fact that there is control and security monitoring in place
- (d) distribution of information about the punishments that have been given to convicted computer criminals

Finally, computer crime can be perceived by employees as a "normal" response to organizational structure. This crime can be controlled by changing the organizational climate and/or how it is perceived by employees. A "criminogenic" environment [16] is where the organizational culture, values, and structure unwittingly contribute to crime by sending certain messages about crime. Security managers should determine if their organization has such an environment and, if so, what can be done to change those messages. Surveys of how employees view information security and computer risks would determine whether an organization is producing positive or negative messages about crime. Do employees perceive that access control measures are put in place? Do they feel that security mechanisms are operating? Do they assume that their bosses have little interest in security? Are crimes often found in the organization, indicating organizational vulnerability? If these factors are found, the organization may have a climate that supports or in other ways fosters computer crime. If this is true, then security personnel need to actively change organizational structures and employee perceptions. [Ibid.]

It is clear that making deterrence a computer crime prevention option will be a difficult undertaking. There are, however, specific changes which are available that can lead employees and others to learn that computer crime does not pay. It is important that the information security community, working with legislators and prosecutors, determine effective deterrent measures that can protect information.



## **BIBLIOGRAPHY**

- (1) Braithwaite, J. and T. Makkai. (1991). "Testing an Expected Utility Model of Corporate Deterrence," *Law and Society Review*, 25, 1, 7-39.
- (2) Charney, Scott. (1992). *The Computer Crime Initiative: The Justice Department's Response to the Growing Threat Posed by Computer Criminals*. Washington, D.C.: Department of Justice.
- (3) Cook, P.J. (1980). "Research in Criminal Deterrence: Laying the Groundwork for the Second Decade." In N. Morris and M. Tonry, (Eds.), *Crime and Justice: An Annual Review of Research*, Vol 2. Chicago: University of Chicago Press, 211-268.
- (4) Cornish, D.B. and R. V. Clarke. (1986). *The Reasoning Criminal: Rational Choice Perspectives on Offending*. New York: Springer-Verlag.
- (5) Grasmick, Harold G. and Donald E. Green. (1980). "Legal Punishment, Social Disapproval and Internalization as Inhibitors of Illegal Behavior," *Journal of Criminal Law & Criminology* 71 (Fall): 325-335.
- (6) Hollinger, Richard C. and John P. Clark. (1983). *Theft by Employees*. Lexington, MA: Lexington Books.
- (7) Jacob, Herbert. (1979) "Rationality and Criminality," *Social Science Quarterly* 59: 584-85.
- (8) Katz, J. (1988). *Seductions of Crime: Moral and Sensual Attractions in Doing Evil*. New York: Basic Books.
- (9) Myers, David G. and Helmut Lamm. (1976). "The Group Polarization Phenomenon," *Psychological Bulletin* 83: 602-27
- (10) Nelson, B. (1991). "Straining the Capacity of the Law: The Idea of Computer Crime in the Age of the Computer Worm," *Computer/Law Journal*, April, Vol. 11, No. 2, 299-321.
- (11) Parker, Joseph P. and Martin F. Wiskoff. (1991). *Temperment Constructs Related to Betrayal of Trust*. Monterey, CA: PERSEREC.
- (12) Piliavin, Irving, et al. (1986). "Crime, Deterrence and Choice," *American Sociological Review*, 51:101-119.
- (13) Reichman, N. (1989). "Breaking Confidences: Organizational Influences on Insider Trading," *The Sociological Quarterly*, 30,185-204.  
Roache, J. Y. (1968). "Computer Crime Deterrence," *American Journal of Criminal Law*, 13, 3 (Summer), 391-416.
- (14) Sarbin, Theodore R. (1993) "The Power of Resentment: Some Observations on Trust and Betrayal with Special Reference to Computer Crime". A talk delivered at the Fifth Annual Conference of the Department of Defense Security Institute, Williamsburg, VA, May 4-8.

- (15) Sherizen, Sanford. (1985). *Federal Computers and Telecommunications: Security and Reliability Considerations and Computer Crime Legislative Options*. A Contractor Report for the Office of Technology Assessment, February, 1985. (Available from NTIS as Report PB 86-208931.)
- (16) \_\_\_\_\_ . (1993 A). *Computer Crime As A Unique Personnel Security Problem: Understanding The Problem And Developing Potential Solutions*. A Report Prepared for PERSEREC, Monterey, CA.
- (17) \_\_\_\_\_ . (1993 B). *Federal Sentencing Guidelines: New Information Security Management Considerations*. (Unpublished) Natick, MA: Data Security Systems.
- (18) \_\_\_\_\_ . (1993 C). "Can Computer Crime Be Deterred?" A paper presented at the Computer Crime: A Peopleware Problem Conference, sponsored by PERSEREC, Monterey, CA, 24 -25 Oct.
- (19) Sprent, Peter. (1988). *Taking Risks: The Science of Uncertainty*. New York: Penguin Books.
- (20) Stoll, Clifford. (1989). *The Cuckoo's Egg*. New York: Doubleday.
- (21) Sykes, Gresham and David Matza (1970). "Techniques of Neutralization: A Theory of Delinquency," in Marvin E. Wolfgang et al., Ed., *The Sociology of Crime and Delinquency*, 2nd ed. , New York: John Wiley, 292-299.
- (22) U.S. National Institute of Justice. (1991). *State Computer Crime Statutes*. Washington, D.C.: Government Printing Office.
- (23) Zimring, Franklin. (1971). *Perspectives on Deterrence*, Public Health Service Publication, No. 2056, Chevy Chase, MD: National Institute for Mental Health.
- (24) \_\_\_\_\_ and Gordon J. Hawkins (1973). *Deterrence*. Chicago: University of Chicago Press.
- (25) Zuboff, Shoshanah. (1990). *In the Age of the Smart Machine: The Future of Work and Power*. New York: Basic Books.

# DEMONSTRATING THE ELEMENTS OF INFORMATION SECURITY WITH THREATS

Donn B. Parker  
SRI International  
333 Ravenswood Avenue  
Menlo Park, CA 94025 U.S.A.  
Tel. (415)859-2378, Fax (415)859-2986  
Net address: donn\_parker@qm.sri.com

January 1994

**Abstract:** This paper presents a rigorous demonstration that the elements of the purpose of information security should be expanded from availability, integrity, and confidentiality to availability and utility, integrity and authenticity, and confidentiality and possession. This discussion identifies loss scenarios that information security clearly should address and demonstrates that each scenario is addressed by one and only one of the six elements. Therefore, all six elements are needed. The six elements aid in identifying a far more extensive list of threats than has been previously produced. In addition, by adding possession to the list, new insights are gained about the differences in military/government and business information security.

## INTRODUCTION

The purpose of information security that most information security specialists identify is to preserve the three elements of confidentiality, integrity, and availability of information. In a 1991 paper, "Restating the Foundation of Information Security" [1], I argued that this is a dangerously oversimplified definition of information security. The preservation of these three elements does not include protection from many kinds of information losses that information security should address. My intent is to demonstrate in more rigorous fashion that these elements must be expanded for information security to be sufficiently comprehensive to protect information appropriately in all of its security aspects.

Accordingly, I have added utility, authenticity, and possession of information as additional elements that must be included. I discovered the last element, possession of information, in dealing with the theft of small computers, wherein the value of loss of the exclusive possession of the information content of the stolen computers is often greater than that of the computers. Yet the thieves may not even be aware of the information and therefore violate neither the possible confidentiality nor availability of it when the victim still possesses a backup copy. The victims have lost exclusive possession of the information in these cases but not its confidentiality, availability, utility, integrity, or authenticity. The victims might suffer a loss from extortion, for example, even if none of these other elements are violated.

### Rationale for Expanding Security Elements

The stated pairing and order of these six required elements and the resultant deeper understanding of information security also have some logic and practical value as will be seen. I will demonstrate the need for these six elements through scenarios of loss that information security must address when each loss is explicitly covered by one and only one of the elements. Therefore, if a loss scenario is accepted

as a subject for information security attention, then the element covering the loss in that scenario must be attributed as an element of information security. In addition, I suggest some controls that are needed specifically to protect the information from each loss. Some of these controls might be overlooked if any one of the six elements has not been explicitly included. This demonstrates the usefulness and practical application of the elements.

The possibility should always be anticipated that more elements of information security than the six presented here may be needed to cover additional types of losses. This could happen as information technology advances, criminals become more innovative, or the scope or nature of information security is changed.

The inverse application of the elements must also be included for completeness in information security. Each element is applied in terms of preserving attributes of information. The inverse applications include the removal of the harmful attributes of information. Examples are: removing the possession of information from those wrongfully possessing it, destroying the integrity or authenticity of obsolete information so that it is complete and valid in its new form, removing the availability or utility of information that is not supposed to be available or useful to certain parties at certain times and locations, and preserving the right and method to make confidential information publicly known.

The recovery and correction functions of information security often come into play here. These inverse applications of the elements will be considered to be implicit in this exposition of the elements. Explicit treatment of them and the implications for the scope of information security will be left for further analysis and a future paper.

If the elements of information security are not rigorously, comprehensively, and logically stated and addressed in terms of correct English language meanings of the words used to state them, I claim that information security will remain an incomplete and flawed folk art as it is today. Technical definitions may narrow the meaning of words but must not conflict with common usage. For example, integrity has been abused in this regard by defining it incorrectly to include the meaning of authenticity. (See the appendix for the dictionary and proposed formal information security definitions of the elements.) Without such definitions, information security and its practitioners would ultimately lose the confidence of society, and the perpetrators of information loss would continue to successfully take advantage of information security shortcomings both in practice and under the law.

For example, all information security specialists should understand that protecting the possession of information as intellectual property is an obvious requirement under common, copyright, trade secret, and patent law. Yet possession cannot be included within the meaning of the original three elements of preserving confidentiality, integrity, and availability. To illustrate, possession but not confidentiality can be lost if the victim encrypted the information before it was stolen. Moreover, by definition, integrity is not lost or changed in this example, because integrity is an intrinsic property of information content and is not associated with the extrinsic property of possession. On the other hand, possession does not affect the content and its integrity. Finally, possession but not availability can be lost if, for example, the new possessor makes the stolen information available for timely sale to the owner, such as in a case of extortion. Exclusive possession can also be lost but availability preserved if only a copy of the information is stolen. Loss of exclusive possession is unique to information in contrast to stealing copies of tangible objects that are not authentic originals. Two or more people can simultaneously possess the identical authentic information, and information security must explicitly take that into account.

Possession is an extrinsic property of information similar to confidentiality. The information may or may not be possessed or held confidential, but this has no effect on the information itself. Examination of the information does not necessarily identify who possesses the information or if anyone possesses it; it could be in the public domain. In addition, the information may contain the ownership identity but not the identity of the current possessor. For information security purposes, ownership should be considered to be a form of possession, and ownership means possession or the right to possess unless denied by a higher authority. For example, a judge could rule that a computer criminal has the right to own a database held in escrow but only for the purpose of selling it or giving it away, not possessing it. Under law, one party may possess information but another may own it. Stealing information may be different from stealing the ownership of information.

I believe that possession has not been fully considered as a unique element of information security because government, where possession and confidentiality are mostly considered synonymous, has dominated the development of information security technology. Treating possession and confidentiality separately reveals a profound underlying difference in the security needs of business and democratic government, and makes clear why democratic government security and business security differ.

In a democratic government, information is collectively owned by all the people governed; it is public information, and the only constraint is whether it should be kept confidential for the best interests and with the consent of the people. Otherwise, at least in the United States, the Freedom of Information Act requires that the information be shared with the public. A democratic government holds no exclusive copyright, patent, or trade secret right to it. Government does not buy, sell, barter, or trade information, except in some cases to cover costs of publication or to offset costs of other services.

Consequently, in business, information is a commodity or facilitates a service that is bought, sold, bartered, and traded to make a profit. The primary purpose of information security is to protect most business information as an asset or property.

The consequences of loss also differ between government and business. When government information is stolen, only loss of confidentiality is feared, but when business information is stolen, possession or exclusive possession is lost. Loss of confidentiality in business is only a severe negative consequence in a few cases after loss of possession. For example, the huge problem of software piracy is the loss of possession including control over its use, and confidentiality is rarely an issue. Business does have a small amount of high-value information for which loss of confidentiality rather than loss of exclusive possession is the greatest concern, resulting most often in loss of profits. A loss of confidentiality in government, such as premature revelation of date and location of war games, would result mostly in loss of military or diplomatic advantage. In business if a date and location for marketing a new product were known to a competitor who preempted the effort with its own new product marketing effort, profits could be lost.

We must conclude that business and government information security have some of the same confidentiality concerns, but business information security has the additional element of possession that government does not have. Taking most kinds of information from the government is not stealing and no loss is incurred. Taking most kinds of information from a business is stealing, and loss of possession or at least exclusive possession is usually most serious.

As concluded from the *TCSEC Orange Book* and the many other publications from the National Computer Security Center and the National Institute for Standards and Technology, these differences make clear that in government employee clearances, the principle of need-to-know, mandatory access

control, classification of information, and cryptography are typically the most important controls. In business, the owner, custodian, and user accountability principle of need-to-withhold; discretionary access control; copyright and patent; and digital signatures are typically the most important controls as seen from the proceedings of commercial information security conferences and trade journals.

### Value of Expanded Security Elements in Identifying Threats

Now consider the value of the expanded and more comprehensive elements of information security for the purpose of identifying threats.

More actions that adversaries may take against information can be conceived than the typically stated modification, destruction, disclosure, and use if the security elements are separated into the more distinct six parts. For example, I am led to derive a more comprehensive threat list for information security [2]. The following is a far more complete list of abusive actions against information derived by considering all six elements and from collecting and studying more than 3500 computer abuse cases since 1958 [3]:

- Threats to availability and usefulness
  - Destroy, damage, or contaminate
  - Deny, prolong, or delay use or access
- Threats to integrity and authenticity
  - Enter, use, or produce false data
  - Modify, replace, or reorder
  - Misrepresent
  - Repudiate (reject as untrue)
  - Misuse or fail to use as required
- Threats to confidentiality and possession
  - Access
  - Disclose
  - Observe or monitor
  - Copy
  - Steal
- Exposure to threats—endanger by exposure to any of the above threats.

The last item, exposure to threats, was added as a separate category to deal with the human failing—and sometimes crime—of negligence on the part of managers, owners, custodians, users, and information security specialists. Some of the threats listed might logically appear under different elements such as damage and contamination that can cause loss of integrity and authenticity as well as loss of availability and utility. The threats are placed, however, where they would be expected to first cause the most likely loss and where a security specialist would probably look first.

## **FORMAL DEMONSTRATION**

I contend that the following six scenarios of information losses derived from real cases are well within the range of threats, from the list above, and that information security should protect against them. Following each scenario is an analysis of why each of the six proposed elements does or does not address the loss scenario. Because one and only one element of information security covers each scenario, that element must be included as a stated descriptor of information security. My suggested formal definition (consistent with the dictionary definition) is given with each element as it applies to information.

### **Loss Scenario I: Availability** (Immediately usable, capable or accessible for use, or may be obtained for use)

Scenario I discusses the significance of the element of availability in a computer data file theft. In an act of sabotage, the name of a data file is removed from the file directories in a computer possessed by the victim. The data file is no longer available to the users because the computer operating system recognizes the existence of information for users only if it is named in the file directories.

The other information security elements do not address this loss because the utility, integrity, authenticity, confidentiality, and possession of the unavailable information have not been changed in the scenario as stated. Therefore, since availability is prevented as a result of this act, preservation of availability must be accepted as a purpose of information security. This scenario is based on a case in Los Angeles where a credit union was shut down for 2 weeks in an extortion attempt to renew a program maintenance contract. It is surely a case for information security concern.

The severity of availability loss can vary considerably. For instance, all copies of a data file can be misplaced and not found until after the need for them is passed, or a data file can be partly usable with delayed recovery at moderate cost. Or, the user may have merely inconvenient access to the file with timely full recovery.

### **Loss Scenario II: Utility** (Useful for a purpose)

In this scenario, a serial killer encrypted detailed descriptions of his killings in his PC so that he could relive them, yet they would be safe from others' attempts to read them. When he was captured, the police needed the clear text material as evidence, but the suspect claimed that he had forgotten the key. The usefulness of the information had been lost and in this case could only be restored if cryptanalysis could be successfully accomplished. (Cryptanalysis was successful, and the suspect was convicted.) The loss of the information as evidence is surely an important information security concern.

Although this scenario could be described as a loss of availability of the key that was forgotten, the loss described in the scenario of concern here focuses on the usefulness of the information, not on the key. The only purpose of the key was to facilitate the encryption. In this illustration, the loss of utility of the information was the concern. The loss of the key would be a different kind of loss. The information in this scenario is available for decryption but in a form that is not useful for its intended purpose until it has been decrypted. The integrity, authenticity, and possession are unaffected. Unfortunately, confidentiality was greatly improved temporarily, but after cryptanalysis was not an issue.

The loss of utility can vary in severity. The most severe case would be the total loss of usefulness of the information with no recovery. Less severe cases could range from somewhat useful with full usefulness of data restored at moderate cost to less than perfect usefulness with timely full recovery.

### **Loss Scenario III: Integrity** (Complete, whole, and in readable condition)

A software company under pressure to meet a delivery date provided a client with an accounts-payable application program without including an important control. The master copy held by the software company contained the control that functioned according to specifications. The omission was not discovered because no known violations of the control occurred. An accountant in the client company, however, discovered that the control was missing and that the program had failed to check for duplicate payments. The accountant took advantage of the omission and engaged in a large accounts-payable embezzlement. The client company sued the software supplier for negligence. This composite case, derived from two reported cases, is an important information security problem.

The software application performed as intended except that the duplicate billing control was missing. Because the program was incomplete, however, the product lacked integrity. (The strict English dictionary definition of integrity stated in the appendix is used here and not the definition often used in information security that incorrectly incorporates the definition of authenticity of conformance to fact and reality.) Integrity is limited to mean a state of completeness, wholeness, and soundness when applied to information.

Availability and utility were not violated in that the program was in use, was useful for its intended purpose, was authentic, and performed correctly as far as it went. Its failure to perform the duplicate billing control meant that the program performed incorrectly under some circumstances—not because the control was incorrectly programmed, but only that it was missing. If the control was present but failed to conform to specifications, the program would lack authenticity, but conforming to specifications was not relevant because the control was missing. The software company's failure was omitting the control in the program delivered, not the failure of the program as far as it performed according to specifications. It was also a genuine program from the software company. Thus, the program lacked integrity, not authenticity. Confidentiality and possession are not affected and not at issue in the scenario.

The severity of integrity loss can vary. Significant parts of the information can be missing or misordered but be short of total unavailability, and with no recovery possible. Or, with delay, a few parts of the data in that condition can be restored at moderate cost. Finally, small amounts of missing information can be recovered in a more timely way at low cost.

### **Loss Scenario IV: Authenticity** (Conforms to fact and reality, valid, true, real, and genuine for a purpose)

A software distributor obtained a computer program on a disk from an obscure publisher. The distributor changed the name of the publisher on the disk to a well-known name and, unknown to either publisher, distributed it successfully in a foreign country. This is one of many frauds called software piracy, and huge losses worldwide make it a serious information security concern.

The software was misrepresented as being published by a well-known publisher. Therefore, it did not conform to reality and was not an authentic program from that publisher.

Availability and utility are not at issue in this case. The software also had integrity because it was complete and sound. The software publisher lacked integrity in not conforming to ethical practice, but that is not the subject of the scenario. The correct owner also possessed the software even though copies of it were deceptively represented as having come from the popular publisher. Although the distributor



would have attempted to keep the popular and the obscure publishers from knowing what had been done with the software, confidentiality of the content of the program was not at issue.

The severity of authenticity loss can take several forms ranging from no conformance to genuineness or to fact or reality with no recovery possible. Or authenticity loss can be moderately false or deceptive with delayed recovery at moderate cost, or information can be mostly factual.

**Loss Scenario V: Confidentiality** (Known only to one or a limited few)

An individual inserted a radio transmitter into an ATM that received signals from the touch-screen CRT used for inputting customers' PINs and conveying account balances. The device then broadcast the information to a receiver that recorded the PINs and account balances on a VCR for retrieval. The thief in this case was convicted and sent to Leavenworth Prison for 10 years for stealing several million dollars. The security of PINs and account balances in ATMs is surely an important information security concern.

The secrecy of the customers' PINs and account balances was violated. Hence, at the very least their privacy was invaded.

Availability, utility, integrity, and authenticity are unaffected in the confidentiality violation. The customers' and the bank's exclusive possession of the account balances was lost but not possession per se because they still held and owned the information.

The severity of loss of confidentiality could vary. The loss in the worst circumstance would be disclosure to the most harmful party with permanent effect. It could also be known to several moderately harmful parties with a moderate-term effect or be known to one harmless, unauthorized party with short-term effect.

**Loss Scenario VI: Possession** (Having or owning and controlling)

A gang of burglars aided by the disgruntled and recently fired operations supervisor broke into a computer center and stole all copies of a company's master files on tapes and disks. They also raided the backup facility and stole all backup copies of the files. They held the materials for ransom in an extortion attempt in this famous computer crime that occurred in Europe in the 1970s. It was an important physical security computer crime. Three defendants were convicted. Such loss of possession is certainly a serious information security concern.

The burglary resulted in the lost possession of all copies but not loss of legal ownership of the master files and media on which they were stored. Loss of ownership would be accomplished if the materials were never returned and the victims were to stop trying to recover them.

Availability is delayed in this scenario but could be accomplished by paying the ransom or using legal force to recover the materials. Utility, integrity, and authenticity are not an issue. Confidentiality would not be violated unless the files were read or disclosed, and they were not in this case.

The severity of loss of possession varies with the nature of the offense. In a worst case scenario, the most harmful party would take the information along with any and all copies with no recovery possible. Or a moderately harmful party could take it for a moderate period of time before it would be recovered at moderate cost. In the least harmful case, a harmless party would possess one copy of the information with timely recovery possible.

## USE OF ELEMENTS TO IDENTIFY AND SELECT CONTROLS

A collection of controls for each of the six elements is presented below. The controls have been drawn from a number of sources based on the scenarios given and on the definitions of elements presented in the appendix. In a real information security analysis, some of these controls might not be identified were all of the elements and threats not considered. Therefore, using all six of the elements for conducting threat and vulnerability analysis with the list of threats provided above and for selecting controls as indicated here can help in achieving more complete and comprehensive information security. I did not attempt to identify specific threats with controls because it was beyond the scope of this paper.

Several controls are used to preserve or restore availability of data files in computers. These controls include having: a backup directory with erased file names and pointers until the files are purged by overwriting with new files, good backup practices, good access controls to computers and specific data files, use of more than one name to identify and find a file, utility programs available to search for files by their content, and shadow or mirror file storage.

To preserve utility of information, four controls are suggested. These include internal application controls such as verification of data before and after transactions, security walk-throughs during application development to avoid the appearance of unresponsive forms of information at times and places of use, minimization of adverse effects of security on information use, and control of access that may allow unauthorized persons to reduce the usefulness of information.

Several controls can be used to prevent loss of integrity of information. These controls include using and checking sequence numbers and check sums or hash totals for series of ordered items to ensure completeness and wholeness; doing reasonableness checks on types of information in designated fields; performing manual and automatic text checks on presence of records, subprograms, paragraphs, or titles; checking for unexecutable code and mismatched conditional transfers in computer programs.

A number of controls can be applied to ensure authenticity of information. These include confirming account balances, transactions, correct names, deliveries, and addresses; checking on genuineness of products; segregating duties or dual performance of activities; using double entry bookkeeping; checking for out-of-range values; and using passwords, digital signatures, and tokens to authenticate users at workstations and LAN servers.

Controls to maintain confidentiality include using cryptography, training employees to resist deceptive social engineering attacks to obtain their technical knowledge, physically controlling location and movement of mobile computers and disks, and controlling access to computers and networks. Security also requires ensuring that resources for protection should not exceed the value of what may be lost especially with low incidence. For example, protection against radio frequency emanations in ATMs (such as in the confidentiality scenario described above) may not be advisable in a particular situation considering the cost of shielding and access control, the paucity of such high-tech attacks, and the limited monetary losses possible.

Several controls should be used to protect the possession of information. These include using copyright, patent, and trade secret laws; implementing physical and logical access limitation methods; preserving and examining computer audit logs for evidence of stealing; using file labels; inventorying tangible and intangible assets; etching identification on computer equipment; using distinctive colors and labels on disk jackets; and assigning ownership to organizational information assets.

## CONCLUSION

Some scenarios of losses that information security should address require all six elements of preservation to be used to specify the security to be applied. The six elements are independent of one another, however, as demonstrated in the scenarios presented here and by having unique definitions. The one exception occurs when the only possible definition of an element is included within the definition of another element; for example, when loss of confidentiality results from loss of possession. A violation of confidentiality always causes a violation of loss of exclusive possession as well. Loss of exclusive or nonexclusive possession, however, does not necessarily result in loss of confidentiality, as seen in the above scenario of stealing information without examining it or when the information stolen is not confidential.

All six elements of information security presented here must be used. This is essential if information security is to be complete and accurately described. Moreover, to adequately reduce or eliminate vulnerabilities and threats, the use of all six elements is critical to ensure in applying appropriate controls, such as those identified above, that nothing is overlooked. These elements also aid in identifying abusive actions that adversaries could take before the actions are experienced. As technology advances, adversaries become more sophisticated, or the concept and scope of information security changes, more changes or additions to the six elements may be required.

All six elements can be paired into three double elements for simplification and ease of reference, and the order of presentation should have some meaning as well. Availability and utility fit together as a double element to preserve the usability and usefulness of information. Controls applicable to both of them include secure location, appropriate form for secure use, and accessibility of backup copies.

Integrity and authenticity fit together where the loss comes from change of information or change of reality. One is concerned with internal structure and the other with value conformance with external facts or reality. Controls for both include double entry, reasonableness checks, use of sequence numbers and check sums or hash totals, and comparison testing. Control of change applies to both.

Finally, confidentiality and possession go together in that they are only partially independent as previously stated. Commonly applied controls include copyright protection, cryptography, digital signatures, escrow, and secure storage.

The order of the three sets used here also is a logical priority. The second pair, integrity and authenticity, generally have value only if the information is available and useful. The third pair, confidentiality and possession, have sufficient meaning only if the value of the information is sufficient because it has integrity and authenticity.

All other candidate elements that I have thought of, such as quality, auditability, timeliness, reporting, collection, creation, and others, are definitionally subsumed by the six selected elements, or I considered them outside the scope of information security. Preserving the quality of information is done by quality engineers, auditability is a control and is done by auditors, timeliness is subsumed by utility and availability, and the last three are functions of information processing that are to be made secure by applying the six elements. Suggestions of any other candidate elements from readers of this paper are welcome.

## REFERENCES

- [1.] Donn B. Parker. "Restating the Foundation of Information Security," *Proceedings of the 14th National Computer Security Conference 1991*.
- [2.] Donn B. Parker. "A Simple Comprehensive Threats List for Information Security," *Auerbach Journal of Information Systems Security*, Summer 1993.
- [3.] Peter G. Neumann. "Rainbows and Arrows: How Security Criteria Address Computer Misuse," *Proceedings of the 13th National Computer Security Conference 1990*.

## APPENDIX: DEFINITIONS OF SECURITY ELEMENTS

The following definitions are the relevant abstractions taken from *Webster's Third New International Dictionary*.

**Security:** Freedom from danger, fear, anxiety, care, uncertainty, doubt; basis for confidence; measures taken to ensure against surprise attack, espionage, observation, sabotage; protection against economic vicissitudes (old age guarantees); penal custody; resistance of a cryptogram to cryptanalysis usually measured by the time and effort needed to solve it.

**Availability:** Capable of use for the accomplishment of a purpose, immediately utilizable, accessible, may be obtained.

**Utility:** Useful, fitness for some purpose, capacity to satisfy human wants or desires.

**Integrity:** Unimpaired or unmarred condition; soundness; adherence to a code of moral, artistic, or other values; the quality or state of being complete or undivided; material wholeness.

**Authenticity:** Quality of being authoritative, valid, true, real, genuine, worthy of acceptance or belief by reason of conformity to fact and reality.

**Confidentiality:** Quality or state of being private or secret; known only to a limited few.

**Possession:** Act or condition of having in or taking into one's control or holding at one's disposal; actual physical control of property by one who holds for himself, as distinguished from custody; something owned or controlled.

The following formal definitions are offered for the six elements of information security applied to information.

**Availability:** Immediately usable, capable or accessible for use, or may be obtained for use.

**Utility:** Useful for a purpose.

**Integrity:** Complete, whole, and in readable condition.

**Authenticity:** Conforms to fact and reality, valid, true, real, and genuine for a purpose.

**Confidentiality:** Known only to one or a limited few.

**Possession:** Having or owning and controlling.

# The Aerospace Risk Evaluation System (ARiES): Implementation of a Quantitative Risk Analysis Methodology for Critical Systems

Charles H. Lavine, Anne M. Lindell, and Sergio B. Guarro  
The Aerospace Corporation  
2350 E. El Segundo Boulevard, El Segundo, CA 90245-4691

## ABSTRACT

In recent years, quantitative risk analysis has been employed as an effective security review technique applicable to a wide range of systems security tasks. A number of standards and regulations applicable across a broad range of systems require that risk analyses be performed. However, these documents only provide broad guidelines for risk analysis. The Livermore Risk Analysis Methodology (LRAM) was developed to provide users with a detailed description of specific steps to perform risk analyses on a variety of systems. This methodology was recently enhanced and automated in the Aerospace Risk Evaluation System (ARiES). ARiES is a concise engineering tool that directly and clearly relates the results to the information input by the user. Its risk model structure is designed to permit the systematic identification and evaluation of information systems assets, potential threats to these assets, possible consequences that may result from the impact of threats on assets, and risk reduction benefits that may be obtained by selecting and applying certain preventive and mitigative controls. This paper discusses the enhanced LRAM methodology and the ARiES implementation.

## 1. INTRODUCTION

The commercial and government sectors of the U.S. economy are increasingly relying on information, data processing, and computer systems, so that the security of these systems is becoming an area of increasing importance. As a result, the field of information systems risk management has expanded to address the various areas of security concern. In recent years, quantitative risk analysis has been employed as an ef-

fective security review technique applicable to a wide range of systems security tasks.

Quantitative risk analysis is distinct from qualitative risk analysis in that it employs specific parameters whose definition is objective and not dependent on context, although the quantification process may require subjective estimates. Quantitative risk analysis provides a framework with which analysts may justify systems security expenditures, determine the magnitude of systems security risk, and evaluate the relative attractiveness of measures to control that risk.

A number of standards and regulations, applicable across a broad range of systems (e.g., Air Force Regulation 205-16 [AF205], National Bureau of Standards and Office of Management and Budget documents [OMB]), require that risk analyses be performed on a regular basis, with recommendations and requirements concerning the execution of risk analyses. These documents do not specify the exact steps to be performed; they are only meant to provide broad guidelines for risk analysis. The Livermore Risk Assessment Methodology (LRAM) was developed by Sergio Guarro with the intent of providing users with a detailed description of specific steps to be executed. [LRAM] More recently, Charles Lavine and Anne Lindell, with assistance from Dr. Guarro, enhanced and automated the methodology in a tool known as the Aerospace Risk Evaluation System, referred to as ARiES.

ARiES is a concise engineering tool that directly and clearly relates the results of the analysis to the information input by the user. Its risk model structure is designed to permit the systematic identification and evaluation of information systems assets, potential threats to these assets, possible consequences that

may result from the impact of threats on assets, and risk reduction benefits that may be obtained by selecting and applying certain preventive and mitigative controls.

## 2. ARiES METHODOLOGY OVERVIEW

In overall terms, quantitative risk analysis involves the estimation of risk, given as the occurrence of undesired consequences (losses) per unit time. Undesired consequences are defined by the scope of the analysis. The consequences for an information system may include the loss of the ability of the system or fa-

frequency of occurrence. [DENN] The analysis of controls entails the determination of the probability of their failure and whether additional controls or modifications are cost-effective.

The combination of a threat initiator, its propagation path (i.e., the way in which the threat is carried through), the asset, the consequence and the control's effectiveness is defined as a *risk element* (RE). The logical summation over all risk elements gives the total risk to the facility, system or subsystem being analyzed.

Fig. 1 shows the essential components of the LRAM risk model in both diagrammatic and quanti-

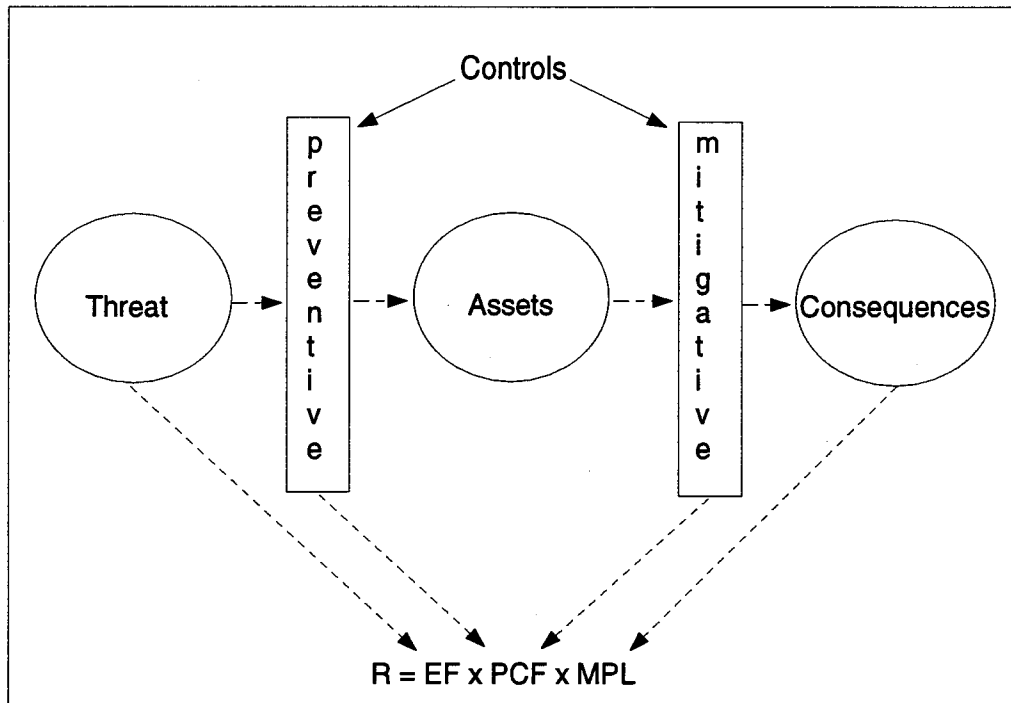


Fig. 1. Basic risk analysis model used by ARiES

cility to fulfill its mission, disclosure; deletion or alteration of important information; denial of service; and any undesired effects on the organization operating the facility. Consequences are examined and quantified with respect to system assets, including hardware, software, information, and personnel.

To determine the occurrence of consequences, threats that may have a direct adverse effect on system assets must be identified and the effectiveness of controls that prevent and/or mitigate these consequences must be analyzed. Threats (which are composed of an initiator and its path to the asset) are quantified using historical data and/or subjective judgement on their

tative representation terms. The diagrammatic part shows the logical relations between the threat initiator (e.g., a human attacker, such as a saboteur, or a natural agent, such as an earthquake), the potential target assets (e.g., computer and communication hardware, software, or data), and the consequences that could result if the threat agent reaches the assets (e.g., destruction of hardware, software, or data). The security controls are supposed to inhibit the progression of the threat initiator on this path: *preventive controls* (e.g., computer guard system, armed guard) are placed on the path from threat to assets and have the intended function of preventing the threat agent

from affecting the assets in any significant way; *mitigative controls* (e.g., fire extinguisher, system backups) are, on the other hand, positioned along the path from asset to consequences, and have the intended purpose of limiting and minimizing losses in those cases in which the preventive controls fail to keep the threat from affecting the assets. Fig. 2 contains an example of a risk element.

The qualitative model just described can be quan-

the threat and failure of all applicable controls. The PCF is the equivalent fraction of times the integrated control set will allow a loss equal to the MPL out of all the times that the threat it was intended to prevent or mitigate will occur.

Note that LRAM does not require or use a total risk measure, but rather focuses on the risk from single occurrence losses. In LRAM, sorting and screening of certain constituent parts of the RE and certain com-

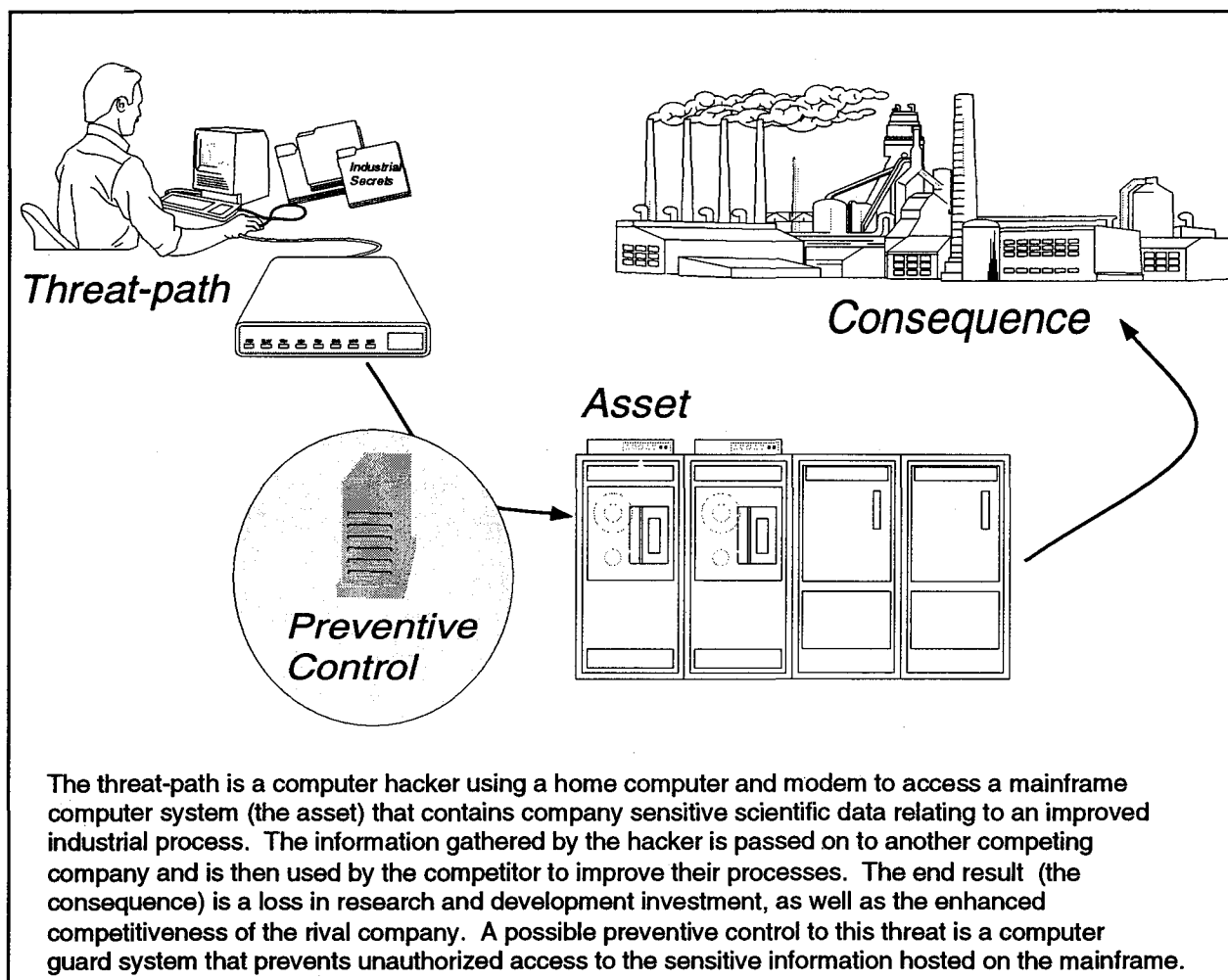


Fig. 2. Risk Element Example

tified using the formula shown in the lower portion of Fig. 1. The formula indicates that an annualized measure of the *risk* (R) resulting from any given RE can be calculated as the product of the *maximum potential loss* (MPL), the *probability of control failure* (PCF) of the combined sets of preventive and mitigative controls, and the annualized *expected frequency* (EF) of the threat. The MPL is the expected loss value of the RE for a given asset, assuming a single occurrence of

binations of the constituent parts is performed to focus the analysis on those REs of highest importance, i.e., having the highest risk. This feature is discussed further in the next section.

Assets can be sorted into those having only monetary value and those that are critical, sensitive and/or classified. Assets with monetary value are screened at a "materiality level" (It is also possible to screen assets based on their non-monetary attributes). Those

assets whose monetary value exceeds the materiality level are retained in the analysis.

For the assets remaining in the analysis, the assets are paired with applicable consequences and the possible applicable threats and their paths are identified to establish an RE. This form of an RE assumes that the threat has occurred and the controls have failed in order to estimate the MPL for the RE. REs are then screened out if their MPL value is below a threshold established by management.

For each of the remaining REs, the applicable current controls are identified and their failure probability estimated. The MPL is then combined with the PCF to establish a *loss potential indicator* (LPI) for each RE. The LPI represents risk in the form of the loss one can expect to incur once a threat against an asset has actually materialized.

$$\text{LPI [risk element]} = \text{PCF [controls]} \times \text{MPL[consequences]}$$

The REs are then screened for risk acceptability. Those REs with an LPI less than a user defined threshold are eliminated from further consideration. The unacceptable REs (those with LPI equal to or greater than the threshold) require that new controls or control

upgrades be proposed and new LPI values determined. The new LPI is subjected to the same screen as the original LPI. If the LPI is found acceptable, the analysis proceeds to the cost-benefit analysis. If not, an iterative procedure is necessary until new controls or control upgrades are identified that will produce an acceptable LPI value for the RE or it is determined that no controls are available that can render a particular RE acceptable.

A cost-benefit analysis is then performed on the new controls or control upgrades. This analysis requires an estimate of the incremental cost of implementing the new or upgrade control(s) beyond the cost of the current controls, and an estimate of the reduction in risk associated with each RE due to the new or upgraded controls as compared to the current controls. A cost-benefit ratio (CBR) is developed by dividing the reduction in risk by the incremental cost for the new or upgraded controls.

$$\text{CBR} = \frac{\text{Reduction in risk}}{\text{Incremental cost of control}}$$

This ratio is then compared to a user defined threshold value to determine if the new or upgraded

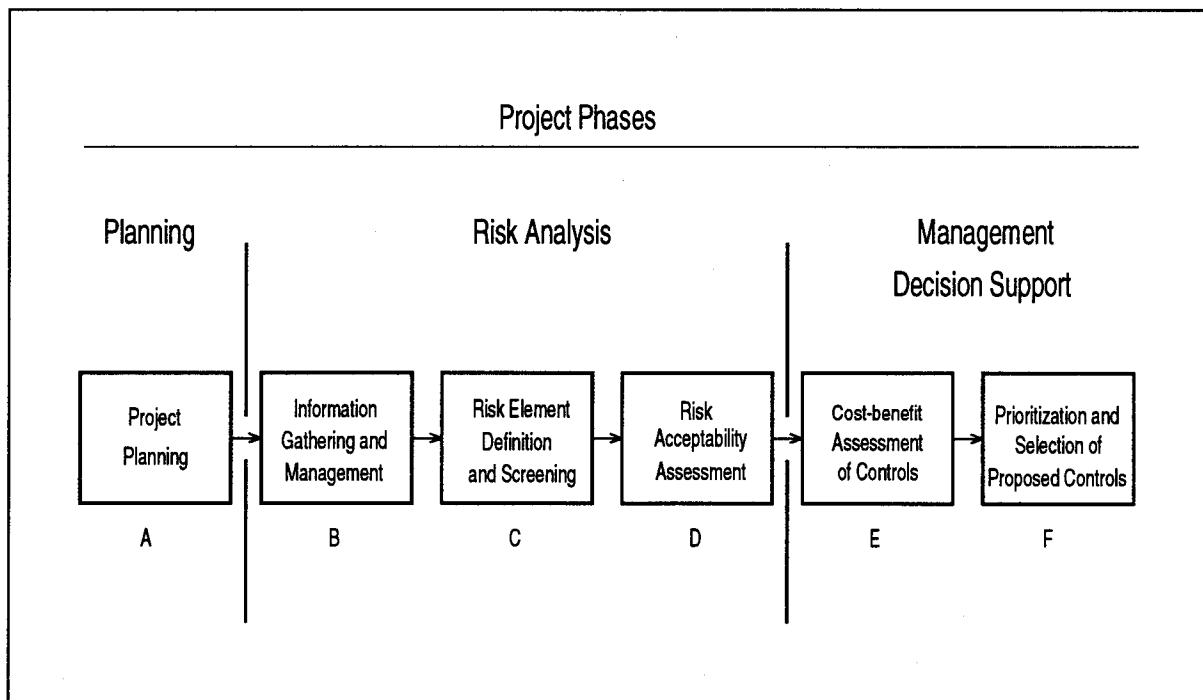


Fig 3. Risk Analysis steps used by ARiES.



controls are acceptable. If they are not, different new or upgraded controls are proposed and the process of LPI acceptability and cost-benefit analysis is repeated.

The new or upgraded controls that have an acceptable CBR are prioritized, selected and budgeted for installation. The prioritization process considers several weighting factors chosen by the organization operating the facility in order to select and budget those new or upgraded controls that will fulfill their security concerns.

### 3. ARiES IMPLEMENTATION

The Livermore Risk Analysis Method (LRAM) which ARiES implements is divided into the following six stages:

- A. Project Planning
- B. Information Gathering and Management Input
- C. Risk Element Definition and Screening
- D. Risk Acceptability Assessment
- E. Cost-benefit Assessment of Proposed Control Sets
- F. Prioritization and Selection of Proposed Control Sets

The six stages are combined into three phases as shown in Fig. 3. A discussion of how each of the stages is implemented through ARiES is presented below.

#### *A. Project Planning*

The Project Planning stage is required to define the scope of the analysis, identify resources and personnel commitments, organize execution of the following stages, and define personnel and management interfaces needed in the execution itself. The results from this stage is used as input to the modeling process in ARiES.

#### *B. Information Gathering and Management Input*

The information gathering stage encompasses the collection of information that will be required in sub-

sequent phases of the risk analysis. It can be thought of as the activity that initiates the risk analysis. Some of the information gathering steps are performed upfront, i.e., before any of the modeling and associated activities are initiated, while others are more effectively performed in the risk analysis activities with which they can be directly associated. An example of this is the collection of threat frequency data (an information gathering type of activity) which can be chronologically associated with the steps forming the cost-benefit assessment stage of the risk analysis when risk is determined using the threat frequency data. From the practical point of view, it is very important to delay this particular type of data collection until the cost-benefit assessment stage, since at that stage there will be a smaller set of threats than that initially identified for which threat frequency data has to be collected.

The first information gathering activity in an ARiES analysis involves specifying the list of assets that should be included in the analysis. As stated earlier, importance of an asset is based on the monetary value of the asset as well as the non-monetary aspects (i.e., criticality, sensitivity, and classification) of the asset. ARiES allows the user to define, modify, and review the levels of priority associated with the non-monetary aspects. Once these levels have been defined, they can be applied to any defined asset.

ARiES displays assets currently included in the analysis and their relationship to each other by use of a hierarchical, graphical diagram, called an asset tree, as shown in Fig. 4. This tree provides a method to quickly obtain information on any of the assets defined for the analysis. The root of the tree is the parent to which all other assets are related. Through the asset tree, it is possible to modify existing assets or add new ones. The assets can be arranged in the asset tree to any arbitrary depth. When a new asset is added, a sub-window is provided to name the asset, provide a description of the asset, state the direct loss value of the asset, and associate a classification, criticality, and sensitivity level with the asset. It is also possible to specify whether an asset is to be carried through the analysis without being screened out by marking it as a Pet.

After defining the assets to be included in the analysis, ARiES allows the user to define a loss value (materiality) threshold, and classification, criticality, and sensitivity (non-monetary) thresholds against which the assets are to be screened for importance. Assets with materiality values and non-monetary at-

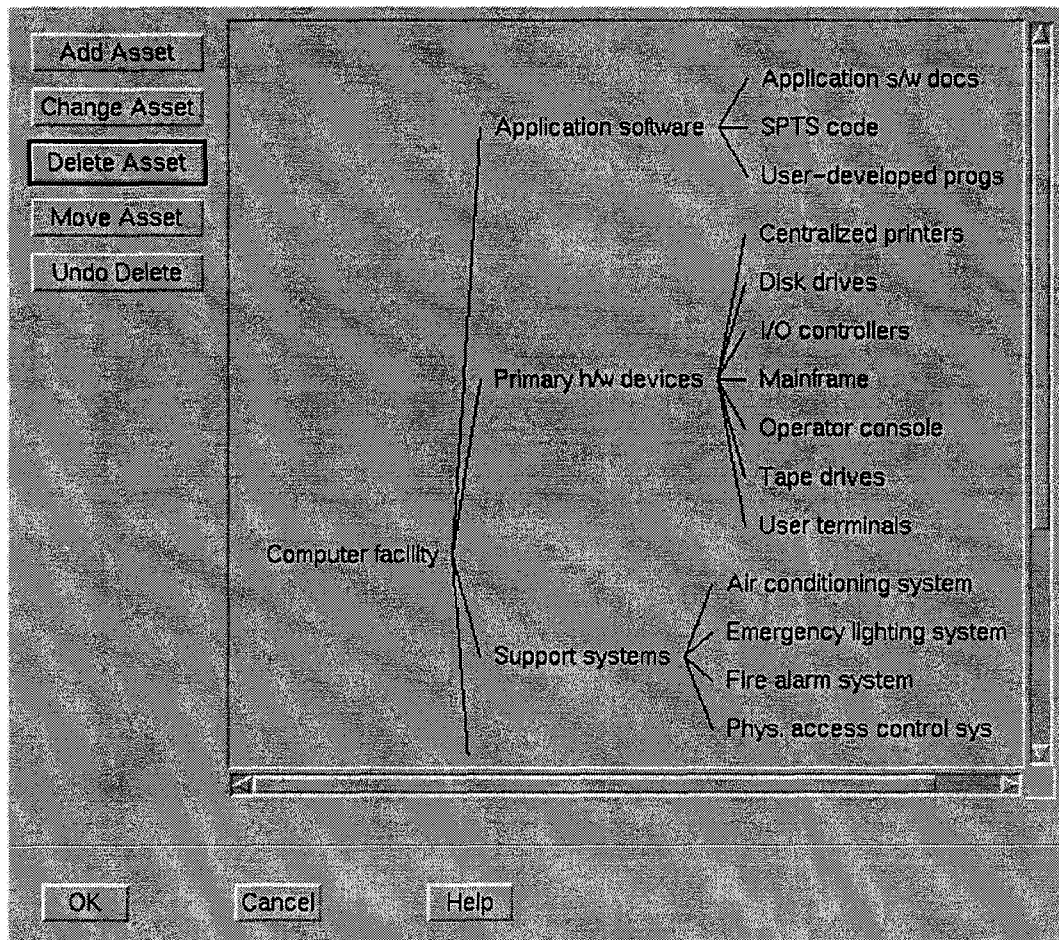


Fig. 4. Asset Tree

tributes less than the user defined thresholds will be removed from further consideration for the remainder of the analysis unless the asset is a Pet. ARiES also allows the user to review the results of screening in real time or through a generated report. It should be noted that it is not essential or necessary to perform this screening, especially if the user does not feel that the screening process is needed or desired. Alternatively, high thresholds can be selected to screen out all but the most important assets.

### C. Risk Element Definition and Screening

The definition and screening stage includes those steps in the analysis in which: a) REs are identified by establishing the correspondence of their threat, asset, and consequence components, and b) these REs are screened out of the analysis according to iterative

evaluation of the importance of their components.

As Fig. 5 shows, the REs available at the end of this phase of the analysis will consist of a combination of specific threats, their propagation paths, affected assets, and the resulting consequences that might occur if the asset is lost or compromised. Threats are defined first through a separate window and can be placed within four generic threat classes (i.e, human intentional, human unintentional, environmental natural, and environmental fabricated). Consequences are also defined through another window and have a monetary value associated with them. At this point, it is likely that all the REs defined thus far will have unacceptable consequences. This is because the security controls that are employed to prevent or mitigate the consequences are not considered until the next stage of the analysis. It is also possible to specify whether a RE is to be carried through the analysis without being screened out.

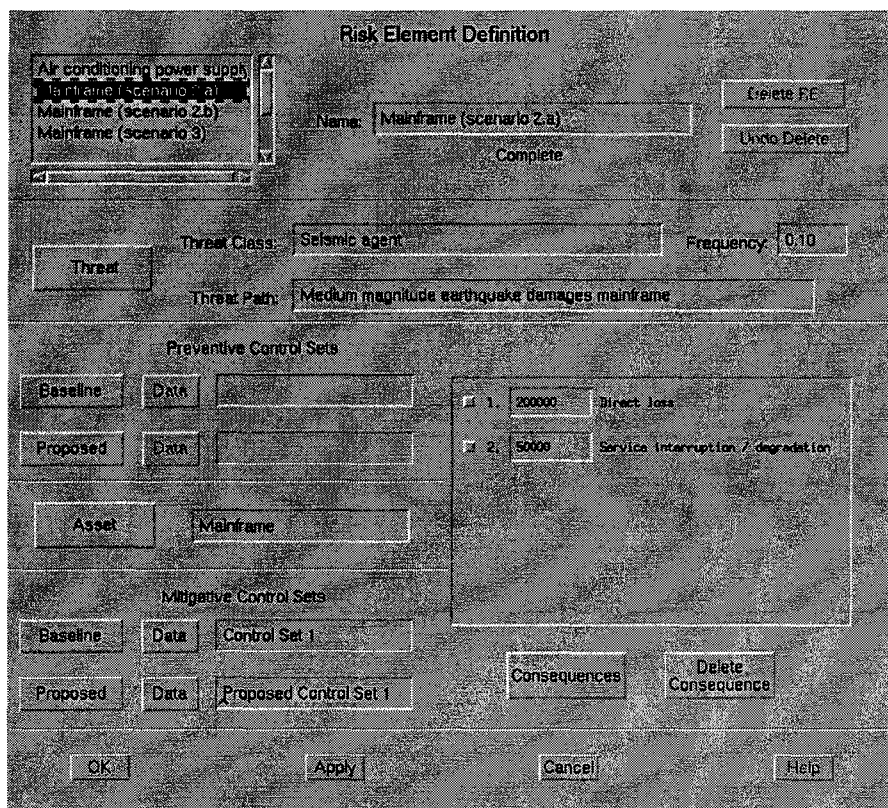


Fig. 5. Risk Element Definition Window

After defining the REs to be included in the analysis, ARiES allows the user to define a MPL level against which the REs are to be screened. ARiES calculates an MPL value for each RE and removes REs with MPLs less than or equal to the defined threshold from further consideration for the remainder of the analysis, unless the RE is a Pet. As before, ARiES allows the user to review the results of screening in real time or through a generated report. The screening process is not essential, but it does provide a way to minimize the amount of data and modeling to be carried into the later stages of the risk analysis. Even though it may appear to make the risk analysis process unnecessarily complicated, this actually saves a significant amount of tedious assessment and quantification work in later stages.

#### D. Risk Acceptability Assessment

The acceptability assessment stage serves the purpose of formally identifying those REs, among all the significant ones carried through in the RE definition stage, which pose or contribute an unacceptable risk

to the operation of an ADP system and/or facility. Acceptability or unacceptability of the risk posed by an individual RE is determined by the comparison of a quantitatively defined risk parameter with a predetermined "acceptability threshold."

ARiES provides the facilities to make an assessment of the acceptability of the REs still under consideration based on the following inputs: (1) the previously defined REs with MPL values above the materiality threshold; (2) information concerning the currently employed controls; (3) data on control failure probability; and, (4) management input concerning the acceptable level of risk used to screen the REs for risk acceptability.

Facilities to define, review and alter current controls and to associate controls with specific REs are also provided by ARiES. For each control, a description, installation cost, annual operating cost, and useful lifetime associated with this control are specified. As shown in Fig. 6, a graphic-oriented editor is provided to graphically combine controls into the control sets (both preventive and mitigative) associated with each RE.

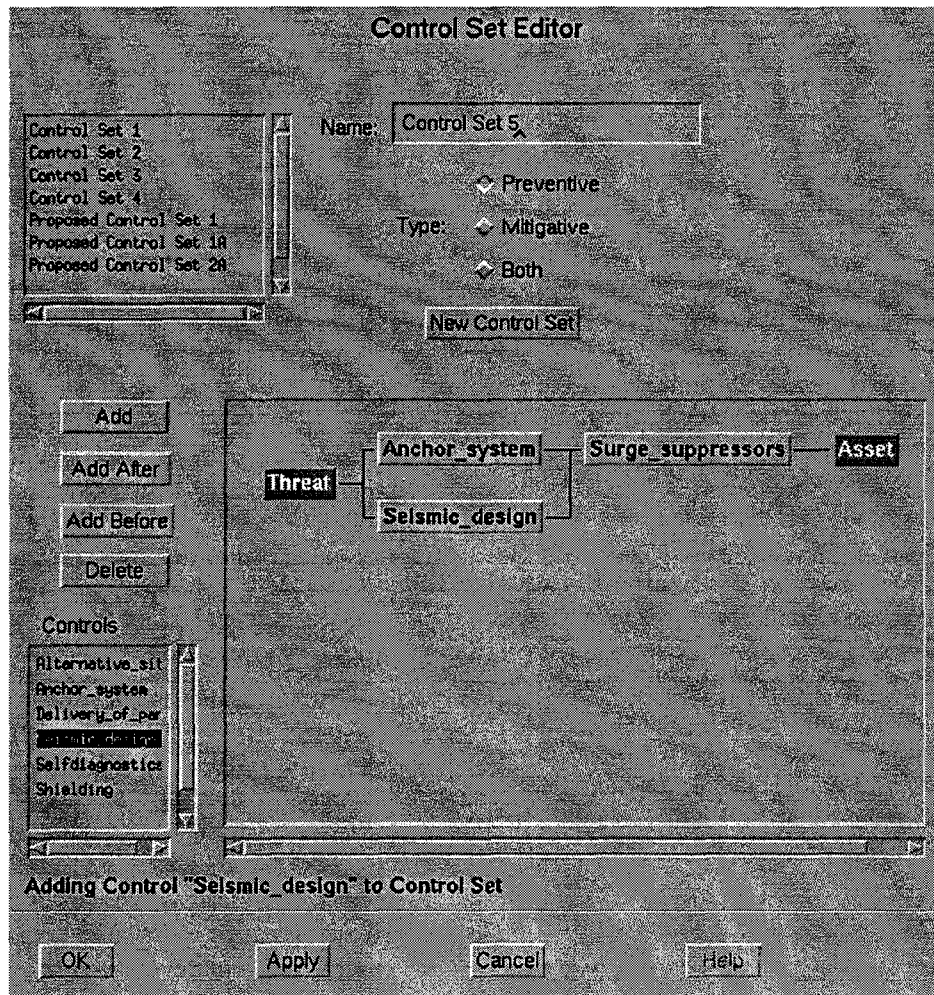


Fig. 6. Control Set Editor Window

After the appropriate control sets have been associated with an RE, an LPI value (i.e., the quantitatively defined risk parameter) is calculated by ARiES for each RE. The user can define an acceptable LPI value (which is the acceptability threshold) against which REs are to be screened. Those REs with acceptable LPI values are removed from further consideration. If after incorporating currently employed controls an RE is found to have an unacceptable LPI value, new controls or control upgrades can be proposed. Proposed controls are defined and associated with REs in the same manner as current controls. In fact, the current control set is used for the initial proposed control set.

Proposed controls are selected to augment the current controls to reduce the LPI values. Proposed controls can come from the existing list of controls or from new controls that are added to the control list. ARiES supports repetition of the acceptability assess-

ment process until either (a) the new controls render all risk elements acceptable or (b) the unacceptable REs are thoroughly examined and it has been determined that no new control would be acceptable. The risk acceptability assessment concludes the risk assessment phase of the risk analysis and provides the necessary input for the following decision support phase.

#### *E. Cost-Benefit Assessment of Proposed Control Sets*

Cost-benefit assessment opens the management decision support phase of the risk analysis. In this stage, control sets which have been identified to eliminate or reduce undue risk, and which have been already evaluated and accepted from the risk acceptability point of view, are also evaluated to determine the cost-effectiveness of their procurement, installa-

tion and implementation.

ARiES provides the facilities for calculating and evaluating the cost-benefit (in the form of a CBR) of the proposed control sets. These controls are those identified in the previous stage of the risk analysis as being able to provide acceptable risk. Only those proposed control sets that have been shown to provide adequate security will be subjected to a cost-benefit evaluation.

ARiES determines the minimum benefits from the proposed control sets by using the LPI value calculated with the current controls and the proposed LPI value calculated with the implementation of the proposed control set. Threat frequency is calculated into a yearly benefit determination. Dividing by the annual cost of the proposed control sets, a CBR is determined which can be compared to a threshold chosen by the user. The threshold chosen is usually one; however, if special considerations justify acceptance of costs in excess of expected benefits, or demand achievement of benefits in excess of costs, the threshold chosen may be smaller or greater than one. The acceptable proposed control sets are sorted based upon a calculated index value. This index may be used in association with the other decision support indices described below in the prioritization and selection stage.

#### *F. Prioritization and Selection of Proposed Control Sets*

This stage concludes the management decision support phase and the risk analysis process itself. Its purpose is to prioritize proposed control sets according to a rational and integrated prioritization and selection scheme, accounting for important factors such as applicability of control sets to more than one significant threat, expected effective life of a proposed control set, and availability of funds. As a result, proposed control sets can be listed in order of identified priority for implementation and selected accordingly. This stage is designed to be integrated and applied in coordination with the yearly budget allocation process and constitutes a useful and practical tool for the managers that have responsibility for budget preparation and planning.

ARiES supports this stage by providing options for prioritizing controls that were determined to have an acceptable cost-benefit ratio according to four indices: cost-benefit index (CBI); net benefit index (NBI); expected useful life index (ULI); and global prioritization index (GPI). When the prioritization index is selected, ARiES will calculate the selected prioritiza-

tion index value for each proposed control set and rank them by index value and scheme.

#### 4. CONCLUSION

ARiES is an automated version of the Livermore Risk Analysis Methodology. It is a quantitative tool specifically designed for the information systems security decision-maker, but, owing to the versatility of its algorithms, it could be applied to most system models for security or safety analysis. Some examples of areas that ARiES can be employed in include: (a) systems design efforts to ensure that appropriate controls are built in; (b) systems upgrades efforts to make sure that retrofitted controls are appropriate; (c) systems security standards definition efforts to make sure the standards are justified; (d) control change budgeting efforts to ensure that monies are spent where they are needed the most; and/or (e) security- or audit-review planning to allocate staff resources in the most cost-effective manner.

ARiES facilitates easy collation of data from different data files. The data files generated by ARiES are in ASCII form and are readable, making quick review of data possible. This design allows multiple data files to be combined into one analysis; thereby giving users the option of performing risk analyses separately. This feature is especially useful in highly distributed systems at multiple sites. Additionally, the ability to maintain versions of data files makes the configuration management of on-going risk analyses easy to perform; enabling users to compare multiple data sets from several system configurations.

Users are not required to perform the risk analysis methodology in the recommended sequential steps. Experienced users may want to deviate from the sequences and/or use the tool in a limited way to obtain specific data. Users are allowed to define all data that is used in the various calculations and screenings. Once the data is defined, it is easily modified, thereby making it easy to try out different scenarios.

#### *Future Plans for ARiES*

ARiES was developed and hosted on Sun-compatible file servers and workstations running the UNIX operating system. The software package used for developing the graphical user interface was TeleUse, which runs under the Motif window manager and generates C code output. We are looking into hosting ARiES on other platforms.

Other future plans for ARiES include the incorporation of Bayesian techniques [BAYES] into the calculations and work to determine the appropriateness of the tool for safety applications.

## 5. BIBLIOGRAPHY

[AF205] Air Force Regulation 205-16, Computer Security Policy, Department of the Air Force, Headquarters US Air Force, Washington DC 20330-5000, April 28, 1989.

[Denn] Dennison, Mark W.L., and Toth, Kalman C., "Practical Models For Threat/Risk Analysis," 14th National Computer Security Conference, Washington, D.C., October 1-4, 1991.

[LRAM] Guarro, Sergio B., "Risk Analysis and Risk Management Models for Information Systems Security Applications, Reliability Engineering and System Safety," 25 (1989) 109-130.

[NIST] NIST Special Publication 500-174. Guide for Selecting Automated Risk Analysis Tools. October 1989.

[OMB] Office of Management and Budget Circular A-130, Dec. 12, 1985.

[BAYES] Lewis, Nina, "Computer Security Analysis: Bayesian Updates of Expert Opinion, Intrusion Detection Workshop," SRI, Menlo Park, CA, May 10-11, 1990.

# THE SECURITY-SPECIFIC EIGHT STAGE RISK ASSESSMENT METHODOLOGY

David L. Drake (drake@mls.saic.com)  
Katherine L. Morse (morse@mls.saic.com)  
Science Applications International Corporation  
10770 Wateridge Circle  
San Diego, CA 92121  
© 1994 SAIC

## ABSTRACT

Existing security risk assessment methodologies have three major flaws: they rely on the assessor to formulate the chain of events that describe each of its threat scenarios, their models cause a combinatorial explosion of calculations due to analysis of the effectiveness of each countermeasure against each threat/vulnerability pair, and they do not spotlight the specific area of improvement needed when threat scenarios are deemed too high risk. This paper presents an eight stage model that is specifically for security threat scenarios, which will directly address these three flaws. The eight stage model is designed to be incorporated into existing risk assessment methodologies at the point where the assessor is to identify threats and analyze the effectiveness of existing countermeasures. By making a distinction between the time a threat occurs, the time a security breach occurs, and the time the harm of that breach occurs, it becomes clear where the countermeasures are in place to break this chain of events. By providing this generic chain of events, the assessor can reduce the number of scenarios analyzed down to one per threat/asset pair, and at the same time identify the specific type of countermeasures that are lacking.

## INTRODUCTION

Traditionally, risk assessment methodologies are based upon a simplistic model of risk which identifies threats and the vulnerabilities they exploit to affect a security breach. Countermeasures are identified which mitigate the threat/vulnerability pairs. Loss due to a security breach is calculated based on the probability of the threat overcoming the countermeasure and creating the breach. This traditional model is assumed to be complete in its ability to model all of the countermeasures and represent all of the loss. We have not found this to be the case. Threat/vulnerability pairs are all crossed with the countermeasures and the assessor must decide which countermeasures are effective against which threat/vulnerability pairs. While this model is conceptually simple, understanding and implementing it is tedious and counter-intuitive. This paper presents a new security risk assessment methodology which addresses these issues.

The eight-stage security risk assessment methodology offers three improvements over traditional security risk assessment methodologies. First, it provides a more intuitive model of an entire security breach as a chain of events. This is particularly true when a threat that is not deterred leads to an actual security breach, which are subsequently followed by additional events that lead to eventual harm to the

overall system mission. Second, it identifies stages at which countermeasures can detect threats and their resultant security breaches and mitigates them rather than assuming wholesale loss. Finally, the methodology eliminates the combinatorial explosion of crossing all threat/vulnerability pairs with all countermeasures. The model takes advantage of the fact that security countermeasures are specifically designed and implemented to address particular threat scenarios. This permits the assessor to focus on a small number of countermeasures per threat scenarios, rather than analyzing the strength of each countermeasure against all possible threat/vulnerability pairs.

This risk assessment methodology was developed under contract F33657-93-C-2114 for the Air Force Aeronautical Systems Center.

## 1. BACKGROUND

"Risk assessment is a well-developed science that has been successfully applied to fields other than security." [1] In this reference Osgood presents a very complete history of risk assessment in the computer security arena along with its deficiencies. Improvements in risk assessment have been developed by Jaworski [2], and Smith and Jalbert [3]. Jaworski has developed a tandem threat scenario methodology that extends the traditional risk assessment methodology by analyzing the perpetration of successions of threats at multiple vulnerability points. The Los Alamos Vulnerability/Risk Assessment (LAVA) system developed by Smith and Jalbert automates a mathematical model based on classical risk assessment, hierarchical multi-level system theory, decision theory, fuzzy possibility theory, expert system theory, utility theory, and cognitive science. The eight stage model can be incorporated into an existing risk assessment methodology, e.g. as the initial two steps of Tandem Threat Scenarios in which the assessor identifies threats, and identifies and analyzes the effectiveness of existing countermeasures.

## 2. METHODOLOGY

The methodology described in this paper is based on a risk assessment model that is specifically tailored for security. In this model, eight distinct stages are used to represent the activities that occur starting from the steps taken to prevent a threat to the system through to the resultant harm that can be caused, as shown in Figure 1, The Eight-Stage Model.

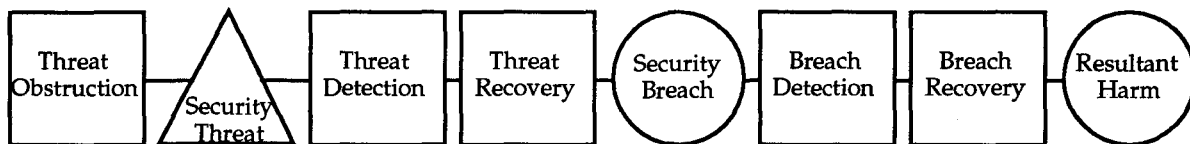


Figure 1. The Eight-Stage Model



## 2.1 The Eight-Stage Model

The driving principle of this model is that not all of the losses caused by a security breach occur at the time of the security breach itself, but most of the losses occur later when the consequences of the breach are enacted. A second principle is that the security mechanisms for a system have three opportunities to reduce the harm that could be caused by a threat: before the threat occurs, after the threat occurrence is detected but before a security breach occurs, and after a security breach occurs and is detected.

The model is designed to allow the assessor to list all of the threat scenarios that are of interest to the system at hand. Each threat scenario that could bring about harm will be a separate entry in this list. For each entry, an eight-stage model of the events is constructed. A risk analysis is calculated for each threat scenario, based on the probability of the occurrence of the threat and the effectiveness of the countermeasures. Expected losses are calculated based on the risk level and the associated potential losses.

When multiple opportunities for harm are possible for a particular threat scenario, as will often be the case in the tandem threat scenario methodology, each opportunity will have a separate entry in the list of threat scenarios, and its own eight-stage model of events.

The reader should note that the traditional listing of system vulnerabilities has been eliminated from the eight-stage model. This is because in security risk assessment, each system vulnerability can be linked directly to the lack of a countermeasure. By concentrating on the effectiveness of existing countermeasures, needless tracking of "potential vulnerabilities" is eliminated.

In Figure 1, the external influence to the system is depicted as a triangle, the internal influences are depicted as squares, and the consequences as circles. The hope of the system's security engineer is that the unwanted consequences of the security threat are prevented by the activities represented in the squares. The consequences, represented by circles, will occur if these activities are insufficient. Figure 2, A Physical Example of the Eight-Stage Model, is a classical physical security example to help illustrate each stage.

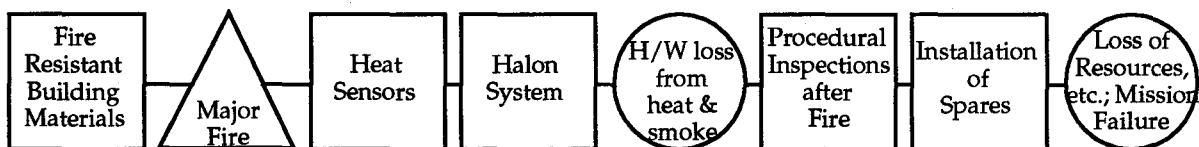


Figure 2. A Physical Example of the Eight-Stage Model

Figure 3, A COMPUSEC Example of the Eight-Stage Model, contains the simplified version of a Computer Security (COMPUSEC) example. The scenario is of a unauthorized user attempting to access a system by guessing a password and then reading classified material, thus compromising it.

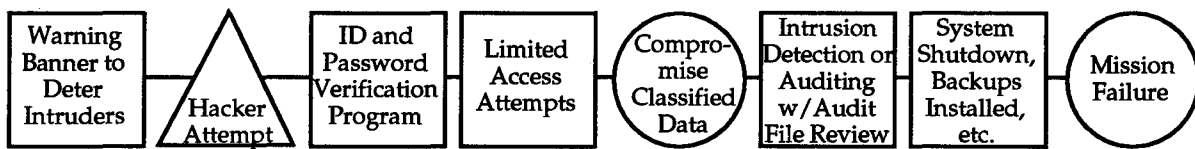


Figure 3. A COMPUSEC Example of the Eight-Stage Model

The eight stages of the model, with additional examples, are:

**Stage 1. The obstruction of a threat occurrence.** An attempt is made to prevent a security threat from even occurring. In this model, a clear distinction is made between the existence of a threat, which is omnipresent, and a threat occurrence. Example threat obstructers are building structures and guards to prevent unauthorized personnel from entering into a building.

**Stage 2. The occurrence of a threat.** The occurrence of a threat is initiated. Example threat occurrences are the start of a fire, the initiation of sabotage, and initiation of an attack by a disgruntled employee. The occurrence of a threat does not imply that damage or harm to the system has occurred, only that the threat scenario has been enacted.

**Stage 3. The detection of a threat occurrence.** Example threat detectors are smoke detectors, and password mechanisms that keep track of the number of times an incorrect password can be entered. In many cases there may not be a formal detection method beyond Standard Operating Procedures for system personnel. For example, the initiation of a flood would most likely be detected by listening to weather reports and being aware of the external environment. All detection mechanisms that are brought to bear against the threat occurrence are included in this stage.

**Stage 4. The recovery from a threat occurrence.** In this stage, if totally successful, the threat occurrence is prevented from causing a security breach. For example, stopping a fire before any damage to the system occurs is a successful recovery from the threat of fire. All recovery mechanisms that are brought to bear against the threat occurrence are included in this stage.

**Stage 5. The occurrence of a security breach.** There are three possible security breaches:

- Compromise of classified, proprietary, or sensitive information
- Loss of data or software integrity
- Loss of system availability

This model makes a clear distinction between the security breach itself and the harm that the breach causes, which is modeled in stage eight. This allows us to model the ability to recover, to whatever extent possible, after a breach occurs but before harm is brought to the system. For example, for threats that disable hardware, the security breach is the loss of system availability. If backup systems are installed in a timely manner in stages six and seven, the resultant harm is minimized.

**Stage 6. The detection of a security breach.** Sample security breach detectors are procedural hardware inspections for tampering, and periodic automated search of audit files to find a possible security violation. All detection mechanisms that are brought to bear against the security breach are included in this stage.

**Stage 7. The recovery from a security breach.** In this stage, an attempt is made to limit or eliminate the harm caused by a security breach. For example, the installation of spares after theft of a system component. All recovery mechanisms that are brought to bear against the security breach are included in this stage.

**Stage 8. The occurrence of harm.** The term "harm" is used specifically for losses that are external to the system. There are five possible harms:

- Failure of mission
- Loss of personnel
- Loss of resources
- Loss of dollars
- Loss of time

For most types of security breaches, more than one of the harms can be the final result. Note that the compromise of information by itself, is not considered a harm, but rather a security breach. In the case of a compromise, the harm could be the failure of a DoD mission and the loss of personnel. In the risk assessment's numerical analysis, all five of these harms will be represented as a dollar loss per year. Though somewhat insensitive, risk assessments often quantify loss of personnel in terms of a dollar amount. In this analysis we will do likewise, but only because it allows a quantitative comparison of risk and loss. Other methodologies suggest using a qualitative measure of loss associated with non-physical assets. Since this results in an "apples to oranges" comparison of where the system's security weaknesses exist, this model avoids this practice.

## **2.2 The Numerical Analysis for the Eight-Stage Model**

In Figure 1, the external influence, the internal influences, and the consequences are depicted as different shapes. This distinction is reflected in the numerical analysis for the eight-stage model, since of the type of data that is associated with each is also different. Each external influence (threat) has an associated probability of occurrence per year, which is a number between zero and one, inclusively. Each internal influence (detection or recovery countermeasure) has a Countermeasure Effectiveness probability, which represents the probability that a single occurrence of a threat or security breach will be detected or the extent to which the damage will be mitigated. Each consequence (harm) has an associated dollar loss per occurrence.

The symbolic representations for the numerical modeling are:

Threat Obstruction	Threat	Threat Detection	Threat Recovery	Security Breach	Breach Detection	Breach Recovery	Resultant Harm
CE <sub>TO</sub>	PR <sub>T</sub>	CE <sub>TD</sub>	CE <sub>TR</sub>	PL <sub>B</sub>	CE <sub>BD</sub>	CE <sub>BR</sub>	PL <sub>H</sub>

Where:

- **CETO** is the countermeasure effectiveness, stated as a probability, in obstructing a threat before it occurs. This measure should take into account the entire set of obstructers for the threat being analyzed.
- **PRT** is the potential risk (the probability) that a threat will occur within a year.
- **CETD** is the countermeasure effectiveness of a security breach detection mechanism.
- **CETR** is the countermeasure effectiveness of all of the threat recovery mechanisms in preventing the threat from causing a security breach.
- **PLB** is the potential loss (in dollars) associated with a security breach.
- **CEBD** is the countermeasure effectiveness of all of the applicable security breach detection mechanisms.
- **CEBR** is the countermeasure effectiveness of all of the applicable security breach recovery mechanism. That is, the extent to which the mechanisms will prevent the security breach from causing a resultant harm.
- **PLH** is the potential loss (in dollars) associated with the resultant harm.

A distinction is made in this model between **potential risk** and **effective risk**. Potential risk is risk associated with an external event, one that cannot be controlled by the system or the security procedures associated with it. Effective risk is the residual risk after the system or the system's security procedures mitigate the potential risk. A similar distinction is made between **potential loss** and **effective loss**: potential loss is associated with the loss outside the control of the system and the security procedures associated with it, and effective loss is the residual risk after the system or the system's security procedures mitigate the potential risk.

The numerical calculations are grouped into three areas: those associated with the level of risk and probable loss up to the possible security breach, those associated with the level of risk and probable loss from the time of the breach up to the possible resultant harm, and the numerical calculations associated with the level of risk and probable loss for the entire eight stages.

The numerical calculations for effective risk and effective loss are as follows:

- The **effective risk of a security breach** resulting from the ineffectiveness of the obstruction, detection, and recovery mechanisms is:  $ERB = PRT \cdot (1 - (CETO \cdot CETD \cdot CETR))$ . Note that the higher the effectiveness of the obstruction, detection, and recovery mechanisms, the lower the risk that a security breach will occur.
- The **effective loss due to a threat causing a security breach**, due to the ineffectiveness of the detection and recovery mechanisms, is:  $ELB = ERB \cdot$

PLB. This represents the average loss in dollars per year that can be expected from a particular threat due to the security breach alone.

- The **effective risk of a harm** resulting from the ineffectiveness of the detection and recovery mechanisms is:  $ER_H = (1 - (CEBD \cdot CEBR))$ . This is the risk that a harm will result after a security breach. Note that this risk level assumes that the security breach occurred.
- The **effective loss due to harm**, due to the ineffectiveness of the detection and recovery mechanisms, is:  $EL_H = ER_H \cdot PL_H$ . This represents the average loss in dollars per year that can be expected for a particular harm due to a security breach. Note that this level of expected loss assumes that the security breach occurred.
- The **total effective risk** is defined as:  $ERT = ER_B \cdot ER_H$ . This represents the overall level of risk that a threat could bring about a harm to the system. This is the probability that a threat causes a security breach which subsequently causes the resultant harm.
- The **total expected loss** is defined as:  $EL_T = EL_B + ER_B \cdot EL_H$ . This represents the total average loss in dollars per year due to a threat. Note that the expected loss due to a harm is multiplied by the risk of the security breach happening, because the loss due to the harm will not happen unless the security breach happens.

This model permits the calculation of a dollar loss against a security breach, even if there is no resultant harm. In the case of vandalism where hardware components are damaged, a timely replacement with spares may prevent any resultant harm. The model will reflect the dollar loss due to the damaged equipment and installation time, but may reflect little or no loss due to resultant harm.

### 3. PARTIAL RISK ASSESSMENT EXAMPLE

The following example is the analysis that would be performed on a single threat scenario. Although the analysis is extensive for this example, and there may be as many as one hundred scenarios, this is still far less effort than the traditional method of constructing a full matrix of all threats versus all vulnerabilities, and then crossing those pairs against all countermeasures. The substantial problem of deducing the probabilities of events and the effectiveness of detection and recovery measures is outside the scope of this paper. Table 1, Example Risk Assessment Matrix, provides the results from analysis of this example.

Threat Scenario: A subverted, authorized user attempts to surreptitiously print multiple copies of classified text on the system printer. His plan is to hide the fact that multiple copies were made, so that the additional printouts can be secreted away. The likelihood of occurrence in one year of this threat scenario is 0.05.

Threat Obstruction: The following activities may prevent the threat from being acted out: standard security briefings keep all employees aware of the security

procedures in place and the consequences of being apprehended if procedures are violated, the knowledge of the in-place auditing, and the watchful eyes of cleared co-workers. Likelihood of obstruction is 0.25 since subverted employees will consciously avoid security procedures.

**Threat Detection:** The following activities may detect the subversive employee before he has created the multiple prints: automated auditing analysis (intrusion detection) detects abnormal behavior, co-workers observe his behavior, a supervisor detects a personality change or subversive behavior. Probability of detection is 0.9.

**Threat Recovery:** Activities include: Information System Security Officer detects mismatch between classified output log and audit records before subverted user completes the printing, co-worker stops subverted user, and supervisor takes procedural steps due to personality change. Probability of recovery is 0.9.

Table 1. Example Risk Assessment Matrix

STAGES	DESCRIPTION	CALCULATION	VALUE
Threat Obstruction	Briefing In-place auditing Co-workers	$CE_{TO}$	.25
Threat Scenario	Subverted user printing multiple copies	$PR_T$	.05
Threat Detection	Audit Co-workers Supervisor	$CE_{TD}$	.9
Threat Recovery	ISSO audit Co-worker Supervisor	$CE_{TR}$	.9
Security Breach	Cost of paper	$ER_B = PR_T \cdot (1 - (CE_{TO} \cdot CE_{TD} \cdot CE_{TR}))$ $PL_B$ $EL_B = ER_B \cdot PL_B$	.04 = .05 • (1 - (.25 • .9 • .9)) \$0.25 \$0.01 = .04 • \$0.25
Breach Detection	Audit Co-workers Supervisor	$CE_{BD}$	.9
Breach Recovery	ISSO audit Co-workers Procedures	$CE_{BR}$	.9
Harm	Failure of mission Loss of personnel	$ER_H = (1 - (CE_{BD} \cdot CE_{BR}))$ $PL_H$ $EL_H = ER_H \cdot PL_H$  $ER_T = ER_B \cdot ER_H$ $EL_T = EL_B + (ER_B \cdot EL_H)$	.19 = (1 - (.9 • .9)) \$1,000,000 \$190,000 = .19 • \$1,000,000  .0076 = .04 • .19 \$7600.01 = \$0.01 + (.04 • \$190,000)

**Security Breach:** The financial impact of the security breach is low: only the cost of the additional paper. This is a critical point. The cost of the breach itself is very low,

and if subsequent detection and recovery measures are effective, the harm will be minimal.

**Breach Detection:** The following activities may detect the subversive employee after he has created the multiple prints: automated auditing analysis (intrusion detection) detects abnormal behavior, co-workers observe his behavior, a supervisor detects a personality change or subversive behavior. Probability of detection is 0.9.

**Breach Recovery:** Activities include: Information System Security Officer detects mismatch between classified output log and audit records before subverted user completes the printing, co-worker stops subverted user after printout has occurred, and procedural steps are taken when a compromise of data has occurred. Probability of recovery is 0.9.

**Resultant Harm:** The financial impact of the resultant harm is high: in our calculations, we typically use \$1,000,000 per compromise.

#### **4. RESULTS THAT CAN BE DRAWN FROM THE EIGHT-STAGE MODEL**

In addition to the obvious detailed threat and cost information generated by the model, higher level trends can be extrapolated from the model. High risk areas are highlighted by the annual expected loss. The absence of procedural security activities, particularly those associated with detection, is obviously indicated by holes in the risk assessment matrix. Unbalanced security efforts that emphasize post-breach activities will be highlighted by clustering in the matrix. The periodicity of post-breach detection activities, such as audit trail analysis, will highlight the length of time a breach may go undetected.

#### **5. ISSUES NOT ADDRESSED BY THE MODEL**

The model primarily addresses factors which are immutable. By this we mean that the threats don't change without direct intervention and time is not a factor except as it applies to the chain of events.

A factor of the former type is cost to the adversary to overcome a countermeasure. Even though a vulnerability may exist, the cost to an adversary to exploit it may exceed the value gained through a successful breach. By virtue of the cost to exploit, the risk has changed without intervention.

An example of the latter type is cost/benefit over time. This can be thought of as the reverse of the previous example. Perhaps the cost to prevent a breach exceeds the value of the asset to be protected. The other factor which is directly related to time is the expiration of sensitivity. Some information such as mission plans may only be sensitive until the mission has been completed. Under these circumstances, the countermeasure to protect the information only needs to be effective for the period of sensitivity. A good analogy for this is a safe which is rated for the number of hours it can withstand attempts to break it.

## 6. FUTURE RESEARCH

We have identified two areas for future research to improve the model: tandem threat management and cost/benefit analysis. Tandem threat management [2] addresses scenarios where more than one threat is actively attempting to breach the system at a particular time. The model would need to address the interaction between the scenarios, particularly when the same countermeasure applies to more than one active threat. Implementation of cost/benefit analysis in the model requires inclusion of adversary cost information, i.e. cost to the adversary to affect a breach, and distribution of countermeasure cost over multiple threats.

### REFERENCES

- [1] T. W. Osgood, "A Risk Analysis Model for the Military Environment," Proceedings of the 11th National Computer Security Conference, October 1988, pp. 43-52.
- [2] L. M. Jaworski, "Tandem Threat Scenarios: A Risk Assessment Approach," Proceedings of the 16th National Computer Security Conference, September 1993, pp. 155-164.
- [3] S. T. Smith, M.L. Jalbert, "LAVA/CIS Version 2.0: A Software System for Vulnerability and Risk Assessment," Proceedings of the 13th National Computer Security Conference, October 1990, pp. 460-469.
- [4] DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, December 1985.
- [5] DoD 5200.28-D, Security Requirements for Automated Information Systems, 21 March 1988.
- [6] DoD 5220.22-M, Industrial Security Manual for Safeguarding Classified Information, January 1980.
- [7] DoD 5220.22-R, Industrial Security Regulation, December 1985.
- [8] MIL-STD-1785, System Security Engineering Management Program Requirements, 1 September 1989.
- [9] DoD 5200.1-R, DoD Information Security Program Regulation, June 1986.
- [10] DoD 5200.1, DoD Information Security Program, 7 June 1982.
- [11] FIPS PUB 31, Guidelines for Automatic Data Processing Physical Security and Risk Management, U.S. Department of Commerce, National Bureau of Standards, June 1974.
- [12] FIPS PUB 65, Guidelines for Automatic Data Processing Risk Analysis, U.S. Department of Commerce, National Bureau of Standards, 1 August 1979.



# SECURITY AWARENESS AND THE PERSUASION OF MANAGERS

Dennis F. Poindexter  
Center for Information Systems Security  
Professionalization Directorate, TGB  
3701 N. Fairfax Drive  
Arlington, VA 22203-1713  
(703)696-1906  
POINDEXD@CC.IMS.DISA.MIL

Security Awareness changes the way people think about risks and controls. It is about marketing the products and services of the computer security community to its constituency that is largely ignorant about what computer security is, or what it does. Most often it is a Information Systems Security Officer as advocate, representing the security position with management. This is not a mechanical process nor one that lends itself to a technical solution. It is about persuasion and argumentation. Kurt Lewin describes the organizational aspects as a three-step process: unfreezing, making changes, and refreezing<sup>1</sup>. Put another way, it is the process of making an environment for change, getting the change implemented, then making the changed condition the norm. Some preparation must be made for each phase. This is fluid process that demands attention to where a process is, what stage it is in, the support it has (and does't have), and the arguments necessary to continue movement towards a goal or sustain a policy after it is implemented.

## Environmental Factors

How difficult this may be depends upon factors that are not controllable, nor subject to much influence by a security function, but are the basis for the amount of change that is possible in a business system. Richard Pascale calls these factors that influence learning - the ability to adapt and change<sup>2</sup>. One can also look at the same items in the context of control systems being exercised in the organization. These are subtle controls on individual's ability to influence change:

1. The extent to which an elite group or single point of view dominates decision-making.
  2. The extent to which employees are encouraged to challenge the status quo.
  3. The induction and socialization of newcomers.
  4. The extent to which external data on performance, quality, consumer satisfaction, and competitiveness are cultivated or suppressed.
  5. The equity of the reward system and distribution of status and privilege.
  6. The degree of empowerment of employees at all levels.
  7. The historical legacy and folklore.
  8. The integrity of management contention processes, particularly with respect to surfacing hard truths and confronting reality.
-

These would seem to have very little to do with computer security, but they represent a control system that every business function must operate in, a control system that computer security is a part of by the nature of the kinds of restraints it puts on business processes. The social controls represented by Pascale would not be difficult to recognize inside a company. If a Security Officer should find him/herself in an organization that is dominated by a single point of view, discourages employees from challenging the status quo, treats newcomers like outsiders, ignores external data which affects its business reputation, rewards people who cause the least trouble, centralizes all power in a clique and grants no authority below it, has a legacy of failure or repeated problems, and will not face harsh truths, a reasonably intelligent person would find a job in another company. Change is impossible. This is a place that does not want a security person to correct problems that are identified; it wants someone to blame when the system fails.

### Evolution or Revolution

This is the type of environment that almost demands revolutionary change because evolutionary ones are protracted or impossible to attain. In any organization *there will be change*, but these factors influence how much there will be and how it will occur. Revolution simply means many large changes will occur at once to obtain the control objectives management will want.

Evolutionary change is less painful, but slower and less impacted by single events. The kind of organization that fosters evolutionary changes is decentralized and listens to its employees, allowing ideas with merit to be heard, debated, and quickly implemented. The management terms representing these concepts currently are "reengineering" and "total quality management".

In 1988, the President's Council on Integrity and Efficiency published its report on computer security, outlining 55 management controls that are necessary to insure confidence in systems performance. Many of the controls are not security in the traditional sense, and are not computer security as it is currently represented. They are largely the presence or absence of management controls over business processes. While adoption of this approach to business control severely increases the number of issues to be brought to management attention, it focuses attention on issues that are more closely aligned with the values of the audience.

There are four basic things described in this Report as the situation in controls today<sup>3</sup>:

1. There are many directives and policies that prescribe secure systems, but there are few simple, clear guidelines on how to build controls into new or existing automated information systems *and* at the same time show compliance with the directives.
2. There is no formal methodology currently in use that will *easily* identify needed controls as systems are being developed. As a result, extensive control reviews are needed after the system becomes operational.

3. There is no control process defined that is compatible with, and an integral part of, the total systems process. Rather, there is a tendency to address control issues separate from the many other systems activities.

4. Control and security responsibilities are often assigned to personnel who are organizationally remote from systems development and operation.

In systems that demands revolutionary changes, these four things will not matter as much. Even if all four were present to the advantage of the security function, it would be difficult to affect any change if the other environmental factors worked to its disadvantage.

### **Precipitous Events and Common Causes**

The greatest gains and losses in controls will probably be precipitated by a control failure that causes a perception of consequence to management and a resulting backlash of reaction that Arthur Miller, Harvard University, calls an irrational management response<sup>4</sup>. Viruses and hackers in systems are two examples he cites. The reaction is misdirected at security functions. Viruses and hackers are disturbing because they throw open visions of a lack of control that are potentially dangerous. The loss of confidentiality of secrets, the integrity of data, and its availability to those that need it are threatening to the personal and business reputations of individuals. They are not likely to be easily dealt with through evolutionary changes. Good management should have prevented the circumstances and equally good management will correct it. The corporate value system will support an overreaction in the name of recovery. In the extreme, it may even promote revolutionary changes.

Managers need to hear other issues that are related to what they do. Events like viruses and hackers are not the norm and an everyday approach is better served by the words of W. Edwards Deming, the well-known management analyst who changed Japan's way of doing business: A point beyond limits on a control chart, or a significant result in an experiment or test, indicates almost certainly the existence of one or more special causes. Points in control, or showing no significance, indicate that only common causes of variation remain... When you find most of the special causes and eliminate them, you have left common causes of variability.... Common causes are more difficult to identify than special ones are. Moreover, the removal of common causes calls for action by administration at a high level.<sup>5</sup> If executive management is to be reached, it must be reached with common causes.

### **Arguing a Position with Management**

The times we live in are dangerous for implementation of controls. As painstaking as it may be to argue for controls and to get them in place, the difficulty in keeping them lies in the control level that will be tolerated by management. The current slump in the world economy make this a difficult time. Mergers, acquisitions, downsizing, and downturns in business activity create an intolerance for controls and a focus on profitability, to the exclusion of many other things. New managers are everywhere, erasing the corporate memory on why many of the controls are in effect at all. New managers bring new values. Downsizing

of staff creates productivity demands that are inconsistent with many of the controls in effect and challenges will ensue<sup>6</sup>. It would be easy to enjoin this as a broad opportunity to excel, but it can be an overwhelming time.

The importance of corporate memory, values, and renewed challenges to control systems lie in their central role in persuasion and argumentation, the actual deliberation of a control process with management. The ability to argue a position successfully has three variables<sup>7</sup>. Argument, in this context, means simply the statement of a position and the support offered for it:

1. a perception by the receiver that the argument is rational
2. a perception that the argument is congruent with his/her values, and
3. a perception that the argument comes from a credible source

There is no magic formula or algorithm for the relative values that each of these holds. Argumentation depends upon the perceptions of the person(s) being influenced.

### **Rational Argument**

Rational does not necessarily mean logical. In computer security, where formal logic is almost a way of life, it is difficult to think about argument in any other way. Rieke and Sillars describe it this way<sup>8</sup>: *Argumentation and formal logic are not the same, nor does formal logic necessarily strengthen argumentation. There is ample evidence to show that people do not follow the laws of formal logic when they argue.* <sup>9,10,11</sup> Decision makers do not make decisions using formal logic and it can be counter-productive to pursue it. This does not mean that our decision makers are illogical, only that the strength of an argument made to them does not lie in its formal structure or proof.

Rational arguments require support. A simple assertion, a statement advanced by one person and adhered to by another without development, is rarely adequate. For those who inaccurately believe that their expertise will carry an argument or sustain a position, the result is usually failure. Some other evidence is required: (1) specific instances -- argument by generalization and illustration of a general principle once established<sup>12</sup>; (2) Statistics -- a means of citing a large number of specific instances without citing each one; (3) Testimony -- credible facts or opinions of another about an argument position<sup>13</sup>.

### **Values**

**What are managers really looking at when they make changes like restructuring the company?**

Why Restructure?

reduce expenses	89%
increase profits	83%
increase productivity	71%
competitive advantage	67%

shareholder return	60%
improve cash flow	56%
improve decision making	56%
reduce bureaucracy	55%
increase customer satisfaction	54%

\_Wyatt Co. 6 June 1991 Wall Street Journal

It would appear from this example that profitability, in one form or another, is the motivation for reorganization. This has all the elements of good argument: it is credible because it comes from the Wall Street Journal, rational because all the elements relate to one another, and it fits the perceptions of values in the Western business community. One would conclude that unfreezing management to allow for changes in this area requires some, or several measures of profitability.

Using faulty logic, one might say that security procedures, in order to be successfully changed, must be tied to profitability because that is what drives management decisions. While this may be true, the reference does not support this contention because it shows no relationship to the security of systems. Yet new security systems or procedural changes in existing ones, may be portrayed to management as having some economic impact on the organization, almost as if there were a direct correlation between the value of resources and the cost of protecting them. In both the case of reorganization and attending to security, the value system supports decisions made on the basis of profitability. Whether either of these are truth would not matter to the outcome.

Pascale argues that management reorganizes to get fit or to create constructive tension that is manageable <sup>14</sup>. The end result may be that the business makes more money, or it may be that the rationalization for the action will be in terms of cost verses benefit, whether it makes money or not. In the same way, security is not about money; it is about control of processes which, if unrestrained become detrimental to the company. They create risks which cannot be resolved by continuing the status quo.

Risks can cause political, economic, and social consequences in an organization that far outweigh any consideration of risk in a strictly monetary sense. We define these in terms of confidentiality, integrity, and availability but there is a different bottom line involved in the failure of these processes. The confidentiality of an internal memo, such as the one written by Bryant Gumble about one of his coworkers, does not have much value to the national defense, but it has a great deal of value to a personal business reputation. Major credit reporting activities have reason to be concerned about the accuracy of databases which cause enough public concern to damage their business reputation. Sears and IBM consistently deny rumors, which may not be true but affect business reputation, of the reading of mail on their on-line service, Prodigy. The availability of telephone and data line services have caused AT&T, which has publicly given reasons for failures, a certain amount of damage to their business reputation. Where the perception of the receiver is concerned, truth does not matter. The damage is the same.

Managers live on reputation and so do businesses. Public or private embarrassment, and the ensuing damage to personal and business reputations, are the greatest management risks, absent prosecution for criminal behavior. These risks are traditionally ignored, yet are a key ingredient in the unfreezing of managers.

### **Credible Sources**

**The vast majority of people working in your company have absolutely no idea what you do there, and the rest are laboring under misconceptions.** <sup>15</sup>

**Mark McCormack**

The perception of the receiver must be that the argument comes from a credible source. McCormack's statement may help explain why a person inside an organization can frequently have less credibility than one with no more experience or knowledge, but coming from outside the business. Nobody knows what an outsider does, or is supposed to do.

Some managers do not know what security does for them other than change passwords or write contingency plans. These narrow views come from an obvious lack of exposure to common causes of control failures that require a security function input. These opportunities are not frequent and demand preparation. This requires quite a bit of work in advance of the opportunity. The action plan is an outline of how best to pursue this type of change.

### **Create a Plan of Action**

When there is opportunity for change, a person must be ready to argue a position that supports it. This is the purpose of a brief. Briefs are like contingency plans, kept sometimes for years, sometimes forever. A good source of briefs are the risk analyses which identify vulnerabilities and a range of responses, but may not result in change. A brief comes from the same concept used in the legal community:

#### **Brief**<sup>16</sup>

1. A statement of the claim for which adherence is sought.
2. A statement of any definitions necessary.
3. Statement of material which virtually all those involved with the claim agree on, including shared values
4. Statement of potential issues.
5. Outline of each issue with claims and support for *both* sides.

## Action Plan

An action plan starts with a brief and is mapped according to audience and issues. The brief outlines what audiences have shared values and what objections they may have to the policy or procedural changes required. Action plans are required for only a small portion of briefs, those representing the most serious common causes which have not yet been corrected. They are necessary for preparation and are superior to corporate memory. The action plan is a representation of what is required to make a change once the audience is receptive to making it. Practice of the approaches, even mental practice, is essential. It requires patience to wait for the opportunity, or create opportunities where they can be manufactured.

There are seven basic factors governing an action plan:

1. No single action will sustain an argument over time.
2. There is a target audience for each category with different shared values.
3. Time will be short for each opportunity to argue a position, probably less than 15 minutes.
4. The time slot for this program is not likely to be prime time .
5. The message must be:
  - simple
  - in standard language
  - current and credible
  - repeated often
  - repeated in different media
6. The manager must understand what action is necessary, even if this means paying attention to the problem, but doing nothing.
7. The manager's motivation must be sustained until the action is taken.

Action Plans and Briefs and simple exercises, mental practice, in being prepared for the many opportunities that present themselves -- knowing what to say when the audience makes time available for the presentation of the security position. The economic environment and the constant change of business have made these opportunities more frequent., while making them no easier. Managers are more difficult to reach and the stakes in the arguments being made are very high, causing increased tension at every level. At the same time, a variety of management initiatives allow more access and greater chances of making changes that can be successfully argued.

### REFERENCES:

1. Kurt Lewin, *Field Theory in Social Science*, ed. D. Cartwright (Harper and Brothers, New York, New York) 1951, p. 37.
2. Richard T. Pascale, *Managing on the Edge* (Simon and Shuster Inc., New York, New York) 1990, p. 236.

3. President's Council on Management Improvement and the President's Council on Integrity and Efficiency, Model Framework for Management Control Over Automated Information Systems, January 1988, pp. 4-5.
4. Against the Odds, Public Broadcasting System, March 1991.
5. Mary Walton, *The Deming Management Method* (Putnam Publishing Group, New York, New York) 1986, p. 97.
6. Dr. Robert W. Edwards, banking consultant and President, Risks Ltd.; from an interview in Keadysville, Maryland, 12-19-91.
7. Richard D. Rieke and Malcolm O. Sillars, *Argumentation and the Decision Making Process* (John Wiley and Sons, Inc. New York, New York) 1975, p. 23.
8. Ibid, p. 75.
9. Morris R. Cohen, *A Preface to Logic* (Henry Holt and Company, New York, New York) 1944, pp 2-3.
10. Karl E. Weick, Process of Ramification Among Cognitive Links , Theories of Cognitive Consistency: A Sourcebook, Robert P. Abelson et al., eds. (Rand McNally and Company, Chicago, Illinois) 1968, pp. 512-519.
11. Mary Henle, On the Relation Between Logic and Thinking , *Psychology Review*, 69 (July 1962) pp. 366-378.
12. Chaim Perelman and Olbrechts-Tyteca, *The New Rhetoric* (Notre Dame Press, South Bend, Indiana) 1959, p. 357.
13. Rieke and Sellars, pp.97-113.
14. Pascale, p. 24 and 36.
15. Mark McCormack, *What They Don't Teach You in Harvard Business School*, (Bantam Books, Toronto, Canada) 1984, p. 79.
16. Rieke and Sillars, p. 158.



# **THE NETWORK MEMORANDUM OF AGREEMENT (MOA) PROCESS: LESSONS LEARNED**

William C. Barker  
Lisa M. Jaworski  
George R. Mundy  
Trusted Information Systems, Inc.  
3060 Washington Road (Rt. 97)  
Glenwood, MD 21738

## **ABSTRACT**

In this paper, we will describe the approach we developed for the execution of network Memoranda of Agreement (MOAs) for the Defense Simulation Internet (DSI). The purpose of establishing MOAs is to ensure that the minimum set of security requirements for the network is met by all nodes, specifically in the event that the nodes are accredited by different Designated Approving Authorities (DAAs). Although the MOA requirement is stated in many Department of Defense (DoD) and Service regulations, there is no standard MOA execution process described in these documents. Thus, many of our lessons were learned as the result of our experience in establishing such a process. In addition, there are no standard MOA templates available within the accreditation community; hence, we had to draft a standard MOA. Our MOA template includes the set of rules that all user sites (i.e., nodes) must agree to meet prior to being granted connectivity to the DSI. Although these rules for connection were developed specifically for the DSI, which is a dedicated mode network, they can be used, with some modification, as the basis for other network MOAs. Lessons learned as a result of the DSI MOA execution process and the rationale behind the rules for network connection are documented and discussed herein.

Keywords are: accreditation, DAA, MOA, and network.

## **INTRODUCTION**

The DSI is a network accredited to operate in the dedicated mode under the provisions of DoD Directive 5200.28 [5] and the Advanced Research Projects Agency (ARPA) Instruction #49 [3]. Both of these documents describe the Interconnection of Accredited Automated Information Systems (AISs) (IAA) view of network accreditation. This view requires that MOAs be established between the network accreditor and the accreditors of each of the user systems. Although the MOA requirement is stated in many DoD and Service regulations, there is no standard MOA execution process described in these documents. Thus, much of the information presented here was gained through our experience in establishing such a process. In addition, because there are no standard MOA templates available within the accreditation community, we had to draft a standard MOA. Our rules for connection, which all sites must agree to meet prior to being granted connectivity to the network, are presented below. Although these rules for connection were developed specifically for the DSI, they can be adapted for use by other network accreditors.

## **SYSTEM DESCRIPTION**

The DSI is being developed by ARPA and the Defense Information Systems Agency (DISA), with the support of the Defense Modeling and Simulation Office (DMSO). The DSI is a high capacity network testbed supporting a full spectrum of warfighting simulation

interoperability activities. It is intended to expand the commercial networking technology base available for defense modeling and simulation and to develop an experience base for expanded DoD use of distributed warfighting simulation. The Network Encryption System (NES), developed by Motorola, Inc., and approved by the National Security Agency (NSA) under the Commercial Communications Security (COMSEC) Endorsement Program (CCEP), provides the required security protection for user systems that connect to the DSI. The DSI has three classified subnets, which are cryptographically separated, and an unclassified subnet. The shared goal of ARPA, DISA, and DMSO is to transition the DSI into a core component of DISA's Defense Information Systems Network (DISN), which will become the common network infrastructure for DoD.

The DSI has evolved from the ARPA networking testbed known as the Terrestrial Wideband Network (TWBNet). ARPA simulation projects have been using the TWBNet since its inception due to the unique capabilities it provides via the Internet Stream (ST) protocol. These capabilities are: multicast, whereby multiple sites can receive a packet stream from a single source, and bandwidth reservation for support of real-time applications (e.g., virtual simulation and videoteleconferencing). Because the TWBNet has accomplished its objectives as a networking testbed, ARPA has evolved it to a testbed for distributed simulation applications, so as to preserve and extend its unique capabilities for the distributed defense simulation community.

### **ACCREDITATION APPROACH**

Accreditation is a formal declaration by the DAA that an AIS is approved to operate in a particular security mode using a prescribed set of safeguards. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security. The DSI is accredited to operate in the dedicated mode under the provisions of DoD Directive 5200.28 [5] and ARPA Instruction #49 [3].

Both DoD Directive 5200.28 and ARPA Instruction #49 discuss two approaches to network accreditation: IAA and unified. The approach taken for the accreditation of the DSI is the former. Each of these network accreditation approaches has different implications for the MOA process. These implications are discussed in the following paragraphs.

#### **Requirements for MOAs**

An MOA is a statement containing the record of agreement between the DAAs of interfaced or networked systems. It addresses the accreditation requirements of each system in order to maintain an acceptable level of risk for the interconnection. It is DoD policy that when AISs managed by different DAAs are interfaced or networked, an MOA is required that addresses the accreditation requirements for each AIS involved. The MOA must include:

- a. A description and classification of the data
- b. Clearance levels of the users
- c. Designation of the DAA who shall resolve conflicts among the DAAs
- d. Safeguards to be implemented before interfacing the AISs.

MOAs are required when one DoD component's AIS interfaces with another AIS, either within the same component or in another component, and when a contractor's AIS

interfaces with a DoD component's AIS or to another contractor's AIS (e.g., a backside connection). (A component is synonymous with an organizational structure.)

Given the IAA approach, an MOA is required between the DAA of each user system that connects to the DSI and the DSI DAA. User system DAAs are identified by the site. The DSI DAA is the Director of ARPA, who has designated his Deputy Director to serve as his agent. DoD Directive 5200.28 states that the heads of Government agencies are empowered to accredit their own systems under certain circumstances. MOAs are required only between the network DAA and the user systems/ sites. The sites need not establish MOAs with other sites.

Given the unified network accreditation approach, MOAs are not required because there is only one DAA, who has cognizance over the network and all of its nodes. Initially, this is the easier approach to network accreditation. However, the network would have to be reaccredited every time a node (i.e., user system/site) is added. Given the fact that the DSI was expected to grow rapidly, this approach would have been too costly and cumbersome in the long run. In addition, it is implicit in the unified network approach that, if adopted, ARPA would have been responsible for the security of each user system. Clearly, it was not in the best interests of either ARPA or the user systems for ARPA to have assumed such a role.

### **Definition of Security Boundary**

ARPA is responsible for ensuring that the rules for connection and secure operation are followed by the connecting user systems. As stated in the MOAs, the boundary of each of the classified DSI subnets is the unencrypted, clear interface to the DSI NESs. The DSI DAA has the security responsibility for the proper operation of the DSI NES system. The user system DAA is responsible for ensuring that all AISs connected in any way to the DSI NES interface meet the rules for connection and secure operation of that particular classified subnet. It is important to note that in the case of the DSI, the security boundary is not implicit according to who owns the equipment. The DSI Program Office provides equipment that will operate on the RED (unencrypted) side of the NES to the user sites. However, the Program Office does not have the security responsibility for this equipment after it has been installed at a site.

There is one exception to the differentiation between DSI security responsibility and equipment ownership: the Network Operation Centers (NOCs). There are two NOCs associated with the DSI. One is used to monitor the classified subnets and the other is used to monitor the unclassified subnet. Despite the fact that the AIS equipment is located at a contractor site and subsequently accredited by the Defense Investigative Service, it falls under the security purview of the DSI. This is because a large part of implementing the security responsibility for the network lies with the NOCs.

### **Backside Connection MOAs**

Because the IAA approach was adopted, and because of the nature of real-world network connections, it was anticipated that many of the user systems would, in turn, be interconnected with other systems. To be truly effective, DSI security must be ensured to the very end of the network wire. This means that the user systems that have backside connections have to establish MOAs with each of their backside connections. A requirement was established that a copy of all signed backside connection MOAs be sent to the DSI Information System Security Officer (ISSO) prior to activation of the backside connection.

## **Unclassified Site Agreements**

Because there are no NESs present on the unclassified subnet, the unclassified subnet boundary had to be defined in a different fashion from the classified subnets. Per ARPA direction, the network boundary for the unclassified subnet is the network gateway. In lieu of establishing MOAs for each unclassified site, it was required that, prior to permitting any user system to be activated, a statement be signed by the user system's Security Administrator to ensure that the users understand and acknowledge the security risk present in the unclassified subnet (i.e., no security mechanisms are provided) and that the users will not intentionally introduce malicious software into the network.

### **DRAFTING OF MOAs**

ARPA was responsible for developing the rules for connecting to the DSI and a template MOA. The template MOA was distributed to each user system/site several months prior to the network's anticipated initial operating capability. Instructions for completing the MOAs and checklists for obtaining the user system DAA's signature were also developed. This Site MOA Information Package was distributed as early as possible because it was anticipated that many of the user systems would not be formally accredited. This assumption turned out to be true. Because a copy of the user system's accreditation statement is a mandatory attachment to the MOA, it was important to allow the sites as much time as possible to obtain a formal accreditation statement.

Detailed information pertinent to the DSI rules for connection, as specified in the MOAs, is presented in the following paragraphs.

### **Rules for Connection**

The following rules for connection pertain to user systems directly connected to one of the classified subnets:

1. Before a backside connection to a DSI user system can be established, the requesting site (i.e., the site directly connected to the DSI) must make a formal written request to and gain approval from the DSI ISSO.
2. The boundary of the DSI is defined to be the unencrypted/clear interface to the DSI NES. The DSI DAA has security responsibility for the DSI AIS (i.e., the DSI NES). The user system DAA has the responsibility to ensure that all AISs connected in any way to the DSI NES interface covered in this MOA meet the rules for connection to and secure operation of the DSI.
3. All DSI user systems must, at a minimum, meet the DoD Directive 5200.28 requirements for dedicated mode of operation at the specified security level (e.g., Secret-Not Releasable to Foreign Nationals (NOFORN)). The accreditation statement for the user system will be provided by the user system DAA and become a part of this MOA.
4. If the user system covered in this MOA provides connectivity to any AIS(s) not managed by the user system DAA, then the user system DAA will establish an MOA with the DAA of the connecting AIS in accordance with the requirements of DoD Directive 5200.28. Prior to activating any backside connection, the DSI ISSO must have been provided a copy of the MOA signed by the directly-connected user system DAA and the backside

system DAA. This is to ensure continued compliance with the rules for connection to and secure operation of the DSI.

5. Every direct and backside user system covered in this MOA must be illustrated via a block diagram. This block diagram will be provided by the user system DAA and become a part of this MOA.
6. Every site must meet all installation, physical protection, accounting, procedural, and access control protection mechanisms required for the operation of the DSI NES and the accredited AIS at its site.
7. The user site agrees to operate the DSI NES in accordance with the NSA Operational Doctrine and the doctrine provided by DSI management.
8. User sites must have COMSEC accounts and must use DSI Network Administrator-approved, NSA-provided keying material for the DSI-managed NES cryptographic device.
9. User systems may be untrusted systems operating in the dedicated mode at the specified security level (e.g., Secret-NOFORN). (This is expected to be the normal operational mode for systems directly connected to the DSI.) In this mode of operation, all users must have the clearance and need-to-know for all data handled by their AIS. In addition, the user system DAA acknowledges that all other users of the DSI may have access to the data contained within his/her accredited AIS.
10. User systems may be untrusted systems operating in the system high mode at the specified security level. User systems that connect to the DSI and that are accredited to operate in this mode acknowledge that the DSI provides no protections within the DSI or other user systems beyond the DoD Directive 5200.28 accreditation requirements for the dedicated mode of operation. User systems accredited to operate in the system high mode accept responsibility for the possibility of increased risk to their AISs because of interconnection with systems accredited to operate in the dedicated mode.
11. User systems may connect with a single security level labeled port on a trusted system accredited to operate in the multilevel mode in accordance with the risk range identified in DoD Directive 5200.28. User systems that connect to the DSI and that are accredited to operate in this mode acknowledge that the DSI provides no protection within the DSI or other user systems beyond the DoD Directive 5200.28 accreditation requirements for the dedicated mode of operation. User systems accredited to operate in the multilevel mode accept the responsibility for the possibility of increased risk to their AISs because of interconnection with systems accredited to operate in the dedicated mode.
12. User systems that employ trusted operating systems must operate the trusted operating system in accordance with the system's Security Features User's Guide and Trusted Facility Manual.
13. User systems must treat all information received via the DSI ports (directly and indirectly) as classified at the specified security level (e.g., Secret-NOFORN) until such information is manually reviewed and downgraded,

as applicable. Permanent storage media for information will be labeled and controlled at the specified security level.

14. Each user system/site must identify its facility accreditation authority and provide evidence of site accreditation at the specified security level (e.g., Secret-NOFORN) before connecting to the DSI (directly or indirectly).

It is important to stipulate that both accreditation statements and block diagrams for user systems be attached to the MOAs for proof of accreditation and configuration control purposes, respectively. It is important that the person who signs the accreditation statement is actually authorized to do so. Generally, for the Services and agencies, the Commanding Officer and the head of an agency are identified as DAAs, respectively. In the case of contractor sites, the Defense Investigative Service is the accreditor for systems that process Top Secret information and below. If the accreditation statement is signed by someone in a different role, a letter of designation should be sent along with the accreditation statement. Block diagrams allow the DSI DAA to determine exactly where an NES is placed and what is attached to it on the user's side.

### **EXECUTION OF MOAs**

As previously stated, a Site MOA Information Package, which contains instructions for completing the MOAs and checklists for obtaining the user system DAA's signature, was developed and sent to the user sites. This package is discussed in detail in the following paragraphs.

#### **Site MOA Information Package**

When a new user site is scheduled to connect to the DSI, a Site MOA Information Package is sent to the site. This package contains the following:

- a. DoD Directive 5200.28
- b. Direct Connection MOA Template
- c. Backside Connection MOA Template
- d. Site Connection Checklist
- e. List of Points of Contact (POCs).

Use of this package facilitates communication between the user system POCs and the DSI POCs. It also helps to expedite the MOA execution process since user sites are given MOA templates. All that a user site has to do is obtain its system accreditation statement and block diagram and fill in site-specific information such as accreditation date, DAA name and address, complete address of DSI interface point (i.e., the area where the NES will be located), mode of operation, clearance level of least cleared user, and the name, address, and telephone number of the user system/site's Network Administrator.

#### **Level of Resistance and Accreditation Knowledge of Site POCs**

It is to be expected that a user site will resist obtaining an accreditation statement if that site has never been formally accredited. This is because formal accreditation involves a lot of work and the timeframe within which it may have to be done will probably be very short. As previously stated, it is important to distribute the Site MOA Information Package as

early as possible because many of the user systems that are to connect to the DSI have not been formally accredited. Additionally, some sites may have to be reaccredited as a result of connecting to the DSI. Because a copy of the user system's accreditation statement is a mandatory attachment to the MOA, it is important to allow the sites ample time to obtain formal accreditation.

Unfortunately, it is exceedingly common for site POCs to have only a limited knowledge about accreditation. Thus, it is important to provide both the Site MOA Information Package and a network POC who can answer questions regarding accreditation. Although it is not the DSI Program Manager's responsibility to get a site accredited, unless the network provides such a service, it is unlikely that many of the user systems/sites would be able to connect to the DSI per the prearranged schedule.

### **Internal Review**

Prior to forwarding a site's MOA to the DSI DAA for signature, it is imperative that the MOA be reviewed by a DSI POC knowledgeable in accreditation. The body of the MOA should be reviewed word for word, and if the text is changed in any way from the standard MOA, it must be justified or the MOA should be rejected. Also, any MOA that does not have an accreditation statement or a block diagram attached to it should be rejected. The reviewer should compare the signature and title of the DAA on the accreditation statement with the signature and title of the DAA on the MOA. If the accreditation statement was signed recently but by someone other than the person who signed the MOA, the reviewer should inquire of the site why this is so. Finally, only signatures of the true DAA can be accepted (i.e., the site POC cannot sign these documents). It is to be assumed that the DAA's expectations will be high and time constraints demanding; therefore, incomplete or incorrect MOAs will not be processed.

A site may want to rewrite the sample MOAs so as to levy its own accreditation requirements on the network and other user systems/sites in the body of the MOA (e.g., a Navy site may want to include OPNAVINST 5239.1A and SECNAVINST 5239.2; an Army site may want to include AR 380-19; and an Air Force site may want to include AFR 205-16). This is unacceptable from the standpoint of the network because it would effectively result in the levying of those requirements on all other user systems in the network.

### **Delivery of Security Keys**

Delivery of security keys is the critical technical control point for the classified DSI subnets. Without the proper keys, the user system cannot function on a subnet. If a site resists compliance with these MOA execution procedures and user system accreditation requirements, the reviewer should remind the site that it will not be connected to the DSI until all of the required paperwork is completed. This is ensured by the fact that security keys will not be delivered to the site until all such paperwork has been completed and approved by the DSI DAA.

After the MOA has been approved and signed by the network DAA, a network POC must notify the person holding and arranging delivery of the keys to the sites. This network POC must also forward a copy of the approved MOA to the network key manager for purposes of configuration control. Also, when a site is to be administratively removed from a subnet, it is important that the DSI ISSO send a letter stating this to the network key manager.

## **IMPORTANCE OF MOAS AFTER FINAL APPROVAL**

Although at first glance the execution of MOAs appears to be a paper drill, it is not. MOAs serve as valuable contractual vehicles between ARPA and the user systems/sites. The MOAs established between ARPA and the user systems/sites are essentially contracts that define the security responsibilities of both parties and the terms of the agreement between both parties. The network DAA has reserved both the responsibility and the right to revoke a user system's DSI connection privileges if it discovers that a breach of contract (i.e., a violation of the rules for connection to the DSI) has occurred.

One of the rules for connection to the DSI is that before a backside connection to a DSI user system can be established, the requesting site (i.e., the site directly connected to the DSI) must make a formal written request to and gain approval from the DSI ISSO. This is done in order to accurately monitor network performance; to ensure that the rules for connection to the DSI are followed by the backside sites; and to enforce other contractual obligations between ARPA and the user systems/sites.

## **CONCLUSIONS**

Although the drafting and execution of network MOAs is both time consuming and tedious, it is extremely important in terms of the enforcement of the network security policy (i.e., the rules for connection to the network) and in the definition of security responsibilities between the two parties. This process should commence early in the network development process so that there will be sufficient time for unaccredited user system/sites to become accredited and for MOAs to be granted final approval before the projected initial operating capability.

## **ACKNOWLEDGEMENTS**

The authors wish to thank Ms. Lin Flynn for her support in the DSI accreditation process and in the development of this paper. All work was sponsored by ARPA and performed under contract number DABT63-92-C-0020.

## **REFERENCES**

- [1] AFR 205-16, Computer Security Policy, For Official Use Only, Headquarters, Department of the Air Force, Washington, DC, 28 April 1989.
- [2] AR 380-19, Information Systems Security, Headquarters, Department of the Army, Washington, DC, 1 August 1990.
- [3] DARPA Instruction #49, Automated Information System (AIS) Security, Defense Advanced Research Projects Agency, Arlington, VA, 19 December 1991.
- [4] DoD 5200.28-M, Industrial Security Manual for the Safeguarding of Classified Material, DoD, Washington, DC, January 1991.
- [5] DoD Directive 5200.28, Security Requirements for Automated Information Systems (AISs), DoD, Washington, DC, 21 March 1988.
- [6] OPNAVINST 5239.1A, Department of the Navy Automated Data Processing Security Program, Department of the Navy, Washington, DC, April 1985.



[7] SECNAVINST 5239.2, Department of the Navy Automated Information Systems (AIS) Security Program, Department of the Navy, Washington, DC, 15 November 1989.

[8] Site Procedures Manual for the Defense Simulation Internet (DSI), For Official Use Only, Trusted Information Systems, Inc., Glenwood, MD, June, 1993.

[9] TIS Report #414, Risk Assessment for the Defense Simulation Internet (DSI), For Official Use Only, Trusted Information Systems, Inc., Glenwood, MD, 1 December 1992.

[10] TIS Report #415, AIS Security Plan (AISSP)/System Security Document (SSD) for the Defense Simulation Internet (DSI), For Official Use Only, Trusted Information Systems, Inc., Glenwood, MD, 1 December 1992.

# INDEPENDENT VALIDATION AND VERIFICATION OF AUTOMATED INFORMATION SYSTEMS IN THE DEPARTMENT OF ENERGY\*

William J. Huntman  
Los Alamos National Laboratory  
Safeguards Systems Group  
Phone: 505-667-0096  
Fax: 505-667-7626  
(wjh@lanl.gov)

Robert Caldwell  
Department of Energy  
Office of Safeguards and Security  
Phone: 301-903-3019  
Fax: 301-903-8414

## Introduction

The Department of Energy (DOE) has established an Independent Validation and Verification (IV&V) program for all classified automated information systems (AIS) operating in compartmented or multi-level modes. The IV&V program was established in DOE Order 5639.6A [1] and described in the manual [2] associated with the Order.

This paper describes the DOE IV&V program, the IV&V process and activities, the expected benefits from an IV&V, and the criteria and methodologies used during an IV&V. The first IV&V under this program was conducted on the Integrated Computing Network (ICN) at Los Alamos National Laboratory and several lessons learned are presented.

The DOE IV&V program is based on the following definitions. An IV&V is defined as the use of expertise from outside an AIS organization to conduct validation and verification studies on a classified AIS. Validation is defined as the process of applying the specialized security test and evaluation procedures, tools, and equipment needed to establish acceptance for joint usage of an AIS by one or more departments or agencies and their contractors. Verification is the process of comparing two levels of an AIS specification for proper correspondence (e.g., security policy model with top-level specifications, top-level specifications with source code, or source code with object code).

## DOE IV&V Program

The DOE IV&V program is designed to provide an additional level of assurance for automated information systems (AIS) that have a higher level of risk due to the sensitivity of information being processed or due to differences in user clearances. This section will discuss the goals of the IV&V program, when an IV&V is required, the outputs expected from an IV&V, and the administrative issues, such as funding, organization, and management.

The DOE protection requirements are arranged in a hierarchical manner based on the classification level of the information and the clearance level of the AIS users. This hierarchy ranges from zero to five and is called a protection index. A protection index of zero corresponds to a dedicated mode of operation. A protection index of one corresponds to the system-high mode of operation. A protection index of two

---

\*This work supported by the US Department of Energy, Office of Safeguards and Security.

corresponds to a compartmented mode of operation where information is separated into one or compartments and formal access approvals are required for access to the information.

A protection index of three is loosely defined as "secure multi-level" because all AIS users are cleared, but there is at least one level of difference between one or more user clearance levels. For example, an AIS in which some users have a DOE Q clearance (equivalent to a Top Secret clearance) and one or more users have a DOE L clearance (equivalent to a Secret clearance) would have a protection index of three.

A protection index of five is a multilevel AIS where at least one access point, used by an unclassified person, is located outside the security area and is authorized to process only unclassified information. An additional requirement is that all of the access points outside the security area must be located within the boundary of the facility. No access is allowed from off site.

### **IV&V Program Goals**

The primary goals of the IV&V program are to

- support the objective analysis of security risks in an AIS operating with a protection index greater than or equal to two and
- to facilitate the accreditation of AISs by providing assistance to the designated accrediting authority (DAA).

These goals ensure that all AISs with an increased level of risk receive an independent review that is integrated into the accreditation decision. Secondary goals of the IV&V program include

- providing technical input to the AIS certification,
- maintaining a technical library of the results of IV&V activities to reduce redundant activities and to aid AIS developers,
- identifying any policy areas that should be considered for modification or addition to the DOE policy for classified computer security, and
- identifying areas where research and development is needed to enable DOE AISs to meet the policy requirements.

A library of IV&V results should reduce the overall resources needed to conduct future IV&Vs by eliminating the need to repeat previous analyses and reviews. This library is also expected to improve the security of new AISs by allowing the AIS developer or integrator to apply the results of previous IV&V work.

### **When an IV&V is Required**

An IV&V is required for all AISs that have or will operate with a protection index of two or higher. The IV&V process will begin when the tentative or actual protection index for the AIS is determined. The IV&V process is initiated by the AIS security officer who documents the need for an IV&V and forwards the request through the accreditation hierarchy. The security officer is also expected to simultaneously submit a funding request for IV&V support through the appropriate channels.

The actual IV&V activities are expected to start with the preliminary design of the AIS. The maximum benefit will be gained by involving the IV&V team during the AIS design when changes can be made with a minimum impact.

## **IV&V Outputs**

The outputs expected from an IV&V are divided according to the phases of an IV&V. Phase one occurs during the AIS preliminary design phase. Phase two occurs after the AIS has been implemented and during the security certification testing of the AIS.

The outputs required for phase one of an IV&V are

- a report documenting the results of the analysis of the AIS preliminary design including any recommendations for changes and
- a description of the expected IV&V phase two activities including a plan for managing the activities and the estimated costs for the activities.

The report required as output from phase two of an IV&V contains

- documentation of the analysis of the AIS Security Test Plan and the analysis of the security test results,
- any recommendations for changes in the AIS design or implementation or both,
- if necessary, recommendations for additional security testing, and
- the IV&V team recommendations for AIS accreditation.

Depending on the results of the IV&V analyses of the AIS, recommendations may be made to modify or clarify current DOE computer security regulations. The analyses may also identify areas where new or redirected research and development is needed to provide cost-effective solutions to meeting DOE requirements.

## **Funding, Organization, and Management of an IV&V**

All funding for an IV&V is provided by the organization responsible for the management and operation of the AIS. Typically, the initial funding is provided only for the phase one activities. The additional funding necessary for phase two is supplied after the IV&V team has completed the phase one activities. All estimated funding requirements must be reviewed and approved by the accreditation hierarchy before committing any funds. This review will ensure that IV&V resources, such as personnel and money, are appropriate to the required level of effort. Funding for an IV&V for a very complex AIS should not exceed \$30,000 for phase one and \$60,000 for phase two. The values are the maximum expected for an AIS and will be required only when the network involves a number of different computer systems and other network components that all require extensive analysis and review. An IV&V on a typical local area network is expected to cost \$15,000 to \$25,000.

An IV&V is performed by a team. The minimum composition of the team is a coordinator and at least one other individual. Most teams are expected to contain a coordinator and two individuals. The team members are contractors from outside the DOE and DOE contractor organizations to ensure the proper independence in the process. The official team coordinator is the DOE Computer Security Program Manager (CSPM) or a person designated by the CSPM. The CSPM is the DOE person responsible for establishing the computer security policies for classified computing in the DOE. Other individuals may be added to the team either as members or as observers to represent organizations that may have an interest in the AIS. The AIS organization will contribute at least one person who acts as the liaison between the IV&V team and the AIS organization. All personnel who participate in the team activities are expected to contribute to the analyses, reviews, and report preparation.

The team activities are directed by the chairperson. The chairperson is responsible for coordinating the team activities with the representatives of the AIS organization and representatives of the accrediting authority.

## **IV&V Process and Activities**

An IV&V is performed in two phases. Phase one is performed during the initial design and implementation of the AIS. Phase two is conducted after the AIS has been implemented and is ready for security certification.

### **Phase One Activities**

Phase one activities include reviews of documents and interviews with AIS developers, AIS management, and computer security people responsible for the AIS. Critical documents reviewed during this phase include the AIS design specifications and descriptions, the AIS Security Plan, and the AIS Security Test Plan (if it exists). During phase one, the team is guided by the criteria established for the validation phase. These criteria, described in the following section, define the minimum requirements the AIS must meet to comply with DOE regulations.

Phase one is concluded with reports prepared by the team and reviewed with the AIS personnel prior to release to the DAA. The contents of the phase one report document the team's understanding of the AIS, a description of the AIS Security Support Structure (SSS), the results of the team analysis, and the team's initial assessment of the risks or vulnerabilities in the AIS.

The DAA, in coordination with the CSPM, reviews and accepts the phase one reports. The DAA may accept the risks resulting from vulnerabilities or concerns identified by the team. The decision to accept risks will be coordinated with the CSPM and documented by the DAA. Once the DAA accepts the phase one report and documents the acceptance of any remaining risks identified by the team, phase two of the IV&V can be scheduled.

### **Phase Two Activities**

Phase two activities are not scheduled until the developers have implemented the AIS and prepared the Security Test Plan. The first phase two activity is to review and comment on the AIS Security Test Plan. This review is performed by the team members before it returns to the facility. After the team has reviewed the Security Test Plan, the AIS developers and security people will perform the security tests. After the security testing is completed, the team returns to the facility and reviews the results of the tests. This review is focused on ensuring that the security tests are complete and that the results clearly indicate that the tested function is implemented correctly. Depending on the results of the security tests, the team may request additional security tests to address any anomalies in the testing or to address functions missed in the original test activity.

During the review of the Security Test plan and test results, the team is guided by the verification criteria, described in the following section, to ensure that all necessary tests are included in the test plan and that each test adequately addresses the required security features.

After all testing is completed, the team will prepare the phase two report, which will document the team's analysis of the AIS testing, the team's assessment of the AIS risks and vulnerabilities, and the team's recommendations to the DAA. The phase two report is reviewed with the AIS personnel to ensure accuracy prior to release to the DAA. After the DAA has received the phase two report, the AIS organization, the computer security personnel at the site, and the DAA are expected to address any security issues identified by the team. The DAA may choose to accept the risk for any or all of the concerns identified by the team.

During either phase of an IV&V, the team may identify policy issues that may need clarification or modification. The team may also identify areas for new or re-directed research and development. The team will prepare a report describing the issue or need and a recommended solution and forward the report to the CSPM for consideration.

## **IV&V Criteria**

As mentioned earlier, the IV&V team is guided by criteria for validating the AIS design and verifying the AIS implementation. These criteria have been developed to establish a baseline set of requirements for satisfying DOE policy and to guide the reviews and analyses performed by the team. This section will describe the general approach to development of the criteria, how the DOE criteria are consistent with initiatives by the US Government, the DOE profiles defined by the criteria, and the structure of the criteria.

### **General Approach to Development of the Criteria**

The criteria were developed to define the minimum requirements necessary to meet DOE policies for classified computer security. The primary base for the criteria is DOE Order and Manual 5639.6A. Additional criteria that exceeded the DOE Order requirements were identified as desirable or recommended practices. If a protection was identified as desirable but was not reflected in the DOE order, during its development, either the order was updated or the protection was dropped from the criteria. Another concern during the criteria development was to ensure consistency between the DOE requirements, as expressed in the criteria, and other US Government initiatives in information security.

### **Consistency Between DOE Criteria and US Government Initiatives**

A desired goal during development of the criteria was, where possible, to maintain consistency with the draft Federal Criteria (FC) for Information Technology [3] then being developed by the National Institute for Standards and Technology. The consistency was desirable to permit DOE to easily update its criteria when the FC were officially released.

Because the DOE requirements take precedence over the draft FC, we used DOE Order 5639.6A as the baseline. For each DOE protection index defined in the Order, the FC components were mapped into the DOE protection requirements. If necessary, the FC components were modified to meet the DOE requirements and environments. This mapping process resulted in a clear understanding of the differences between DOE requirements and the draft FC. This mapping process created a combined set of requirements that met the DOE Order and incorporated the FC. A by-product of the incorporation of the FC was a structure similar to the profile concept defined in the FC.

This "profile" development process is somewhat different from the process described in the draft FC but has achieved the same results. The FC security environment and policy-requirement mapping descriptions are expressed in the DOE Orders through the protection index structure. The DOE Order and Manual defined the minimum security features that must be present for each protection index. The requirements are defined in very general terms and allow an AIS developer to select and implement the algorithm that is most appropriate for the AIS mission. Incorporating the requirements from the draft FC allowed a refinement of the DOE Order without specifying a particular implementation approach. Once the general requirements were defined, detailed criteria for each requirement were developed and the criteria were then composed into DOE "profiles" for each protection index.

## **DOE Profiles**

The DOE "profiles" have been developed for protection index two (compartmented mode), protection index three ("secure" multi-level mode), and protection index five (multi-level mode). The profiles are hierarchical beginning with protection index two. Most of the differences between the profiles are in the expected strength of the mechanisms. The DOE profiles contain elements that describe the information protection problem addressed by the profile; a rationale discussion that provides the fundamental justification for a profile, including the threat, environment, and usage assumptions; functional requirements that establish the protections that must be provided by an AIS; and development assurance requirements for all phases of an AIS development from initial design through implementation. Evaluation assurance requirements from the draft FC were not included in the DOE profiles.

The functional requirement components in a DOE "profile" include

- Identification and Authentication
- System Entry
- Trusted Path
- Audit
- Access Control
- Resource Allocation (object reuse)
- Security Management (security officer interface to the system)
- Reference Mediation (the involvement of the SSS in all accesses to objects)
- SSS Logical Protection (separate execution of the SSS functions)
- SSS Self Checking (checks for consistency and integrity of SSS components at startup and during execution)
- SSS Startup and Recovery (checks to ensure that the proper SSS is executed at start up and that the SSS always recovers to a secure state)
- SSS Privileged Operations (executions of SSS security functions are restricted to privileged components)
- Ease of Use (requirements for programming interface to SSS security functions)

The DOE "profiles" do not contain any requirement for covert channel analysis because the threats to DOE information do not justify the expenditure of resources necessary to identify and eliminate all covert channels. Some covert channels are identified indirectly as part of the development assurance component, such as penetration analysis and functional testing.

The development assurance components in a DOE "profile" include

- Property Definition (description of the protection properties implemented by the SSS)
- Interface Definition (description of the interface to the SSS, including informal models of the SSS)
- Modular Decomposition (description of the disciplines used during design and implementation of the SSS)
- Implementation Support (description of the configuration control procedures followed during implementation of the SSS)
- Functional Testing (description of the SSS testing and the procedures used to manage the test activities)

- Penetration Analysis (description of the process used to perform penetration analysis of the SSS)
- User Security Guidance (description of the AIS security functions for the users)
- Administrative Security Guidance (description of the AIS security functions for the security officer and system administrators)
- Flaw Remediation (description of procedures for reporting, tracking, and correcting flaws in the SSS)
- Trusted Generation (description of procedures for generating a known version of the SSS)
- Life Cycle Definition (description of the procedures and methods used to manage the SSS through its entire life cycle)
- Trusted Distribution (description of procedures used to ensure no unauthorized modifications are made to the SSS during shipment)
- Configuration Management (description of the procedures to manage the SSS)

The criteria for each protection are organized into two documents. The validation document defines the requirements and criteria that must be met for the AIS to conform to DOE requirements. The verification document contains all of the validation information and adds a generic test description for each criterion.

### **Structure of the IV&V Criteria Documents**

Each IV&V criteria document is organized into three sections. Section 1 describes the required security features and assurances and the environment addressed by the criteria. Section 2 describes the expected target audience of the criteria and the contents of the document. Section 3 contains the components that must be satisfied for the AIS to successfully meet the DOE requirements. Each component description contains

- a general description of the component,
- the specific DOE requirement(s) directly related to the component,
- one or more criteria that must be met to satisfy the component, and
- for each criterion, a generic verification test description.

### **Criteria**

Each functional requirement or development assurance component, such as audit or trusted generation, is decomposed into one or more criteria that must be satisfied to ensure that all of the requirements for the component are met. Each criterion represents a single concept or requirement. The general rule followed during the development of the criteria was that the criteria must be required or clearly implied by the component and the criteria must be easily tested.

During the development of the generic test description, we required that each test must unambiguously indicate success or failure. If we were unable to define a clear test description, we modified or split the criterion until the test description was unambiguous. This guideline also required that, while individual tests may be based on the results of previous tests, the test could not attempt to evaluate more than one criterion at a time.

Another requirement for the criteria was that the statement of the criteria must be independent of specific computer systems or architectures. This approach requires the IV&V team to interpret and apply the criteria to a specific AIS. However, this interpretation is not difficult because DOE requires the specific



security mechanisms in an AIS to be described in a document called the AIS Security Plan. This document provides the details that allow the IV&V team to apply the criteria. An example criterion from the criteria for protection index two is

The SSS shall end the attempted login session after the user performs the authentication procedure incorrectly for a number of successive times. Termination of the session, such as lockout, shall be recorded on the audit trail, the system console, and the system administrator's terminal.

An AIS implementation of this criterion would be described in the AIS Security Plan for the system, using language similar to the following:

The security software in this system will terminate an attempted login session after the user incorrectly enters a password five consecutive times. Each incorrect attempt is recorded in the system audit trail. After the fifth unsuccessful attempt, the session is terminated by locking out the terminal device. After the session is terminated, a message is written to the system audit trail and a message is sent to the operator console.

### **Generic Test Description**

The IV&V criteria documents are intended to provide a complete set of requirements and criteria for each of the protection indices. A generic test description, independent of any specific computer system or architecture, is supplied as part of each criterion. The descriptions are designed to be templates that can be used by a test developer to guide the generation of system-specific tests and to aid the IV&V team in evaluating the test plans and test results. Each test description contains

- Test Purpose (purpose of the test)
- Expected Result (results that should be produced by the test)
- Controlled Configuration (components of the AIS that should be controlled to ensure repeatability of the tests and to minimize impact on AIS users)
- Test Equipment, Material, and Personnel Required (resources required to perform the test)
- Input Used for Test (any special input needed during the test; for example, during a test for SSS self-checking, one of the SSS tables must be modified to introduce an error)
- Test Description (detailed sequence of events: describes the who, what, when, where, and how for the test)
- Pass/Fail Criterion (criteria for successfully passing the test, depends on the AIS and the SSS component being tested; for example, the pass/fail criteria for testing an authentication process that is based on passwords would include a description of the range of acceptable password lengths and the range of unacceptable password lengths)

### **Lessons Learned from First IV&V**

We have completed the first phase of the first IV&V conducted under the DOE IV&V program. This IV&V phase one review was performed on the Los Alamos National Laboratory Integrated Computing Network (ICN). This network is being redesigned and upgraded to support operation at the protection index three ("secure multilevel"). Phase one of the IV&V was performed on the ICN design during February 1994. Phase two of the IV&V will be conducted during the fall of 1994 depending on the progress toward implementing the design.

## **ICN Description**

The ICN consists of several segments and separately accredited networks. The ICN backbone contains an Fiber Distributed Data Interface (FDDI) ring and several routers. Users operate from one of several separately accredited networks that operate in the system-high mode. These user networks are connected to the backbone through the routers. The routers provide a primary control of messages and allowed communication paths.

Network servers, such as file storage, output services, and a CRAY YMP (running UNICOS 8.0), provide services to the users. All of the servers are designed to support multi-level operation. Other management and security services, such as collection and analysis of audit trails and user identification and authentication are provided by a separate network connected to the backbone. These additional services operate in the system-high mode because they do not allow user access or the execution of user processes. These services are provided to all components of the ICN, including the user networks.

## **Lessons Learned**

Early lessons learned from the IV&V phase one include several unanticipated or underestimated benefits. In addition to the objective analysis and review of the ICN design, we identified several areas where the then draft DOE policy needed clarification and one area where the policy need some interpretation to address state-of-the-art networking technologies. During our review of the ICN backbone and the servers, especially the identification and authentication server, we learned that the traditional view of security requirements for a complex network was difficult to apply to individual segments of the network.

When we attempted to review the ICN backbone, the traditional model of users as subjects acting on objects did not apply. Within the ICN backbone, the routers and network control nodes make security and routing decisions on message addresses. While the messages were being sent on behalf of users, there are no "users" in the backbone. We were forced to adapt the normal definitions of subject and object to fit the backbone. The definition we used was that a subject is a computer identified by a unique address and objects are the physical or logical communications paths connecting the computers. This definition of subjects and objects then allowed the team to adapt the IV&V criteria to allow analysis of the backbone. The backbone analysis required interpretation of components, such as access control and audit, using the new definitions of subject and object. For example, access control decisions in the backbone were based on mediation of connection requests between the source and destination addresses. Discretionary access was determined by administrative criteria expressed in the router tables. Mandatory access was determined based on a priori knowledge of data sensitivity through the hard-wired ports on each router and the contents of router tables.

Another segment of the ICN where the team experienced difficulty in applying the traditional view of security was the multilevel servers. For example, the ICN identification and authentication service is provided by the KERBEROS software operating on a platform isolated from the ICN backbone by a router. This approach allows the service to be available to all users and nodes anywhere in the ICN while ensuring that users are not allowed to directly access or execute processes on the server. The traditional model of security requirements is built on the assumption that users have (or may gain) the ability to execute their processes on the system. By creating a distributed system with multiple layers of protection, the identification and authentication server should not be required to meet the requirements necessary for a normal multi-user computer system. During phase one of the IV&V, we decided to analyze these servers from two perspectives. The first view was at the platform level. These platforms are located in an exclusion area, and access is restricted to system administrators, operators, and development personnel. A platform in this environment can operate in the system-high mode if there is adequate assurance that the interface between

the operating system and the application is sufficiently strong to prevent the application activity from affecting the security of the platform.

The second view of the servers was at the application level. Many of the servers in the ICN must operate the application in the "secure" multi-level mode. Analysis of the application from this perspective focuses on the security features of the protocol used to access the service and the interface between the application and the platform. We are currently developing additional criteria for this view of network servers.

Another underestimated benefit of the IV&V was the interaction between the ICN designers and the IV&V team. During the numerous discussions and interviews, the team members were able to offer suggestions to the designers to improve the security and information flow in the ICN. Most of the suggestions have been adopted in the ICN, and the designers obtained a better understanding of the security needs and requirements for the ICN.

### **Applicability to Other Environments**

The IV&V criteria and process appear to be a viable approach to obtaining an objective analysis of an AIS that would work for any other organization. The overall methodology is similar to the accreditation process used in the Department of Defense with the addition of criteria to guide the team's analysis.

Although the IV&V criteria are specific to the DOE, the process used to develop the criteria could be easily applied to other environments and organizations. The DOE criteria could be easily adapted to other situations because the criteria are generic and independent of AIS architectures.

### **Conclusions and Future Work**

The IV&V program and criteria have been demonstrated to be an effective technique for objective analysis of complex computer systems and networks in the DOE. The process provides detailed objective technical support to an accrediting authority and will reduce the residual risk in DOE AISs.

The initial IV&V activities have indicated that new criteria and approaches are needed for network components, client-server architectures, and distributed systems. We are currently working on developing new criteria for these areas.

### **References**

- [1] "Classified Automatic Information System Security Program," DOE 5639.6A, Department of Energy, Office of Safeguards and Security, April 4, 1994.
- [2] "Manual of Security Requirements for the Classified Automatic Information System Security Program," DOE M 5639.6A-1, Department of Energy, Office of Safeguards and Security, April 4, 1994.
- [3] "Federal Criteria for Information Technology Security," Volumes I (Draft) and II (Draft), National Institute of Standards and Technology and National Security Agency, December 1992.

# **Fuzzy Security: Formalizing Security as Risk Management**

**A Panel Presentation to the 17th NCSC Conference  
Baltimore, Maryland  
October, 1994**

## **ABSTRACT:**

This panel explores strategies for building flexibility into the formal aspects of computer security to produce more functional trusted systems.

## **PANELISTS:**

Ruth Nelson, President, Information Systems Security, Chair  
Hilary Hosmer, President, Data Security, Inc.  
John McLean, Supervisory Computer Scientist, Naval Research  
Laboratory  
Sergei Ovchinnikov, Professor, San Francisco State University

## **KEYWORDS:**

Fuzzy logic, Computer security, Network Security, Risk,  
Risk management

## **RATIONALE:**

Some computer security assumptions are so unrealistic it is virtually impossible to build complex trusted systems. For example, multilevel security policies which forbid all information flow from high to low are too restrictive to apply to networked systems where acknowledgements and two-way communications are necessary for reliable and smooth data transfer between machines. How do we get computer systems to perform their required functions with acceptable security?

Acceptable security is basically concerned with risk management. Yet, the formal models most used as paradigms in computer security ignore risk management and its fuzzy and subjective assessments. Mathematical tools, such as fuzzy logic, probability theory, and continuous math, are available to formalize security risk management, but are little used.

The Joint Security Commission, which prepared a report for the Secretary of Defense and the Director of Central Intelligence, concurs. The Joint Security Commission report acknowledges that the existing computer security

(COMPUSEC) paradigm which evolved during the Cold War no longer matches political, economic and technical realities. The Joint Security Commission proposes a new security paradigm based upon risk management in which we no longer look for perfect security to meet worst-case scenarios, but settle for a level of security appropriate to realistic threat estimates.

Fuzzy logic is appropriate to model the new reality. It provides a theoretically sound and rigorous method to handle many possible degrees of security. This panel addresses this fundamental problem from several different viewpoints.

## **PRESENTATIONS**

Ruth Nelson, an MIT-trained mathematician and network security expert who developed the mutual suspicion security concept and contributed to SDNS and Global Grid, will explain how security can be seen as a risk management issue. She will describe the problems and the kinds of mathematical tools available.

Hilary Hosmer, developer of the Multipolicy Paradigm, will illustrate how fuzzy logic can be used to model fundamental computer security concepts, especially "real" world policies and policy interactions.

Sergei Ovchinnikov, a fuzzy logic expert and long-time colleague of L.A. Zadeh, will describe his fuzzy generalization of the Bell and LaPadula model and issues involved in resolving conflicts among multiple policies.

John McLean, who is responsible for formal methods at NRL, will address several formal modeling issues, including the formalization of imprecise concepts.

## **DISCUSSION**

These papers will present views radically different from the conventional security approach, so strong reactions, both pro and con, are expected from the audience. The chair will query the panel with a set of prepared questions which the audience will also be invited to answer.

## **Security is Risk Management**

**Ruth Nelson  
Information System Security  
48 Hardy Ave.  
Watertown, MA 02172  
rnelson@cs.umb.edu**

The history of computer security has been full of conflict between the security practitioners and those more interested in the mission of the system than in security. Part of the reason for this conflict is an absolutist view of security and its assurance. Both the access control and data flow models used in computer security are based on an assumption that a secure system must prohibit all information flow from "high" to "low" security levels in order to be safe. Unfortunately, all operational systems require some such flows in order to work and so must be "insecure" by this definition. In fact, many "mission-oriented" systems<sup>1</sup> include authorized release of information derived from sensitive sources as part of their main function.

A more refined statement of the security requirement is that the system must prohibit the unauthorized release of secrets. Unfortunately for security practitioners, the concept of secret is inherently fuzzy;<sup>2</sup> that is, it is impossible to say whether some particular piece of information will convey something secret to an unspecified observer.

At present, our usual approach to computer security is to work within the "absolutist" models and definitions. We assume that the security goal of the system is preventing all information flow from high to low. We implement MAC policies to assure this. We evaluate the security of a system based on its conformance to these policies.

When, as almost always happens, we must allow output at a lower level than some of the input which may affect it, we either explain it away or we implement the output function in "trusted" code which can violate our model. Trusted downgraders cannot be relied upon; they can be fooled into allowing secrets to leak.<sup>3</sup> The model of security which is based on controlling information flow and which permits totally unexamined and untrusted applications software works only when its access rules are completely enforced. The formalizations of this model cannot describe the results of taking exception to it. With current models and methods, we have no way to measure the risk that allowing particular information flows will actually allow leakage of secrets from the system.

In other areas of security, including disaster management and cryptographic algorithm design, mathematical tools are used to measure risk. Some of these may be useful in computer security, particularly when we examine particular application systems and give up the goal of application-independent security models. In particular cases, we can estimate such quantities as:

- the likelihood that particular applications software is malicious;
- the "secrecy density" of particular data;
- the amount of loss incurred if particular data is disclosed;
- the likelihood that a particular object contains secrets;
- the likelihood that particular outputs will be misused;
- the probability of mislabeling (too high or too low).

The mathematical tools which can allow us to manipulate these estimates include fuzzy logic as well as statistics and probability theory. These tools, unlike those which are limited to two-valued logic, are useful in addressing real, operational systems which must violate the rigid models. The current models may have applicability in general system design, but fail to address the specifics of security in operational systems. Using "fuzzy" and "crisp" tools in combination may lead us to clearer understanding of security ideals and security reality. This understanding may end some of the conflict between operational needs and security and so could lead to more effective, more secure systems.

---

<sup>1</sup> C. Limoges, R. Nelson, J. Brunell, J. Heimann, "Security for Mission-oriented Systems," MILCOM '92, October 1992, San Diego, CA.

<sup>2</sup> R. Nelson, "What is a Secret?," New Security Paradigms Workshop, August 1994, Little Compton, RI

<sup>3</sup> *ibid.*

# FUZZY POLICIES

Hilary H. Hosmer  
Data Security, Inc.  
58 Wilson Road  
Bedford, MA  
email: Hosmer@Dockmaster.ncsc.mil

Most important policies are broad and vague. For example:

Goal: Equality of Opportunity

Policy #1. Thou shalt not kill.

The Ten Commandments

Policy #2. Employers shall not discriminate on the basis of age, race, gender, or national origin.

President Johnson, 1965

Policy #3. Everyone shall have access to the Information Highway.

President Clinton, 1993

Such policies undergo substantial interpretation and reinterpretation. For example, does Policy #1 require us all to be vegetarians? Must Policy #2 apply to someone who hires a personal servant? Does Policy #3 mean that each person on the planet gets a telephone link-up?

Implementing significant policies on trusted computer systems can be difficult. Defining the policies themselves is the first challenge. Translating vague human language and concepts into precise computer steps is the second. This includes representing policies in ways that both policy users and computer personnel can understand. Unfortunately, the abstract mathematical methods now in use are often unintelligible to both groups. Implementing the policies is the third challenge. Many trusted systems don't even provide a way for user policies to be implemented in a trusted fashion.

This presentation explores ways to build policy flexibility into trusted systems. It builds upon our work in multiple policies, resolving policy conflicts, and fuzzy logic.



# Assurance, Risk Assessment, and Fuzzy Logic

John McLean

Center for High Assurance Computer Systems  
Naval Research Laboratory  
Washington D.C. 20375

## 1 Introduction

As I have stressed elsewhere [1], one of the most striking properties of the *Trusted Computer System Evaluation Criteria* [2] and its international successors is that none of these documents contain any attempt to relate their evaluation levels to a measure of how much effort must be expended to break into a system. Hence, it is impossible to compute whether additional protection a higher rating represents is worth the additional cost incurred obtaining that rating. Even if we had such information, however, it would be unclear what to do with it since very little data is publicly available about either the cost the owner of a system incurs when a break-in takes place or the related, yet distinct, metric, the cost a penetrator is willing to incur to break into a system. I applaud any and all efforts to determine such figures since it is impossible to form a meaningful risk assessment without them. I also realize that exact figures are not forthcoming. However, I am not convinced that fuzzy logic provides a solution to this dilemma.

## 2 The Cost of Penetration

*Penetration* has a variety of meanings, depending on the context. A system may be easy to penetrate for the purpose of withholding service, but hard to penetrate for the purpose of obtaining or modifying confidential data. Even if we limit ourselves to one type of penetration, say confidentiality attacks, systems differ. For example, obtaining some types of data is useless if the penetration can be detected after the fact. For other types of data, this is not an issue.

Each one of these senses of *penetration* brings with it a different estimate of the cost incurred by the penetrator and the cost incurred by the owners of a system that has been penetrated. The secondary costs, e.g., the cost to a penetrator of potential jail time and the cost to a system owner that stems from the loss of prestige such a penetration can lead to, are even harder to calculate.

This problem of interpreting the numbers produced is compounded when the measures are manipulated, e.g., to produce compound costs. We know how to combine forces in

physics and we know how to combine probabilities. However, we do not know how to combine penetration costs. One obvious reason for this is that we do not know how to combine assurance levels. For example, on one hand it would seem that it would cost more to penetrate two B3 systems than a single B3 system. Hence, building a secure system from two B3 subsystems, both of which must be broken for a security violation to take place, would seem to increase security. On the other hand, such a system would, itself, simply be a B3 system. There is nothing in such an architecture that would raise it to a higher evaluation level.

### 3 Measuring the Cost of Penetration

One trouble with providing any quantitative measures for these costs, whether fuzzy or not, is that people inevitably believe that they represent something meaningful. For example, some have tried to relate the effort required to break into a system with the notion of mean time between failures, which is found in the dependability world. However, such an analogy fails to pass scrutiny. Dependability analysis assumes independent failures; security break ins are anything but. Once a hacker has learned how to break into one system, this information will be shared among friends and applied to similar systems.

On a more optimistic note, we should realize that there are already in place some quantitative measure for security. For encryption, there is complexity theory, which helps quantify the effort needed to break a code [3]. For confidentiality in computer systems, there are applications of information theory employed in quantitative security models [4, 5] and techniques for covert channel analysis [6, 7]. The difference between these information-theoretic measures of computer security and the sort of fuzzy measures some have advocated is that the former are quite clear about what, in fact, they are measuring. Although covert channel capacity and similar measures are not perfect indicators of this damage, they do, at least, approximate it since they give information about the time required to exploit a channel.[8] Nevertheless, their main benefit may be as a way of quantifying security/efficiency trade-offs in resource utilization algorithms [9].

This is not to say that information theory provides all the information we would like, even if we limit ourselves to confidentiality. Since systems with a capacity of zero can still leak information, we need to supplement capacity analysis with something like the Moskowitz and Kang *Small Message Criteria* [10]. Further, we are interested, not only in the time it would take to gain data from a system, but also in the tools that are required, the risk of exposure during the attack, the detectability of attack after the fact, the type of data at risk, etc. However, the limitations of information theory are well-known. The limitations of a figure that is given as fuzzily representing the security level of a system may be hidden. Information is lost in the single fuzzy metric, just as information was lost when cars replaced a panel of warning lights with a single "idiot light".

Turning to availability or integrity, although it's conceivable that information theory will be fruitful in these areas by quantifying how much secure information can flow in a system under denial of service or integrity attacks (a sort of inverse capacity measure which reflects the worst possible information rate rather than the best), there is no supporting research to demonstrate this. Performing such research would be a worthwhile endeavor.

## 4 Conclusion

To evaluate the effectiveness of techniques used to build secure systems some sort of quantitative measure of penetration resistance is desirable. However, I think that fuzzy logic is the wrong way to go since a single fuzzy metric of system security hides the information that was used to generate the metric and since there is an inherent danger of giving quantitative fuzzy metrics more credence than they really deserve. Certainly with respect to confidentiality, and possibly with respect to integrity and availability as well, information theoretic approaches, though not perfect, are more suitable. I believe that money would be better spent furthering such approaches, rather than developing fuzzy new ones.

## References

- [1] J. McLean, "New Paradigms for High-Assurance Systems," *Proc. of the New Paradigms Workshop*, IEEE Press, forthcoming.
- [2] National Computer Security Center, *Trusted Computer System Evaluation Criteria*, CSC-STD-001-83, Ft. Meade, MD, 1983.
- [3] D. Denning, *Cryptography and Data Security*, Addison-Wesley, Reading, MA, 1982.
- [4] J. McLean, "Security Models and Information Flow," *Proc. 1990 IEEE CS Symposium on Research in Security and Privacy*, IEEE Press, 1990.
- [5] J. Gray, "Toward a Mathematical Foundation of Information Flow Security," *Journal of Computer Security*, Vol. 1, no. 3-4.
- [6] J. Millen, "Covert Channel Capacity," *Proc. 1987 IEEE CS Symposium on Research in Security and Privacy*, IEEE Press, 1987.
- [7] I. Moskowitz and A. Miller, "The Channel Capacity of a Certain Noisy Timing Channel," *IEEE Transactions on Information Theory*, Vol. 38, no. 4, 1992.
- [8] J. McLean, "Models of Confidentiality: Past, Present, and Future," *Proc. Computer Security Foundations Workshop VI*, IEEE Press, 1993.
- [9] J. Gray, "On Analyzing the Bus-Contention Channel Under Fuzzy Time," *Proc. Computer Security Foundations Workshop VI*, IEEE Press, 1993.
- [10] I. Moskowitz and M. Kang, "Covert Channels - Here to Stay?," *Proc. COMPASS '94*, IEEE Press, 1994.

## Using Fuzzy Logic in Formal Security Models

Sergei Ovchinnikov  
San Francisco State University  
San Francisco, CA 94132  
sergei@mercury.sfsu.edu

The Joint DoD and CIA Security Commission proposes a new security paradigm in which we no longer look for perfect security, but settle for a level of security appropriate to realistic threat estimates. Fuzzy set theory is appropriate to model the new reality because it provides rigorous methods to handle many possible degrees of security.

Formal methods and models are inherent components of the computer security paradigm exactly because they provide for provable security. It is possible to develop formal models for computer security in a fuzzy environment and use fuzzy logic techniques to establish provable security. Not necessarily all components of such models must be fuzzy, but if we want to face the reality of computer security, we have to have at least some fuzziness present in formal models.

The core of any formal model based on the Bell-LaPadula (BLP) model is the basic computing machine. There are six elements constituting the BCM: subjects, objects, states, requests, decisions, and the machine's state-transition relation. The first five elements are sets that we denote  $S$ ,  $O$ ,  $Z$ ,  $R$ , and  $D$ , respectively. The last element is the machine's state-transition relation  $W \subseteq R \times Z \times D \times Z$ .

The state-transition relation determines the dynamics of the machine. Let  $\mathcal{X} = R^T$ ,  $\mathcal{Y} = D^T$ , and  $\mathcal{Z} = Z^T$  be infinite sequences of inputs, outputs, and states, respectively. If, while in state  $z_{t-1}$ , the machine receives the input  $x_t$ , then the output  $y_t$ , and the machine's next state  $z_t$ , must appear in  $W$

$$(x_t, z_{t-1}, y_t, z_t) \in W.$$

The *basic computing machine* is the system

$$\Sigma(R, D, V, W, V_0) \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$$

where

$$(x, y, z) \in \Sigma(R, D, V, W, V_0) \Leftrightarrow \forall t \in T, (x_t, z_{t-1}, y_t, z_t) \in W$$

and  $z_0 \in Z_0$  ( $Z_0 \subseteq Z$  is an indeterminate set of initial states).

We assume that all sets in the basic computing machine are crisp sets, but their elements could be represented by fuzzy sets. For example, the set of states  $V$  is defined in the BLP model as

$$V = P(S \times O) \times M \times F$$

where  $P(S \times O)$  is the set of all subsets of the Cartesian product  $S \times O$ ,  $M$  is the set of

all possible access matrices, and  $F$  is the set of all classification/need-to-know vectors. Then a state  $v \in V$  is a triple  $(b, m, f)$  where

$b \in P(S \times O)$  is a fuzzy subset on  $S \times O$ ;  $b(S_i, O_j)$  is the degree to which the subject  $S_i$  has an access to the object  $O_j$ .

$m \in M$  is an access matrix. Entries of  $m$  could be given as values of linguistic variables and represented by fuzzy sets.

$f \in F$  is a classification/need-to-know vector function that could be given as a fuzzy function.

In its simplest form the BLP model defines a secure system as a system  $\Sigma$  such that each of its states satisfies the simple security property. In a fuzzy environment, we introduce the degree  $\sigma_z$  (*security level of  $z$* ) to which state sequence  $z$  satisfies a fuzzy version of the simple security property. System  $\Sigma$  is secure if the security level of any state sequence  $z$  is not less than the security level of the initial state  $z_0$ . The fuzzy version of the Basic Security Theorem establishes conditions under which the system is secure. Under these conditions, a secure system can never reach a state with security level lower than the security level of the initial state.

Modeling policies is an important problem in computer security. It is especially important in the Multipolicy Machine paradigm where the researcher faces such issues as policy combinations, inheritance, order of execution, conflict resolution, etc. Since very often a policy is a *complex* and *inexact* concept, we employ an approach to modeling such concepts suggested by J.A. Goguen who, in the late 60's, demonstrated that, in a very precise sense, L-fuzzy sets is the only tool available for this purpose.

Suppose  $X$  is a set and  $L$  a complete distributive lattice. An *L-fuzzy set*  $A$  on  $X$  is a function  $A : X \rightarrow L$ . Examples of L-fuzzy sets include usual sets ( $L = \{0, 1\}$ ) and fuzzy sets ( $L = [0, 1]$ ).

Let  $\Sigma(R, D, V, W, V_0) \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$  be the basic computing machine. We define a *policy*  $\Pi$  as an L-fuzzy set on  $\Sigma$ . In other words, a policy is defined as a value (taken in  $L$ ) on a computation of the basic machine. This definition covers even standard situations in the framework of the BLP model. Suppose, for instance, that a subset  $S \subseteq \Sigma$  of "secure" computations is given (defined by means of the simple security property,  $\star$ -property, or in any other way). Let  $L = \{0, 1\}$  and consider just a characteristic function  $\Pi$  of  $S$ . Then  $\Pi$  is an L-fuzzy set on  $\Sigma$  representing certain policy. Thus standard security properties can be viewed as policies on the basic computing machine.

The theory of L-fuzzy sets can be successfully applied to problems in computer security. Consider, for instance, the problem of combining policies in the framework of Multipolicy Machine. Suppose  $\Pi_1, \Pi_2, \dots, \Pi_n$  are policies on  $\Sigma$  and  $\Pi$  is a "combined policy". It can be shown that, under rather weak assumptions,  $\Pi$  is an order statistic on the set of individual policies. Particular examples of such order statistics include minimum and maximum.

# Role Based Access Control

Hal Feinstein

Role Based Access Control (RBAC) is an access control strategy based on a user's role within an organization. It assumes a user's authorized accesses follow the lines of responsibility and that access rights are derived from delegated authority. By knowing the specific delegations for each role it is possible to deduce the accesses that role possesses. Recently, role based access control has emerged along two different developmental lines; database design and large transaction systems. In the first, database designers observed that many of their access control problems can be naturally stated in terms of roles. For some time database designers utilized access control analogs (ad hoc structures) for role based security without assigning any formality to the idea. More recently a definition of role based access control has been introduced by the commercial database ORACLE version 7. Role based access control is also being proposed for the future SQL 3 standard.

RBAC's second line of development occurs within distributed transaction systems. Designers are starting to use role based concepts within new large information systems in the medical and financial communities. The environment in these systems is rich in role varieties making it suitable for the expressive power of role inheritances. Much of the awkwardness usually associated with ownership-based access control schemes such as discretionary access controls is avoided.

Another equally significant use of role based concepts is in the cryptologic community. Perhaps the most interesting is RBAC's use in certificate based cryptosystems. Such systems find use over a wide geographical area. A mechanism is needed however, to authorize users to perform administrative functions anywhere the system might be in use. For example, some certificate systems have local authority workstations that act as a local representative of the system's certificate authority. An authorized user can assume the role of a local authority workstation by using his certificate which has been encoded to permit this role. Some certificate systems use the term *personalities* to describe these special roles; however, the concept is very similar to RBAC's use of "roles".

A common question is why groups, or the compartments of the Bell LaPadula model are not sufficient to handle roles. This question can be a bit deceptive because it seems reasonable to expect the group mechanism, perhaps with certain simple additions, to be capable of representing anything that role based access control can. However, from an efficiency standpoint, the complexity of the group representation becomes very high for all but simple role based cases. This makes them inefficient and cumbersome. Some researchers explain this inefficiency as a semantic mismatch between common organizational structures and the group mechanism.

Other examples of RBAC can also be advanced; however, for now it is sufficient to say that RBAC is starting to be seen as a more natural model of access control activity. This is happening in both the commercial and government sectors, civilian and military.

There is excitement in some quarters over the possibilities that RBAC offers. Unfortunately, there is also at this time no clear consensus as to what RBAC is and the debate continues at this time. There are several major issues and a host of lesser more detailed ones that must be tackled. Some of these issues are presented in what follows:

- **What is a role?** From the organizational standpoint roles can be modelled in terms of responsibility, authority and privilege. This part seems clear. Less clear is what the privilege actually means. Many researchers have assumed that privilege is a set of *authorized transactions* paired with each role. But how is a transaction to be defined? Should the transaction be bound to a specific object, class of objects, or even a wider data abstraction?
- **Access control or correctness?** Access control models have avoided the correctness issue by limiting their scope to the access control decision. The access control decision simply determines a subjects access to an object. What can be said when an access control is framed not as access to an object but as a high level transaction? Some researchers argue that there is nothing an access control model should say about a transaction's correctness. Other see advantage in using high level transactions. Indeed, some researchers suggest that formal considerations might even be set aside in favor of the "usefulness" provided by high level transactions.
- **How do we represent RBAC?** An emerging school uses object oriented techniques such as generalization, specialization, and class hierarchies to capture authority, delegation, and organizational chain of command. This is nicely captured by the theory of types. An open issue is how far to pursue the other capabilities offered by an object oriented characterization of RBAC.
- **The constraint problem.** One cannot go far without considering what part constraints should play in RBAC. Constraints are used to eliminate impossible, undesirable, or forbidden roles. For example a surgeon who is his own patient. This is an example of a static constraint. Constraints can also be temporal involving time. For example, enforcing separation of duties to prevent a user from

assuming dual roles<sup>1</sup> or a sequence of roles acquired over time that permit both access to accounting records and the ability to disperse funds. The open question for researchers is the scope and type of the constraints to include in a standard definition of RBAC.

These four issues represent some of the ongoing topics for which consensus is needed. RBAC promises to be a major access control model for new information systems and much work still needs to be done before a common understanding can be reached.

---

<sup>1</sup>Dual or parallel roles are part of another open issue concerning a standard model of computation for RBAC. Some researchers believe parallel roles are acceptable while others take the opposite view and limit a user to a single active role. Both approaches have consequences in terms of their ability to express certain types of valid user behavior.



## Role-Based Access Control Position Paper

Marshall D. Abrams, The MITRE Corporation,  
7525 Colshire Drive, McLean, VA 22102

Access control rules govern permitted modes of information sharing among entities. In general these rules compare the values of security attributes to determine if a proposed information access is permitted. Security attributes may be associated with initiator or recipient entities or with the context.

A position or role in an organization may be known to an information technology system. The system's access control rules define a set of privileges associated with that role. An administrative action identifies those users who may take on a role. In [1] we used the following definition:

*A role* is a set of allowed actions. A role allows selected users to apply specified operators to specified objects. A role is typically defined by a set of privileges and a corresponding group of users that are afforded these privileges.

A simple and safe approach for implementing roles is to restrict a person acting in a role to executing a well-defined set of role-support procedures needed to carry out the functions of that role. In some cases, an automated system's role-related actions may be completely characterized by such a set. Alternatively, the privileges granted to a role may be defined in the system's access control rules. Implicit in this, however, are constraints on which information objects an application or person can operate upon. Either way, role-related misuse of the system can be reduced by automated constraints; in the former case, they determine which users can execute given role-support procedures, and in the latter, they restrict the granting of privileges. The constraints need to be enforced by a reference validation mechanism.

A common challenge in designing roles is to ensure *separation of duty*. Certain actions are sufficiently vulnerable to abuse that no single user should have authorization to perform them. In this case, it is necessary to design distinct roles that ensure separation of functions among two or more individuals acting in these roles while retaining shared responsibility and accountability. Minimum and maximum elapsed time between the separate actions may be specified.

Separation of duty can be either static (being built directly into user role definitions) or dynamic (with access constraints based on the previous access history of the affected entities, as in [2]). The latter case introduces problems concerning "audit" records of previous accesses: How long are audit records retained? How are they managed in a distributed environment?

1. Abrams, M. D., September 1993, "Renewed Understanding Of Access Control Policies," *Proceeding 16th National Computer Security Conference*.
2. Brewer, D. F. C. and M. J. Nash, May 1989, "The Chinese Wall Security Policy," *Proceedings IEEE Computer Society Symposium on Security and Privacy*.

# ROLE-BASED ACCESS CONTROL

## A Position Statement

*Ravi S. Sandhu\**

ISSE Department, Mail Stop 4A4  
George Mason University, Fairfax, VA 22030  
sandhu@gmu.edu

Role-based access control (RBAC) is a good match for the security needs of many organizations. An individual's responsibility and authority in an organization derives from his or her job function(s). RBAC assigns privileges and users to roles. New users introduced to a role automatically acquire all privileges of that role. Similarly, new privileges assigned to a role are automatically granted to all members of the role. This is much more convenient and orderly than assigning privileges exclusively to users. There are corresponding advantages to RBAC when users, or privileges, are removed from a role.

The usual grouping mechanism of classical discretionary access control (DAC) can be used to implement roles. I have often been asked, "What is the difference between groups and roles?" The difference is fundamentally that between policy and mechanism. Roles are a policy component. All users in a role are presumed to be competent to carry out their job functions. Role-based authorization relates a job function to the information required to pursue that job activity. It embodies the principles of least privilege, need-to-know, need-to-do, competent-to-know and competent-to-do.

There are many dimensions to RBAC. RBAC can be extremely simple, much like the group mechanisms of typical operating systems in use today. On the other hand it can also be very complex embodying generalization and specialization hierarchies, such as found in object-oriented systems.

One question I wish to pose for the panel is, "What can the security community do to facilitate incorporation of RBAC in products?" The traditional response to this question would be to develop criteria with respect to which products can be evaluated. While evaluation criteria have their uses and benefits, I would urge caution in proceeding too far down this route. Criteria tend to simplify and rank order alternatives. Given the multi-dimensional nature of RBAC I would be reluctant to settle for a small number of linearly ranked RBAC alternatives, unless there is a strong scientific basis for a such a ranking.

My own answer to the question I have posed is twofold. Firstly, we need to continue theoretical analysis of RBAC and its variations. We should try to quantify the comparative expressive power of different versions of RBAC, and understand which policies are facilitated or hindered in these versions. Secondly, there should be experimental implementation of RBAC to better understand which aspects are easy to implement and which are cumbersome and costly. Implementations should, however, build to a rigorous (perhaps, even formal) model rather than the traditional ad hoc approach to construction of access control products.

Some other questions, and my personal responses, to them are given below.

1. Is RBAC just another fad? I do not think so, and hope others share my optimism.
2. How does RBAC relate to type-enforcement? I see RBAC as policy and type-enforcement as one mechanism. Type-enforcement can enforce some aspects of RBAC.
3. Is RBAC a panacea? No.

---

\*Ravi Sandhu is an Associate Professor and Associate Chairman of Information and Software Systems Engineering at George Mason University in Fairfax, VA.

© 1994 Ravi S. Sandhu

# Role-Based Access Control (RBAC) Position Statement

David Ferraiolo

National Institute of Standards and Technology

Today the best known U.S. computer security standard is the Trusted Computer Systems Evaluation Criteria (TCSEC). It contains security requirements, exclusively derived, engineered and rationalized based on DoD security policy. The TCSEC specifies two types of access controls: Discretionary Access Control (DAC) and Mandatory Access Control (MAC). DAC requirements have been perceived as being technically correct for commercial and civilian government security needs, as well as for single-level military systems. MAC is used for multi-level secure military systems, but its use in other applications is rare. NIST believes that there exists a third type of access control, referred to as Role-Based Access Control (RBAC), that can be more appropriate and central to the secure processing needs within industry and civilian government than that of DAC. Various forms of RBAC have been described and some are used in commercial systems today, but there is no formal standards encompassing RBAC. NIST is promoting research and development of a common approach at modeling and specifying RBAC, and the experimental implementation of protection mechanisms that can be practically and reliably transferred to existing computer and communications systems.

# INFERENCE PROBLEM IN SECURE DATABASE SYSTEMS

## Panel Moderator:

**Bhavani Thuraisingham**  
**The MITRE Corporation**

## Panelists:

**Donald Marks**  
**Department of Defense**

**Teresa Lunt**  
**SRI International**

**Thomas Hinke**  
**University of Alabama**

**Marie Collins**  
**The MITRE Corporation**

**Larry Kerschberg**  
**George Mason University**

## 1. INTRODUCTION

This is a panel on the inference problem in secure database systems which will focus on the practical developments over the past few years and provide directions for further work on this problem. It has brought together the leading researchers on this topic who will give their view points. In addition, a distinguished member of the database systems community will also serve on the panel so that the developments can be evaluated objectively.

This panel introductory paper, prepared by the panel moderator, will provide some background information on the inference problem and introduce the panelists. It is followed by the position papers by some of the panelists.

## 2. BACKGROUND ON THE INFERENCE PROBLEM

It is possible for users of any database management system to draw inferences from the information that they obtain from the databases. The inferred knowledge could depend only on the data obtained from the database system or it could depend on some prior knowledge possessed by the user in addition to the data obtained from the database system. The inference process can be harmful if the inferred knowledge is something that the user is not authorized to acquire. That is, a user acquiring information which he is not authorized to know has come to be known as the inference problem in database security.

We are particularly interested in the inference problem which occurs in a multilevel operating environment. In such an environment, the users are cleared at different security levels and they access a multilevel database where the data is classified at different security levels. The security levels may be assigned to the data depending on content, context, aggregation and time. It is generally assumed that the set of security levels form a partially ordered lattice with Unclassified <

Confidential < Secret < Top Secret. A multilevel secure database management system (MLS/DBMS) manages a multilevel database. An effective security policy for a MLS/DBMS should ensure that users only acquire the information at or below their level. However, providing a solution to the inference problem, where users issue multiple requests and consequently infer unauthorized information, is beyond the capability of currently available MLS/DBMSs.

During the past few years, extensive research and development activities have been conducted on the inference problem. In particular, research has proceeded in many directions. One is to process security constraints, which are rules that assign security levels to the data, during query, update, and database design operations so that certain types of inferences could be handled. Another is to use knowledge-based techniques (such as conceptual graph-based reasoning) to develop inference controllers which would act as advisors to the systems security officer (SSO). A third is to use knowledge discovery techniques for extracting information from the database and consequently prevent certain unauthorized inferences that could occur. The panel will address all three approaches to handle the inference problem.

### **3. THE PANELISTS AND THE ORGANIZATION OF THE PANEL**

Panel Chair: Bhavani Thuraisingham,  
The MITRE Corporation

Bhavani Thuraisingham has conducted research and development activities on secure database systems in general and on the inference problem in particular. Her contributions to the inference problem include security constraint processing, results on the unsolvability of the inference problem, the use of conceptual structures and knowledge-base management techniques, and a logic for multilevel data/knowledge base management systems. She is also conducting research on realtime database systems and massive database management at MITRE.

Panel Member: Donald Marks  
Department of Defense

Mr. Donald Marks is exploring the use of novel techniques for handling the inference problem. In particular, his work is focussing on the use of induction through knowledge discovery techniques. He is also conducting research on constraint processing and intrusion detection. He has published several papers on secure database systems.

Panel Member: Teresa Lunt  
SRI International

Teresa Lunt has conducted extensive research on the inference problem at SRI. Together with her colleagues at SRI, she has developed a tool for inference detection. She has also lead several landmark programs in computer security including SeaView multilevel secure database management system. She has published numerous papers and has chaired conferences in computer security.

Panel Member: Thomas Hinke  
University of Alabama

Thomas Hinke has a distinguished background in secure database systems. He was one of the principal contributors to a secure DBMS architecture called the Hinke-Schaefer architecture. He has also conducted research on the inference problem. In particular, he is exploring the use of knowledge engineering techniques and conceptual graphs.

Panel Member: Marie Collins  
The MITRE Corporation

Marie Collins has been conducting research and development activities on the inference problem at MITRE. Her earlier work was on the use of security constraint processing. She is now developing a tool for inference detection. She is also conducting research on secure transaction processing and has developed applications for database systems.

Panel Member: Larry Kerschberg  
George Mason University

Larry Kerschberg is a distinguished researcher in database systems and knowledge base systems. He has contributed extensively to intelligent database systems, and has published numerous papers on this topic. He serves on editorial boards of journals and has co-edited several books.

While the first four panelists will discuss their approaches to handle the inference problem, Larry Kerschberg will provide a general discussion of the important issues and his view on how the research should proceed. The total time allocated for the panel is 90 minutes. The panel chair will introduce the topic and the panelists. Then each of the panelists will describe their position on the inference problem and the tools they have developed. The total time allocated for the panelists is 50 minutes. The remaining 30 minutes will be a discussion session with the panelists taking questions from the audience.

# An Inference Paradigm

Donald G. Marks

Office of INFOSEC/Computer Science

Department of Defense

Ft. Meade, Md.

## *Abstract*

*This is a study about inference in automated information systems. It attempts to sharpen the understanding of what inference is, what it is not, how it can be used, and especially how it can be controlled. First, it is reasoned that a database can only control material implications, as specified in formal logic systems. Then queries, set theory and predicate calculus are shown to be equally sufficient tools for discovering such material implications. In particular, one set implies another if it is a subset of the second. Database queries or predicate calculus specify the properties of these sets of data and may be easily compared to determine these inferences. It is shown how this applies to human reasoning processes that abstract a concept from data and then apply some known rules to deduce another concept. Finally, a graph based model is developed that leads to the critical element determining an inference threat: can additional restrictions be placed on a dataset without eliminating some of the elements of the set? If so, the dataset has properties that have not been specified in the query and such sets may imply knowledge not evident in the query.*

## **1.0 Introduction**

Inference control has become a topic of considerable interest in secure database implementation. It is generally recognized that access to certain types of information enables the user to *infer* other information, even some that should not be available to them. Such inference does not take place magically, rather it is the integration of techniques applicable to databases and those utilized by humans in making abstractions, both of which are considered in this study. Database terminology is used throughout the paper, but similar arguments would hold for other data storage schemes.

Morgenstern was one of the first to investigate the inference problem for MLS/DBMSs [MORG87]. Since then, several efforts have been reported. One of the major approaches to handling the inference problem is to design the multilevel database in such a way that certain security violations are prevented (see for example the work of Binns [BINN92], Burns [BURN92], Hinke et. al. [HINK92], Garvey et. al. [GARV92], Smith [SMIT90], and Thuraisingham [THUR90]). That is, the security constraints, which are rules that assign security levels to the data, are processed during multilevel database design and subsequently the schemas are assigned appropriate security levels. Other proposed solutions focus on representing the multilevel database application using conceptual structures developed for knowledge-based system applications and subsequently reasoning about the application using deduction techniques (see for example [HINK92, GARV92, and THUR90]). Some proposals focus on developing tools which generate new relational database schemas given the original relational database schemas and the security constraints (see for example [BINN92]), and some others are proposing

the use of semantic data models developed for database design to design the multilevel database as well [BURN88].

The previous studies tended to be narrow in focus and proposals. That is, they propose solutions for specific examples of inference threats, or use specific techniques. It is time for a slightly broader view, both of the inference problem as well as the description of the solution. This study is also limited, of course, it does not address reasoning, or inference processes, occurring completely outside the database. It addresses the problem that occurs when a user is able to query the database, and, from the response, infer additional *database* information. The proposal is to enable the database to protect itself, not protect all knowledge possessed by anyone in the world.

As a general rule, *inference* control is concerned with protecting *knowledge*, not data. Knowledge is inferred from a quantity of data, or a set of data associated with attributes. Standard classification techniques are normally used to restrict the data that is critical to composing the knowledge. In this study, it is assumed that the data is stored in a relational database consisting of a single table. Each row in a table represents a specific instance of an entity associated with that table and is identified by a unique primary key. The column labels identify the attributes, or properties, of the entity. In a secure database context, preventing knowledge from being released requires preventing the release of both the data and the attributes in a manner where they can be associated into a sensitive conclusion. The numbers and/or letters in a database are meaningless until they are associated with an attribute. For example, the word "Washington" could be a person's name, a city, a state, or a codeword. Numbers are even less meaningful without knowing the applicable attribute. The ability to determine the attributes associated with the data, is the critical point of inference. A set of tuples and their attributes will allow inference if it is possible to assign new tuples to the given attributes, or new attributes to the given tuples. Either situation leads to new knowledge. These arguments may be put into a definition as:

*Definition of Database Inference:* Inference in a database is said to occur if, by retrieving a set of tuples  $\{T\}$  having attributes  $\{A\}$  from the database, it is possible to specify a set of tuples  $\{T'\}$ , having attributes  $\{A'\}$ , where  $\{T'\} \not\subseteq \{T\}$  or  $\{A'\} \neq \{A\}$ .

The definition may be stated as an *inference rule*: IF  $(\{T\}, \{A\})$  THEN  $(\{T'\}, \{A'\})$ , which may also be denoted as  $(\{T\}, \{A\}) \Rightarrow (\{T'\}, \{A'\})$ .

Suppose, however, that a user has access to information that is not stored in the database. Then it may be possible to retrieve a set of tuples  $\{T\}$  and the associated attributes  $\{A\}$  from the database and to reason, using data and attributes outside the database, to arrive at a set of tuples  $\{T'\}$  and attributes  $\{A'\}$  that are again within the database. That is, it is possible to form a *chain of reasoning*,  $(\{T\}, \{A\}) \Rightarrow (\{T_1\}, \{A_1\}) \Rightarrow (\{T_2\}, \{A_2\}), \Rightarrow \dots \Rightarrow (\{T'\}, \{A'\})$  where some of the tuples and/or some of the attributes are outside the database system. An automated system cannot deal with information not contained within the system. Therefore, if a chain of reasoning uses either data or attributes that are outside the database, it cannot be followed by the system. Fortunately, it is not necessary to actually follow such a chain of reasoning in order to control the inference threat. If the database system contains the endpoints of the chain  $(\{T\}, \{A\})$ ,



$(\{T'\},\{A'\})$ ) then there will exist what is referred to in logic systems as a *material implication* relating the two sets.

Material implications do not imply any causal relationships as may be present in a chain of reasoning. Material implications only require that the sets of data and attributes occur together, regardless of whether one causes the other, both are caused by a third activity, or they occur by coincidence. If A causes B, and is instantiated in the database, then  $A \Rightarrow B$  will certainly exist as a material implication. However, not all material implication rules will also be causality rules. Database systems are not a suitable mechanism for proving causality, they are limited to dealing with material implication rules. Knowledge-based systems may be used to analyse and control these causality rules ([HINK92],[THUR90]). However, in this case it becomes critical that *all* the applicable rules be included in the knowledge base. Such approaches are inherently limited, since it is generally not possible to determine what is known outside the database. The recognition of this ambiguity and the pervasive mindset of modeling causality rules seems to be the reason that the inference problem is regarded as unsolvable. Limiting the analysis to material implications between datasets offers far better control.

If a material implication exists such that  $(\{T\}, \{A\}) \Rightarrow (\{T'\}, \{A'\})$  where  $(\{T\}, \{A\})$  is classified Low and  $(\{T'\}, \{A'\})$  is classified High, then the database can offer no assurance that there does not exist some chain of inference, using outside knowledge, that can connect the two, enabling a "Low" user to infer "High" information. If, however,  $(\{T\}, \{A\}) \not\Rightarrow (\{T'\}, \{A'\})$  within the database, then it can be guaranteed that no chain of inference, using outside knowledge or not, exists which connects the two sets. That is, the absence of a material implication between two sets of data is *sufficient* to guarantee the absence of any chain of reasoning between these sets of data. It is not *necessary* for inference control, however, since material implications may be coincidental, and not related to any reasoning process. These arguments may be reduced to:

*Limitations on Database Inference:  $(\{T\},\{A\}) \Rightarrow (\{T'\},\{A'\})$  is an inference rule capable of being controlled by the database if and only if all the tuples in  $\{T\}$  and  $\{T'\}$  are in the database, and all the properties in  $\{A\}$  and  $\{A'\}$  are attributes in the database.*

Since automated systems are limited to reasoning only with the information available in the system, they form a *closed world*. Typically, a closed world is taken to mean that the database contains only true information, and all the true information. In our context, the closed world assumption means, not only that the data instances are complete, but also that the domain definitions are exact. The domain for an attribute  $A_i$  in relation R is therefore the projection of R onto  $A_i$ . The domain does not include "allowable" values for which there are no tuples. In order to control inference, it is required that the domain contain all the properties of *interest*. It need not contain all the properties pertaining to an entity, but it must contain all those found in the endpoints of any rules that need to be controlled.

The material implication approach is especially valuable for secure databases that allow "element level" labeling. In this case, individual data items may be classified High, and any tuple containing that data item must also be classified High. Element level labeling is not usually random, rather there is some rule defining when to classify elements in the database, and an entire set of individuals is classified. The inference con-

trol mechanism developed in this study will assume that such a rule exists and is common knowledge. For example, assume the job title "spy" is classified High. Any query accessing the set of "spies" (even without referring to, or retrieving *job title*) would be suspicious, since it must be assumed that the inquirer knows some rule (or some chain of reasoning) capable of assigning the job "spy" to each member of the set.

## 2.0 The Model

Rather than deal with all the intricacies of the relational data model, several assumptions will be made so that the ideas may be illustrated without becoming overly concerned with distracting details. A relation will be denoted  $R$ , and have attributes  $A_1, \dots, A_n$ . The domain of attribute  $A_i$  will be denoted by  $D_i$ . A tuple,  $t=(a_1, a_2, \dots, a_n)$ , in the relation has values for  $n$  attributes and is called an *n-tuple*. Each *n-tuple* is an element of the set  $D_1 \times D_2 \times \dots \times D_n$ .

Assume a relational database that conforms to the following restrictions:

1. A single relation
2. All attributes are directly or transitively functionally dependent upon a single key consisting of a single attribute.
3. Attribute values are unambiguous

The first assumption is not as restrictive as it appears. Many relational databases may be mapped into a "universal relation" database ([ULLM89]) which would meet these requirements. This study has chosen to concentrate on those processes that occur after transformation into a single relation rather than the mechanics of actually forming such a relation.

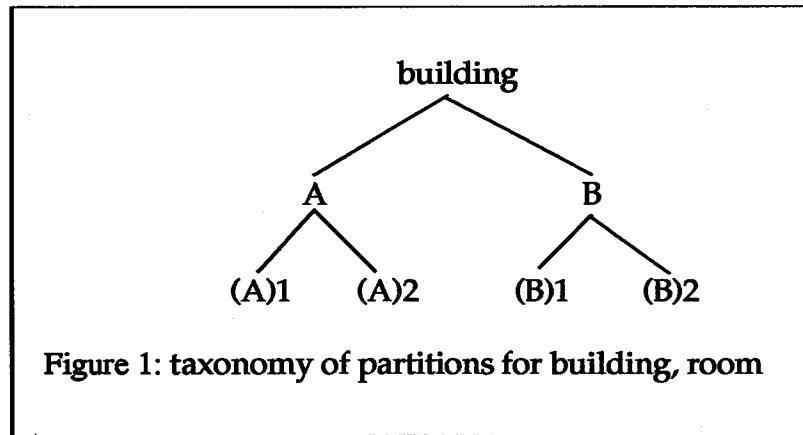
The second assumption implies that every non-key domain *partitions* the key domain. That is, each value of a non-key domain defines a set of key values. The sets thus formed for all the values of this non-key domain are disjoint, and their union covers the key domain. If a non-key domain includes null (unknown value) then it will form its own set of key values. If an attribute,  $A_i$ , is functionally dependant upon another attribute  $A_j$ , then by transitivity the domain for  $A_i$  partitions the set of key values defined for each value in the domain of  $A_j$ . The sets of key values therefore form a taxonomy. For example, consider a relation (name, building, room) in Figure 1. The attribute "name" is the primary key, and is partitioned by the attribute "building" into values A or B. Since the attribute "room" is functionally dependant upon "building" the names assigned to building A may be further partitioned among the rooms in A. Functional dependency also implies that room 1 in building A is different from room 1 in building B, so the values for the attribute "room" also partition the set of names.

*If there is a series of functional dependencies from attributes  $\{B_i\}$  to  $A$ ,  $(B_1 \rightarrow \dots \rightarrow B_i \rightarrow A)$ , the concatenation of attribute values  $b_1 \bullet b_2 \bullet \dots \bullet b_i \bullet a$  must partition the values for attribute  $B_1$ .*

The third assumption (non-ambiguity) arises when there are non-database restrictions on the values of attributes. An example might be a small college with two buildings, one for humanities classes, and one for science classes. Room 101 for a physics class is not the same as room 101 for an English class. The database system cannot deal with

this situation since the string of symbols "room 101" is ambiguous without a designator for "building". This requirement can be stated as:

*If, for some attribute A, which is not functionally dependant upon any attributes, there exist strings of symbols  $s_1, s_2$ , such that  $s_1, s_2 \in D(A)$  and  $s_1=s_2$ , then  $s_1$  and  $s_2$  refer to the same property.*



## 2.1 Inference from Data Sets

"Inference" must still be defined in such a system. We will start by adapting a strict set theory interpretation for the analysis and develop equivalent interpretations as necessary. A relation in a database can be regarded as a set of data where each tuple is an element of the set. Consider a subset of tuples from the relation that all share common properties. Under the closed world assumption, these properties are expressible as a set of database attributes. The *select* operator from relational algebra is therefore sufficient to express the conditions defining any subset of complete tuples from the relation. However, each tuple is itself a set, composed of individual elements also having properties definable as a set of database attributes. The properties of each partial tuple may be expressed by the *project* operator from relational algebra. Each tuple in a query response therefore satisfies two sets of properties, one set determines the rows, one set determines the columns.

A query "SELECT \* WHERE job=engineer" returns a set of complete tuples, each tuple having the property "job=engineer".

A query "SELECT name WHERE job=engineer" returns a set of partial tuples, each tuple having the properties "job=engineer" and "only name is present".

The description of database subsets may be formalized by the use of "predicates" and "predicate calculus". This will allow the translation of certain important results from that formal logic into database terminology. The definitions and terminology of predicate calculus may be found in many mathematical logic textbooks, for example [WOOD88]. Database sets, and later, inference, will be defined using the primitive notion of a "predicate". A "predicate" is a mapping of objects into a set. It is a logical function, operating upon one or more free variables, and evaluating to "true" if the

objects are in the set, to "false" otherwise. If  $P$  and  $Q$  are predicates,  $P(x)$  is the value "true" or "false" returned when  $P$  is applied to the element  $x$ .  $P$  will also denote the set of objects where the predicate  $P$  is true, i.e.,

$P \equiv \{x \mid P(x)\}$       the set of all  $x$  such that  $P(x)$  is true

$Q \equiv \{x \mid Q(x)\}$       the set of all  $x$  such that  $Q(x)$  is true

The predicate "engineer( $x$ )", for example, will evaluate to true whenever the person substituted for  $x$  is an engineer. The set of all engineers is then  $\{x \mid \text{engineer}(x)\}$ , where members are related by having the property "engineer". The predicate father( $x,y$ ) has two free variables, and will be true whenever the person substituted for  $x$  is the father of the person substituted for  $y$ , so  $\{(x,y) \mid \text{father}(x,y)\}$  is the set of all such pairs related by the predicate "father".

All queries of the database access *sets* of tuples (through the select and union commands), and then return a subset of that information (through the complement and project commands) to the user. Predicates may also be used to specify the properties of the set of data accessed from the database. Queries and predicates may therefore be regarded as equivalent means of specifying the data properties defining the referenced database sets and the operations performed on those sets. Predicates are limited to those equivalent to a query. It is therefore allowable to use either database methods on queries, predicate calculus methods on predicates, or set theory methods on sets of tuples to arrive at equivalent conclusions. Since inference is defined in predicate calculus, that definition will be translated into the other systems.

Inference in the predicate calculus system for predicates  $P$  and  $Q$ , is interpreted " $P$  implies  $Q$ ", (" $P(x) \Rightarrow Q(x)$ ") or "If  $P$  holds for  $x$  Then  $Q$  holds for  $x$ ". Usually,  $Q(x)$  is referred to as the "head" of the rule, while  $P(x)$  is referred to as the "body". This definition of inference can be translated into set theory by the following theorem.

**Theorem:** Let  $P(x)$  and  $Q(x)$  denote predicates and  $P(x)$  is instantiated in the database (i.e. there exists at least one tuple  $x$  such that  $P(x)$  is true), then  $P(x) \Rightarrow Q(x)$ , iff  $P \subseteq Q$ .

An informal proof goes as follows: The statement that predicate  $P$  holds for  $x$  is equivalent to stating that  $x$  is an element of set  $P$ .  $P(x) \Rightarrow Q(x)$  is therefore equivalent to  $(x \in P \Rightarrow x \in Q)$ . Semantically, this means that "if  $x$  is in  $P$  then  $x$  is in  $Q$ " or  $P \subseteq Q$ .

In this proof tuples are identified by their primary key in  $P$ . The attributes assigned to these key values may be different in  $Q$ . Obviously, if all attributes in  $P$  are in  $Q$  and  $P \subseteq Q$ , then if  $Q$  is totally disclosed,  $P$  is also totally disclosed. This is not the situation being considered here and such direct disclosure of  $P$  is not considered to be "inference". The predicates considered define a *set membership* of primary keys by listing the properties that tuples possess in order to belong to the set. Subsequent operations on retrieved sets are not of significance to inference. Thus inference is interpreted to deal only with the membership function. A tuple either has the properties specified by the query (or predicate), or it does not. It cannot be transformed so that it has those properties.

There is now a way of finding all possible inference channels in a database. Simply take the primary keys from each possible set of tuples and compare them to the pri-

many keys of all other sets of tuples, checking for set inclusion. By refining our concept of inference, and taking advantage of the database structure, however, this task can be considerably reduced.

## 2.2 Human Inference

Now that inference between datasets is defined, it needs to be evaluated to determine if it applies to processes by which humans make inferences. It is not intended to present a taxonomy of inference methods, many of which are addressed by the fields of statistics or psychology. Rather, a general method, applicable to database questions, will be presented.

When the subset inclusion definition of inference is examined, it is clear that the dataset *definitions* represent the knowledge that enables this mechanism to be used. The individual tuples in the sets are irrelevant, the fact they can be grouped together is crucial. Whenever tuples can be quantified, there is knowledge, not just data. The term concept will refer to the set of data along with its definition or attributes. Inference rules are expressed in terms relating these concepts.

The general form for inference is then given schematically in Figure 2. In this diagram, the data tuples are first aggregated into knowledge concepts (S1). Then a rule is applied, yielding the second knowledge concept (S2). If S2 is specific enough, the data tuples may be immediately listed. Otherwise, specific examples are necessary to move from (S2) to the desired data tuples.

**Example 1:** Suppose that your company gets a new project called "Manhattan". It is decided that the project name itself is not classified, but the names of people assigned to the project are classified. The company database classifies name and project together, but it is common knowledge (i.e. a known rule) that all nuclear engineers are assigned to "Manhattan". This establishes that the set of "nuclear engineer people" is a subset of the set of "Manhattan project people", so retrieval of the name of any nuclear engineer then gives the name of a person assigned to "Manhattan". In this case,  $D1 = \{(name, job)\}$ ,  $S1 = \{(name, nuclear\ engineer)\}$ ,  $S2 = \{name, nuclear\ engineer, Manhattan\}$ ,  $rule = \{(name, nuclear\ engineer) \Rightarrow (name, nuclear\ engineer, Manhattan)\}$ , and the classified concept is

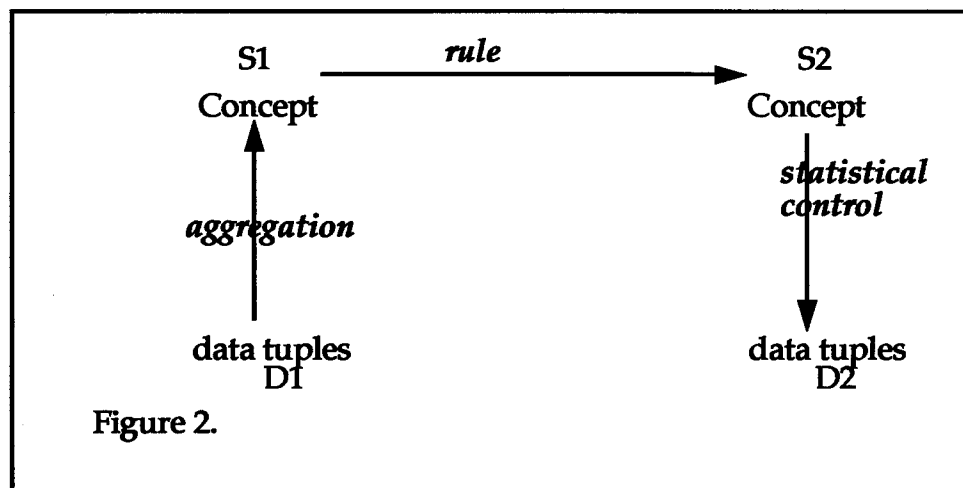


Figure 2.

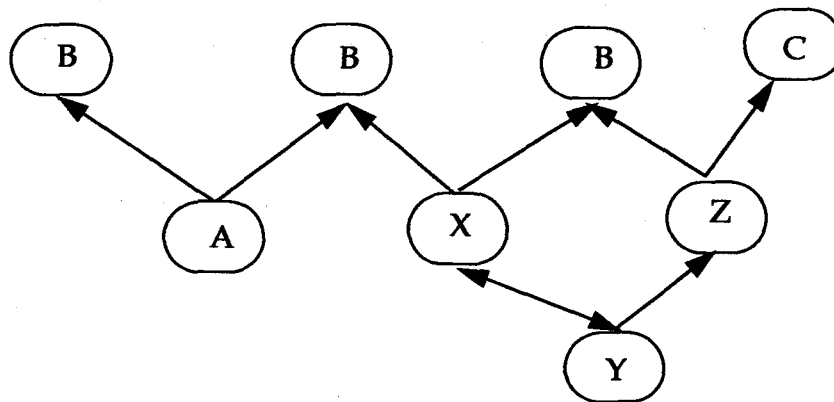


Figure 3. Directed paths in the lattice.  $A \Rightarrow B$ ,  $X \Rightarrow Y \Rightarrow Z \Rightarrow C$

$D2 = \{(name, Manhattan)\}$ . Regardless of the external knowledge of the rule, this type of potential inference problem may be discovered from the database since the names in (name, nuclear engineer) are a subset of the names in (name, Manhattan).

*Aggregation* and *statistical control* are interesting problems in their own right. Aggregation control refers to preventing the release of enough data tuples to create some knowledge (i.e. to define  $S1$ ). It may be permissible for the database to release some individual tuples, but not enough to allow the concept  $S1$  to be determined. Statistical control, on the other hand, is the dual of this process. Here, the concept may be released (i.e. the average value for the tuples), so long as the individual tuples cannot be compromised. This paper is too limited to develop these topics, so their study will be deferred until a later time.

### 2.3 Inference Control

Since inference is defined in terms of subset inclusion, the data sets may be organized into a graphical structure. Each node will represent a subset of data derivable by a query. Two nodes are connected with an arrow  $A \rightarrow B$ , if  $A$  is a subset of  $B$  (Figure 3). This will occur when one predicate (the parent) has more general requirements than the other predicate (the child). More tuples will satisfy the more general requirements, so the parent predicate will be a superset of the child predicate. Therefore, any predicate *implies* its parent concept. All remaining subset relations are then also marked with appropriate arrows. These additional downward pointing arrows can only occur if a parent is a subset of the child, that is, it has an "only\_child" so the parent and child contain identical tuples although their requirements for tuple membership differ.

It is not necessary to actually generate the graph since it is relatively easy to determine if two nodes are directly "related" via a series of parent-child relationships by using a partial order for the queries.

*Definition:* Node  $P_0$  will be "less than" node  $P_1$  ( $P_0 < P_1$ ) if  $P_0$  may be derived by applying an additional *select/project* query to  $P_1$ , regardless of the values in  $P_1$ .

For example, if  $P_1$  contains all values of *job*, while  $P_0$  specifies a specific job, say engineer, then  $P_0$  can be derived, via a *select*, from  $P_1$ . However, if  $P_1$  specifies a single

value for *job*,  $P_0$  must also specify that value (for a *select* query) or specify that the value is missing (for a *project* query), in order to be derivable from  $P_1$ . An *only\_child* relationship would occur if  $P_0$  does not specify a specific value for *job*, but there is only one *job*. Then  $P_0 \Rightarrow P_1$  but  $P_0 \not\prec P_1$ .

Certain pathological conditions requiring more extensive analysis can be avoided if it is assumed that nodes correspond to queries that have at least one specific attribute value. Such datasets are called *simple* datasets. It is now possible to state some properties useful for inference control from the graphical structure. The following theorem follows directly from our previous definitions of inference as subset inclusion, so no formal proof is given.

**Theorem 1:** Assume that  $P_0, P_1, \dots, P_n$  are nodes corresponding to simple datasets where  $P_i \Rightarrow P_{i+1}$ , for all  $i$ , but  $P_0 \not\prec P_n$ . Then there exists at least one link in the path of inferences between  $P_0$  and  $P_n$  that is from a parent to an *only\_child*.

*Therefore: Inference control for simple sets only requires checking for direct select/project transformations and control of nodes (aka subsets, predicates or query responses) having an only\_child.*

Example 1 above infers classified data for the scheme (name, job, project) because the concept (name, nuclear engineer, project) has only the single populated subconcept (i.e. an *only\_child*) of (name, nuclear engineer, Manhattan).

In order to derive sufficient conditions to analyse inference, it is necessary to formalize the notion that a concept can only be inferred by (1) one of its "children" or (2) from its parent if it is an *only\_child*.

**Theorem 2:** If A is a parent of B, where B is an *only\_child* of A, ( $A \Leftrightarrow B$ ), and X is the closest node such that  $X \Rightarrow A$ , and  $X \neq B$  (i.e. there does not exist a concept Y,  $Y \neq B$ , where  $X \Rightarrow Y \Rightarrow A$ ). Then A is an *only\_child* of X, ( $X \Leftrightarrow A$ ).

**Theorem 3:** If a concept  $P_0$  is retrieved from the database, such that  $P_0$  totally discloses  $P_i$  and  $P_i \Rightarrow P_k$ , then either  $P_i \prec P_k$  or  $P_i$  is an only ancestor of some  $P_j \prec P_k$ .

Pf:  $P_0 \Rightarrow P_k$  iff there is a directed path from  $P_0$  to  $P_k$  in the pattern lattice.

If  $P_0 \prec P_k$ , subset inclusion defines the path.

If  $\neg(P_0 \prec P_k)$ ,

by theorem 1, at least one of the links on this path must be from a parent node to an *only\_child*. Assume  $P_i \Rightarrow P_j$  is this link.

Then  $P_0 \Rightarrow \dots, P_{i-1} \Rightarrow P_i \Rightarrow P_j \Rightarrow \dots, P_k$ . By theorem 2,  $P_i$  must be an *only\_child* of  $P_{i-1}$ . Again apply theorem 2, since  $P_{i-1}$  now has an *only\_child*, and it is inferred by  $P_{i-2}$ , so  $P_{i-1}$  must be the *only\_child* of  $P_{i-2}$ . Repeatedly applying theorem 2 eventually yields the fact that  $P_0$  must have *only\_child*  $P_1$ , and hence is an *only\_ancestor* of  $P_j$ .  $\diamond$

### 3.0 Conclusions and Future Work

Theorem 3 gives a way of checking any query response to ensure that no inference is possible. First, compare the query to the restricted concepts. If tuples in the restricted concept are derivable from the query by means of a new *project/select* query,

there is an inference problem. If not, it is still necessary to check for the situation where more restrictions can be placed upon the query without reducing the number of members (this is the "only\_child" situation). All such derived concepts must then be checked against the restricted concepts to see if *they* are derivable by means of a *project/select* query.

The assumptions may be considerably relaxed without loss of correctness. However, such relaxation would require several "special cases" to be considered in the arguments. Such a detailed development is inappropriate for this forum, but will be available as a technical note in the near future. The follow-on study has developed a simple and reasonably efficient method to determine if one query is derivable (via *project/select*) from another query and will be explained in a later paper.

**Acknowledgments:** The author wishes to thank professors Ami Motro and Sushil Jajodia of George Mason University for their comments and stimulating discussion of this topic. In addition, the conference referees and Mr. Darrel Sell provided very helpful comments and editing assistance.

### References:

- [BINN92] Binns, L., August 1992, "Inference Through Secondary Path Analysis," *Proceedings of the 6th IFIP Working Conference in Database Security*, Vancouver, BC.
- [BURN92] Burns, R., October 1992, "A Conceptual Model for Multilevel Database Design", *Proceedings of the 5th Rome Laboratory Database Security Workshop*, Fredonia, NY.
- [BURN88] Burns, R., May 1988, "ER approach to multilevel database design", *Proceedings of the 1st RADC Database Security Workshop*, Menlo Park, CA.
- [GARV92] Garvey, T., et. al., August 1992, "Toward a tool to detect and eliminate inference problems", *Proceedings of the 6th IFIP Working Conference in Database Security*, Vancouver, BC.
- [HINK92] Hinke, T., and H. Delugach, August 1992, "AERIE, an inference modeling and detection approach for databases", *Proceedings of the 6th IFIP Working Conference in Database Systems*, Vancouver, BC.
- [MORG87] Morgenstern, M., May 1987, "Security and inference in multilevel database and knowledge base systems", *Proceedings of the ACM SIGMOD Conference*, San Francisco, CA.
- [SMIT90] Smith, G., May 1990, "Modeling security-relevant data semantics", *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA.
- [THUR90] Thuraingham, B.M., August 1990, "The use of conceptual structures in handling the inference problem", *Tech. Rep. M90-55*, The MITRE Corporation, Bedford, MA. (also published in the *Proc. of the 5th IFIP Database Security Conference*, 1991)
- [ULLM89] Ullman, J., *Principles of Database and Knowledge-Base Systems Volumes I and II*, Computer Science Press, Rockville, Md., 1988, 1989.
- [WOOD88] Woodcock, J., and Martin Loomes, *Software Engineering Mathematics*, Addison-Wesley, 1988.



# The Inference Problem: A Practical Solution\*

Teresa F. Lunt  
Computer Science Laboratory  
SRI International  
Menlo Park, California 94025

## 1 Introduction

The advent of commercially available trusted database systems introduces the capability to manage data at a variety of sensitivities and to enforce security policies that prohibit the unauthorized disclosure of information to unauthorized or insufficiently authorized individuals. With these products, data are labeled with their degree of sensitivity and protected accordingly. However, these products cannot protect data that is incorrectly labeled. One difficulty is that highly sensitive data may be inferred from data labeled lower<sup>1</sup>. In such cases an *inference problem* exists. An inferential link that may allow highly sensitive information to flow to a low user is termed an *inference channel* [1, 2]. It is the difficult task of the data designer to label the data so that the labels accurately reflect the actual sensitivity of the data and adequately protect the information from inference. The latter aim is extremely difficult for the human data designer to attain. SRI has developed an automated tool that can identify potential inference channels in a labeled database. DISSECT [3, 4, 5] (Database Inference System Security Tool) can be used interactively by a data designer to analyze candidate database schemas to assist in the detection and elimination of inconsistent labeling that can constitute inference problems. DISSECT uses *schema-level analysis* to avoid the costly task of data-level analysis with every database query.

DISSECT can detect both compositional inference channels and inference channels that involve type-overlap and near-key relationships. A potential *compositional inference channel* exists if two attributes are connected by a pair of paths consisting of composed foreign key relationships, where the two paths may have different sensitivities. A relationship can be inferred between any pair of entities that are connected by a sequence of foreign key relationships. If a table contains a foreign key to a second table, then there is a functional relationship from entities described by the first table to entities described by the second. A foreign key relationship from the second table to a third table implicitly defines a *composed* functional relationship from entities described by the first table to entities described by the third. If there is another sequence of foreign key relationships connecting the first and third tables, and accessing the two sequences may require different authorizations, there may be a compositional channel, since the two sequences of foreign key relationships may describe the same or a too closely related relationship between the first and third entities.

---

\*This research was supported by the United States Air Force, Rome Laboratory, and the Advanced Research Projects Agency under Contract F30602-91-C-0092.

<sup>1</sup>We use the terms "high" and "low" informally to refer to data that is more or less sensitive.

Compositional channels involve relationships that are explicitly defined in the database schema. The foreign key relationships that compose them are mappings from an attribute<sup>2</sup> of one relation to the primary key of another. The schema contains the information required to search for compositional channels, but the security of the database can still be compromised by more indirect methods. A foreign key relationship requires that the second attribute be a primary key and that every value of the first attribute be included among the values of the second. Foreign key relationships specify the join operations that the data designer intends the database user to perform. However, a user can join any pair of attributes that have values in common. Moreover, neither attribute need be a primary key. If one is a *near key*, joining on it can yield information about dependent attributes nearly as well as the primary key. DISSECT allows the data designer to declare information about attribute joinability and near keys to enable detection and elimination of the additional inference channels they allow.

Rather than require that the data designer state explicitly list every pair of attributes that are joinable, we allow him to associate *types* with attributes. Attributes whose types overlap are joinable. A *type-overlap* relationship occurs between two attributes when the two attributes have been declared to be of the same type and also have some overlap in the allowed sensitivity labels for data elements of that type. For example, there may be some overlap between attributes home-phone-number and office-phone-number, if they are both declared to be of type phone-number, and if elements of each may also match in sensitivity level. Intuitively, a type-overlap relationship is one which would allow the two attributes to be joined on matching data values and sensitivities. A potential inference problem exists if there is a pair of different-sensitivity paths between the same two entities, where the high path consists of a sequence of foreign key links, and the low path consists of both foreign key and type-overlap links. Intuitively, we are looking for ways a low user could use both declared foreign key relationships and fortuitous type-overlap relationships to compromise an explicit high relationship consisting of a sequence of one or more foreign key relationships. To allow DISSECT to discover inference channels that involve type-overlap relationships, the data designer must make type declarations for the attributes in the database. Inclusion of type-overlap relationships in DISSECT's detection algorithms allows DISSECT to detect inference problems caused by a user's *ad hoc* queries that the data designer might not have considered.

The detection of inference channels that involve type-overlap and near-key relationships require the data designer to make type declarations for the attributes in the database. The type declarations need not be complete; where the data designer has not made type declarations, DISSECT assumes nonoverlapping types.

In related work [6], Binns considered two attributes to be related if they had the same name. He created inference paths by concatenating such relationships. A potential problem was detected as a pair of such paths connecting the same end entities but having different security levels. Some problems with his approach are that (1) many spurious inference problems will be detected, since two attributes are not necessarily related or even joinable simply because they have the same name (his solution to this was to impose the unrealistic requirement that attribute names be unique across the database), and that (2) many relationships that could contribute to inference paths could go undetected, since attributes can be meaningfully joined even though they do not share the same name. Our type-overlap approach achieves the intent of Binns' approach (namely, of detecting problems that could not have been anticipated by the data designer), but will detect all and only

---

<sup>2</sup>For simplicity, we will discuss here only the case of relations among single attributes and not primary or foreign keys composed of multiple attributes.

those paths formed of meaningful relationships.

## References

- [1] T.D. Garvey, T.F. Lunt, and M.E. Stickel. Characterizing and reasoning about inference channels. *Proceedings of the Fourth RADC Workshop on Database Security*, Little Compton, Rhode Island, April 1991.
- [2] T.D. Garvey, T.F. Lunt, and M.E. Stickel. Abductive and approximate reasoning models for characterizing inference channels. *Proceedings of the Fourth Workshop on the Foundations of Computer Security*, Franconia, New Hampshire, June 1991.
- [3] X. Qian, M.E. Stickel, P.D. Karp, T.F. Lunt, and T.D. Garvey. Detection and elimination of inference channels in multilevel relational databases. *Proceedings of the 1993 IEEE Symposium on Research in Security and Privacy*, Oakland, California, May 1993.
- [4] M.E. Stickel, X. Qian, T.F. Lunt, and T.D. Garvey. *Inference Channel Detection and Elimination (Second Interim Report)*, Computer Science Laboratory, SRI International, Menlo Park, California September, 1993.
- [5] M.E. Stickel. Elimination of inference channels by optimal upgrading. *Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy*, Oakland, California, May 1994.
- [6] L.J. Binns. Inference through secondary path analysis. *Proceedings of the Sixth IFIP Working Conference on Database Security*, August, 1992.

# Security-Oriented Database Inference Detection\*

Thomas H. Hinke and Harry S. Delugach

Computer Science Department  
The University of Alabama in Huntsville  
Huntsville, AL 35899

## Abstract

This paper defines the database security inference problem and then characterizes it by the nature of the data used to detect inference vulnerabilities. The paper then describes an inference detection tool called Merlin and an inference benchmark database generation tool called Genie that have been developed at the University of Alabama in Huntsville (UAH). The paper concludes with a discussion of the deep knowledge problem inherent in security oriented database inference detection.

## 1 Introduction

A security inference vulnerability exists if a person can use accessible data to derive data that exceeds the person's access privileges. This becomes a database security inference problem if the data required to derive the unauthorized data is stored in a database. The primary research objective in security-oriented database inference is to develop methods to detect whether a database can be used by people to derive information whose sensitivity exceeds that of the data used to perform the inference.

## 2 Characterization of Inference Problem

One way to characterize the database security inference problem is by the nature of the data that must be used to detect a potential inference. We believe that this inference problem can be characterized by three levels of data:

**Schema-level data:** Using the data that describes what is in the database,

**Catalog-level data:** Using data that indicates, for example, that a particular type of part is used on a particular type of aircraft,

**Instance-level data:** Using data that indicates, for example, that specific part, serial number 12345876, was used on a specific aircraft serial number ADF7895.

---

\*This work was supported under Maryland Procurement Office Contract No. MDA904-92-C-5146.

One approach to schema-level inference detection is called the second path approach. This approach was developed by Hinke at TRW[Hin88, Hin90]. Second path inference detection has also been addressed by Binns[Bin92, Bin93] and SRI International[QSK<sup>+</sup>93] and continues at UAH under the AERIE database inference project which is addressing not only schema but also catalog and instance level inference detection [HD92, HDC93, HD93, DH92, DHC93].

An example of second path inference detection, presented at the recently concluded Workshop of Research Progress in MLS Relational Database Systems is shown in figure 1. The figure represents the relationships between various entities within a database system, with classified relationships indicated by dashed lines labeled HIGH and unclassified relationships indicated by solid lines labeled LOW.

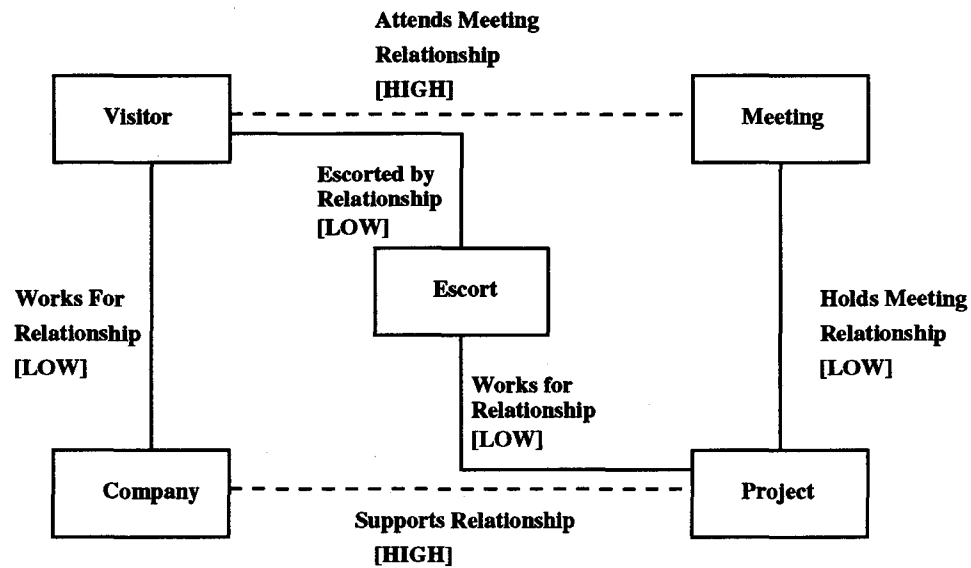


Figure 1: Company-Project Inference Using Escort

The classified data to be protected is the association between project and company. While the figure indicates the potential of making this association through a second path that uses the meeting attendee list, as noted this list has been classified and thus is not visible to the LOW adversary. However, the classified association between project and company provided by the LOW association between the escort's project and the visitor's company provides a LOW second path that permits this association to be made. This forms a second path between company and project.

### 3 Inference Research at UAH

The AERIE database inference project has developed an inference detection tool called Merlin which permits second paths to be detected within database schemas. Merlin uses a fast, path detection algorithm that identifies that a path exists between two attributes but does not have to find such a path to perform this detection[HD93]. Merlin then uses an algorithm, based on the attribute classification levels provided with the database schema to categorize the paths into those with varying levels of potential threat. This fast path detection algorithm is also being coupled to a path enumeration algorithm which will list the paths for those attribute pairs that have been identified as being connected with a second path.

Current work is underway to extend Merlin into catalog and instance data. This research is initially looking at data that has a transitive association such as provided by part-whole databases. This data could

be used to detect that that certain aircraft are based at certain locations using information on the shipment of parts unique to a particular type of aircraft to this location.

Another area of active research is to extend Merlin to include data relationships that do not have a functional relationship. Thus if an escort worked for more than one project or a part was used on more than one aircraft, Merlin could indicate the possible inferences with some indication of inference specificity. Thus, a part used on two aircraft would provide a higher degree of inference specificity than one used on all aircraft.

In addition to the development work on Merlin, the AERIE project is also developing a rule-based inference database generator that can be used to generate the catalog and instance-level data required to test inference detection tools. To ensure that the data provides a coherent inference picture, the Genie tool is structured around a microworld simulation in which database data is extracted at various points in the simulation.

## 4 Open Issues

The primary open issue in security-oriented database inference research is the fact that inference represents a deep knowledge problem. A potential adversary can be anticipated to be highly educated and intimately familiar with the domain of the data to be inferred. Any inference tool that hopes to be useful to protect against real adversaries will have to be able to possess sufficient depth of knowledge that it can counter its highly-knowledgeable adversary. This problem is especially acute at the catalog and instance levels of data.

One approach to addressing this problem is to encode huge amounts of data in a breadth-first approach. The Cyc project has undertaken such an approach, which includes the knowledge contained in a two volume desk encyclopedia along with all of the common knowledge that is required to understand the encyclopedia[LG88]. Even this effort was anticipated to involve many years of work. It is our opinion that even if a 30+ volume encyclopedia were used, this would not be sufficient since valuable inference information such as the parts used on various aircraft is not included in an encyclopedia.

The AERIE project has proposed an approach called inference directed microanalysis that focuses on the data within the database from a number of different perspectives, such as conventional database functional dependencies, part-whole relationships and used-for relationships to name but a few[HD93]. The results of this analysis are encoded in various facets within microanalyzed knowledge chunks<sup>1</sup>. Our research continues to assess the viability of this approach, however it is clear to us that such deep knowledge must be provided in some form if an inference detection tool is to protect against real adversaries at the catalog and instance-levels of data.

## References

- [Bin92] Leonard J. Binns. Inference through secondary path analysis. In *Proceedings of the Sixth IFIP 11.3 Working Conference on Database Security*. IFIP, August 1992.
- [Bin93] Leonard J. Binns. Implementation considerations for inference detection: Intended vs. actual classification. In *Proceedings of the IFIP WG 11.3 Seventh Annual Working conference on Database Security*. IFIP, September 1993.

---

<sup>1</sup>Formally called layered knowledge chunks

- [DH92] Harry S. Delugach and Thomas H. Hinke. Aerie: Database inference modeling and detection using conceptual graphs. In *Proc. 7th Annual Workshop on Conceptual Graphs*. New Mexico State University, July 1992.
- [DHC93] Harry S. Delugach, Thomas H. Hinke, and Asha Chandrasekhar. Applying conceptual graphs for inference detection using second path analysis. In *Proc. ICCS93, Intl. Conf. on Conceptual Structures*, pages 188–197, Laval University, Quebec City, Canada, Aug. 4-7 1993.
- [HD92] Thomas H. Hinke and Harry S. Delugach. Aerie: Database inference modeling and detection for databases. In *Proc. 6th IFIP WG 11.3 Working Conference on Database Security*, Aug. 19-21 1992.
- [HD93] Thomas H. Hinke and Harry S. Delugach. AERIE: Database Inference Modeling and Detection For Databases. In Bhavani M. Thuraisingham and Carl E. Landwehr, editors, *Databases Security, VI Status and Prospects: Results of the IFIP WG 11.3 Workshop on Database Security, Vancouver, Canada, 19-21 August, 1992*. Elsevier Science Publishers, 1993.
- [HDC93] Thomas H. Hinke, Harry S. Delugach, and Asha Chandrasekhar. Layered Knowledge Chunks for Database Inference. In *Proc. 7th IFIP WG 11.3 Working Conference on Database Security*, Lake Guntersville State Park Lodge, Alabama, Sept. 12-15 1993.
- [Hin88] Thomas H. Hinke. Inference aggregation detection in database management systems. In *Proceedings 1988 IEEE Symposium on Security and Privacy*, April 1988.
- [Hin90] Thomas H. Hinke. Database inference engine design approach. In Carl E. Landwehr, editor, *Database Security, II: Status and Prospects*. North-Holland, 1990. Results of the IFIP Working Group 11.3 Workshop on Database Security, October 1988.
- [LG88] Doug Lenat and R. V. Guha. The world according to cyc. MCC Technical Report ACA-AI-300-88, MCC, September 1988.
- [QSK+93] Xiaolei Qian, Mark E. Stickel, Peter D. Karp, Teresa F. Lunt, and Thomas D. Garvey. Detection and elimination of inference channels in multilevel relational database systems. In *Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy*, May 1993.

## **Key Escrowing: Today and Tomorrow**

Session Sponsor: Miles E. Smid, NIST

A key escrow system as defined in the Escrowed Encryption Standard (FIPS 185) entrusts two key components, which can be combined to form a unique key, to two escrow agents. Decryption of lawfully intercepted telecommunications may be achieved through the acquisition of a key component from each of the escrow agents. This session will describe how the U.S. Government's key escrow system works today and the improvements envisioned for the future. The full capability of key escrowing is being implemented in a series of development phases. The panelists will discuss the procedures necessary to program operational chips, to transport key components, to store key components, to release key components to authorized law enforcement agencies, and to perform lawful interception of telecommunications in both current and future phases.

### 1. Where We are Today Miles E. Smid      NIST

Mr. Smid will describe the current key escrow system along with the key players and their roles. The basic system components and their relationships will be introduced. Procedural and technical security features used to protect key components and other sensitive data will be presented. The problems that were encountered will be discussed.

### 2. The Target System Jan Manning      NSA

Mr. Manning will explain several new features planned for the current system. These features will provide for an increased operational capability and improved security. The target system will employ commercial off the shelf products, trusted operating systems, and INFOSEC devices to secure sensitive information.

### 3. Procedures for Lawful Interception of Telecommunications Mike Glimore      FBI

Supervisory Special Agent Gilmore will outline the procedures for obtaining a court order authorizing the interception of telecommunications data. He will also discuss the certification and confirmation sent to the escrow agents indicating that the court order has been granted. Typical controls on the use of recovered information and requirements for key destruction after authorized use will also be presented.

### 4. Future Considerations for Key Escrowing Dr. Dorothy Denning      Georgetown University

It is envisioned that key escrowing will evolve over time. Several issues still need to be resolved. For example, the export of escrowed encryption devices, the establishment of an international key escrow system, the balance between legal, procedural, and technical safeguards, and the use of key escrow with software cryptography. Professor Denning will explore possible solutions to these and other key escrowing issues.



## The Security Association Management Protocol (SAMP) Panel

A security association is an agreement between two or more entities that resolves all of the options (negotiable parameters) of the security mechanisms that perform security services for communication. There can be a security association between users, between encryption devices, between security protocols, between users and a combinations of security mechanisms. The association can be within the same security domain or between different domains. The security association manager will negotiate which algorithm, key, security mechanism, etc. will be used.

Currently, there are two major efforts to define the communication protocol for resolving a security association. The Security Association Management Protocol (SAMP) was started during the ISDN Security Program (ISP). SAMP is being developed under the ISP project by Motorola. The second protocol is the IEEE Key Management Protocol whose origin was the Secure Data Network System (SDNS) Key Management Protocol. The IEEE KMP is currently in draft 5 and uses the Generic Upper Layer Security (GULS) protocol for the security exchange. While both protocols are well along neither have been implemented.

This panel will attempt to address some of the questions, design considerations, and requirements for security associations. After short briefings by each of the panelists an open question and answer session involving the audience and panelists will occur.

Mike White (Booz-Allen & Hamilton) will speak on current work within the Secure Interoperable LAN Standard (SILS) IEEE 802.10C committee and the Key Management Protocol (KMP). Dave Wheeler (Motorola) will discuss the SAMP developed from the ISP program. Dale Walters (NIST) will describe current efforts to get the SAMP protocols adopted by the international community. Amy Reiss (NSA) will describe current research efforts to influence both of the protocols. Jim Leppek (Harris) will describe an implementation effort of SAMP and GULS based on the KMP.

## Other Panelists

Dale Walters  
NIST  
Gaithersburg, MD  
email: walters@osi.ncsl.nist.gov

David Wheeler  
Motorola  
email: David\_Wheeler-P26179@email.mot.com

Mike White  
Booz Allen & Hamilton  
Linthicum, MD  
email: whitem@asq8.bah.com  
phone: (410) 684-6677

Amy Reiss  
NSA  
Ft. Meade, MD  
email: abr@tycho.ncsc.mil  
phone: (301) 688-0849

Maj. Terry Hewitt  
NSA  
Ft. Meade, MD  
email: tgh@tycho.ncsc.mil  
phone: (301) 688-0849

James Leppek  
Harris Corporation  
Melbourne, FL  
email: jlepppek@harris.com  
voice: (407) 984-6476

The Secure Network Architecture Research Environment (SNARE) program is a study involving the implementation of a secure network/system management capability within the OSI framework. This capability is being pursued via the IEEE 802.10 and GULS ISO 11586 draft standards. We are also investigating the current state of ASN.1 and GDMO support for our security design.

The development platform consists of the ISODE and OSIMIS environments along with various other public domain (GNU) tools integrated into a no cost software testbed.

The following issues will also be addressed:

- standards accessibility
- development platform requirements
- draft standards and their interdependency
- Access Control and managed object attributes and operations

## Security Association Management Protocol (SAMP) Panel

### Panel Statement from Dave Wheeler, Motorola

As we experience continued growth in communications, we are also seeing an increasing demand for communication services, including security. We are also seeing growth in the applications and techniques of communications security. Any protocol which hopes to keep pace with this expansion must provide flexibility and expansibility of its services. And any protocol which does not provide some method for backward compatibility to existing systems, risks isolation from the already installed base of communications equipment. The SAMP used in the Secure Terminal Equipment (STE) project addresses the basic requirements of flexibility, expansibility, and backward compatibility. SAMP fulfills the requirement of flexibility by separating the protocol mechanics required to perform key and security management from the implementation specifics of key creation schemes, cryptographic algorithms, authentication techniques, and security protocols. This separation also provides expansibility, by allowing any type of exchange to be modelled through the services provided by SAMP. Backward compatibility to legacy systems can be provided through modelling the algorithms, security protocols, and other attributes of the legacy system using the SAMP services.

Without providing flexibility and expansibility, any protocol devised today will be obsolete tomorrow. Without providing some means for backwards compatibility, any new protocol isolates itself from current systems. If we do not build our protocols for flexibility, extensibility, and backwards compatibility, we will fail before we have even begun.

## **Panel Summary:**

### **Highlights of the New Security Paradigms '94 Workshop**

Eric Leighninger

The New Security Paradigms Workshop '94 is the third of a series of workshops which have been devoted to exploring new ways of viewing and thinking about computer security. New paradigms and models are needed to address resistant problems in policy formulation and specification, trusted systems integration, non-military trusted system modeling, and development of secure applications for open environments. These workshops have brought together computer security practitioners to discuss issues ranging from multipolicy models to uses of object-oriented methods to revision of traditional modes of designing and evaluating trusted systems.

This year's NCSC panel discussion will highlight the best papers of this year's workshop. The topics range from data and information semantics to use of fuzzy systems concepts for intrusion detection and auditing to security requirements for health care systems.

Essin and Lincoln address the security requirements of health care information systems. Electronic Medical Records (EMR) constitute a multipurpose database which due to temporal and dynamic factors requires application level interfaces which utilize indirectness of notation and which preserve atomicity, authenticity, and persistence of data. They present a candidate architecture to address such requirements.

Dobson argues for a theory of information and associated security perspective which is value and relevance-based. Information security can be seen to be a value-adding or value-protecting process in context of the objectives of the organization using the information.

Lin in his paper illustrates the use of fuzzy systems theory to auditing. By applying a "computer" version of a theorem of Weierstrass in mathematics the concept of repeatable patterns in audit data is formalized, and the subsequent concept of deep signatures as indicators of user behavior examined.

Spalka examines the semantics of security in database systems. The definition of confidentiality is reformulated to reflect varying degrees of information present regarding secrets. A generalized, formal semantics of the Simple Security Property and the \* -Property is derived using standard predicated logic.

# Formal Semantics of Confidentiality in Multilevel Logic Databases

Adrian Spalka

Department of Computer Science III, University of Bonn  
Römerstr. 164, D-53117 Bonn, Germany  
Fax: - 49 - 228 - 550 382, Email: adrian@cs.uni-bonn.de

## Abstract

*This paper presents a new formal approach to the definition of confidentiality in multilevel logic databases. We regard a multilevel secure database as an extension of an open database which preserves the database-semantics. We give four definitions of confidentiality which capture various degrees of information on secrets. Three of them are relevant in the presence of the Closed World Assumption. We present their formalisation within standard predicate logic and their interpretation for multilevel databases. From this viewpoint, the definitions lead to a formal semantics of the Simple-Security-Property and the \*-property. In particular, we demonstrate that the traditional interpretation of these properties represents just a special case of our formalism. The presented approach is theoretically sound and completely embodied in standard predicate logic.*

## 1 Introduction

In this section we give an informal definition of an ordinary and that of a multilevel logic database, we motivate our approach and, finally, discuss previous works and related approaches.

### 1.1 Overview

A state of the world as seen by a logic database (LDB) consists of facts, rules and general laws. The LDB maps a state of the world into a set of data and a set of integrity constraints. The LDB uses clauses for the uniform representation of data, constraints and queries. The symbols which can occur in a clause are stored in the LDB's signature. A LDB is valid if the data satisfy the integrity constraints, viz the data allow the derivation of the constraints.

In a multilevel state of the world, a set of security levels is assigned to each piece of information. According to Thuraisingham (1991), information in a multilevel state of the world is the knowledge of the truth value of a statement with respect to a particular security level. A multilevel database (MLDB) consists of two components: a database and a partially ordered classification scheme, where a set of security levels is assigned to each element of the signature, data item and integrity constraint. The classification in the multilevel database is assumed to correspond to the classification in the multilevel world. The handling of integrity constraints and the relationship of information at different levels are controversial issues; they are discussed in the next section.

A security policy regulates the access of processes to a MLDB. The security policy encountered most often is Bell and LaPadula's (BLP) interpretation of the mandatory access control, which is described in Landwehr (1981). BLP assigns a maximum security level to each process (or equivalently, the user on whose behalf the process executes) which is allowed to have access to the database. The security policy of BLP is formulated in terms of explicit primitive read- and write-operations, but its two most important properties are usually translated for MLDB in the following way:

- The Simple-Security-Property requires that a process is only allowed to select a data item if the process' security level is greater than or equal to the item's level.
- The \*-property requires that a process is only allowed to modify the database in such a way that for each data item involved in the modification, ie insert-, delete- or update-operation, the item's security level is greater than or equal to the process' level.

Without going into details, we only note that in order

to avoid some of its implications, the \*-property is often simplified to allow a modification only for data items which have the same security level as the acting process.

The Simple-Security-Property implicitly expresses a MLDB's confidentiality requirements. It is understood that an object must be kept secret from a user if the object's security level is greater than or incomparable with the user's level.

## 1.2 Rationale

The use of standard predicate logic for the description of databases has a number of widely accepted advantages. To us, the two most important ones are the unambiguous semantics and the uniform representation of data and constraints. The most important semantical task of an ordinary, open LDB is to watch over the validity of the data with respect to the constraints. This is obviously not the only task of a LDB, but if the constraints are removed from a database, then, in our opinion, this is no longer a database. It is rather an arbitrary set of data with some sophisticated methods which can answer queries and modify the contents of this set.

The original definition of BLP expresses the confidentiality requirements of a multilevel system through read- and write-operations. This is appropriate in a file- and record-orientated environment in which the only (direct or indirect)\* way to obtain the contents of a record or file is by reading it itself. This view assumes that if only non-confidential information is transmitted to a user, then the confidential information is kept secret from him.

The situation changes when we move to a logic-based environment. To *read* a clause from a set of clauses means:

- i) the clause is a member of the set
- ii) the clause is derivable from the set

Since a clause is derivable from itself, the read-operation should be replaced by the process of deriving a clause. Now it is possible that a user can gain knowledge of a clause even if it is not transmitted to him.

There is a second problem. In the original environment, the allowance and prohibition of a read-

---

Since the discovery of covert-channels we are aware that there are indirect ways to simulate a read-operation. The reason for their existence is a discrepancy between a theoretical model and its implementation. Thus covert-channels can be eliminated if this gap is closed.

operation are complementary actions, and the confidentiality of, eg, a record is based on this fact. It is kept secret if it cannot be read. For a clause, the properties of being or not being derivable from a set of clauses are not the only possible relationships between a clause and a set of clauses. Therefore the precise meaning of the statement 'A clause is secret if it is not derivable' is 'The secrecy of a clause is preserved in any other case except when it is derivable'. Does this match our intuition? We argue that it does not and that in a definition of confidentiality, it is necessary to name explicitly the relationship that must hold between a clause and a set of clauses.

Let us at last assume that such a definition of confidentiality is given. From the viewpoint of logic, the only difference between any set of clauses and a set forming a database state is that the former's contents may be arbitrary, while the latter's must satisfy some (static) integrity constraints. Thus, to affect a clause's derivability or confidentiality, or in the broadest sense, its relationship to the data of a state, it may no longer suffice to modify just these data. From now on we must take also the integrity constraints into consideration, eg whether they allow a particular modification of the data, or can they themselves be modified. We are in no case allowed to ignore the integrity constraints – they form an integral part of a database.

We can summarise the situation in logic databases as follows:

- The notion of reading a record is substituted by the notion of deriving a formula.
- Non-derivability of a clause is the weakest definition of confidentiality out of the possible ones.
- The derivability or confidentiality of a clause depends on the data of a state. The contents of a state are in turn fixed up to a degree of freedom which is determined by the integrity constraints.

In this light we think it incorrect to speak of a *fundamental conflict* between confidentiality and integrity. It is possible that the degree of freedom is insufficient to keep a particular secret, but can we simply assume that a secret can always be kept? As in real life itself, if there are some known boundary conditions which uniquely identify a thing, then it is useless to try to keep it secret.

The main objective of this paper is to give an interpretation of the BLP appropriate to multilevel logic databases.

## 1.3 Related work

The relevant works most often concentrate either on a

formal definition of confidentiality or a practical construction of multilevel relational databases.

According to Gougen/Meseguer (1984), a confidentiality requirement expresses that 'under certain conditions, certain individuals *should not* have access to certain information'. Its formalisation as non-interference is specifically intended to model trusted processes, but the authors also introduce a simple model of a multilevel-secure database in proof-theoretical view which has neither integrity constraints nor updates, and in which the Closed World Assumption<sup>†</sup> (CWA) is not made. In this context, they interpret non-interference as non-derivability.

Morgenstern (1987) notes that in order to keep a piece of information in a deductive database secret, it may not be sufficient to make it directly inaccessible. The author speaks of deductive databases in an informal manner and uses them mainly to accentuate some new problems which arise during the transition from relational databases.

Cuppens/Yazdanian (1991) extend a relational database with horn-clauses. Similar to Morgenstern (1987), the authors consider the inference problem. Rather than present a solution, they emphasise that logic is a suitable framework for the study of security problems in databases.

The first basic attempt of a formal treatment of confidentiality is presented in Thuraisingham (1991). The author's main idea is to formalise the multilevel security properties in NTML, a non-monotonic logic. Although this approach points to the right direction, NTML has been shown to be not sound.<sup>‡</sup>

The work of Bonatti/Kraus/Subrahmanian (1992) deals with the confidentiality of formulae in deductive databases. The authors interpret confidentiality as non-derivability. The formalism and results are based on a mixture of standard predicate and an extended modal logic. The database-model is very simple; it lacks the CWA, integrity constraints and update operations. Moreover, rather unrealistic assumptions on a user's own knowledge are made. Finally, no motivation is provided for the choices made in this approach, eg the unit of protection, the range of answers and the preference or necessity of modal logic in comparison to standard predicate logic.

Berson/Lunt (1987a) and Berson/Lunt (1987b) investigate the possibility of the application of the MAC-model to deductive databases. They point out many

new problems and suggest an approach to tackle them, but, due to the initial nature of these works, no solutions are offered.

Meadows/Jajodia (1987), Burns (1990) and Wiseman (1990) are examples of early approaches which consider a multilevel relational database in which primary key and foreign key constraints are the only classes of integrity constraints. Burns (1990) and Wiseman (1991) note that there is a fundamental conflict between secrecy and integrity, since each of them can only be enforced at the expense of the other.

Lunt/Millen (1989), Garvey/Lunt (1990) and Garvey/Lunt (1991) choose an approach which considers deductive databases as a special case of object-oriented databases. Although their motivation has its origins in deductive databases, the presentation is based on the terminology of object-oriented databases. Hence it is difficult to regard this approach as a contribution to a predicate-logic based theory of secure databases.

The handling of polyinstantiation has also received a lot of attention, eg in Jajodia/Sandhu (1990), Lunt (1990), Sandhu/Jajodia/Lunt (1990) and Lunt (1991). Many of the proposed solutions are of a syntactical character, thus each solution solves one problem while opening the way for another.

Denning et al (1988), Jajodia/Sandhu (1990) and Jajodia/Sandhu (1991) are three of the first papers which recognise that not every tuple in a multilevel relational database (ML-RDB) corresponds to a true fact in the real world. To exclude the unwanted tuples from a security level, they introduce the notion of a filter function. However, their definition does not prevent the database from violating integrity.

In the approach of Smith/Winslett (1992), a tuple is only believable to a user if both have the same security level. Since the authors speak of believability in an informal manner while trying to enforce a common set of integrity constraints for all security levels, they offer only a partial solution to the problems.

The most recent paper on ML-RDB is Qian (1994). The author considers a ML-RDB with a tuple-level classification and notes that integrity should be enforced at every security level only on those tuples which are believable at each particular level. She uses filtering functions to compute the non-conflicting information of two tuples. The value of such a function is defined through a table which, however, does not take the semantics of its parameters into account. Lastly, the author believes<sup>§</sup> that ML-RDB with gen-

\* Gougen/Meseguer (1984):75.

† cf Reiter (1978).

‡ cf Garvey et al (1992):160.

§ Qian (1994):213, line 15.



eral integrity constraints unavoidably introduce a random choice, ie a random semantics – a standpoint which in our opinion is definitely wrong.

## 2 Basic definitions

Following Gallaire/Minker/Nicholas (1984) and Cremers/Griefahn/Hinze (1993), we consider databases from the viewpoint of predicate logic. Thus the discussion and the results are also valid for relational databases in proof-theoretical representation. Some advantages and disadvantages from the security perspective of this approach are discussed eg in Michael et al (1992) and Stickel et al (1993).

### 2.1 Predicate logic

**Definition 1** A signature  $\Sigma$  is a pair  $\Sigma = (\mathbf{FS}, \mathbf{PS})$ . The set  $\mathbf{FS}$  contains ranked function symbols and  $\mathbf{PS}$  ranked predicate symbols. Both sets,  $\mathbf{FS}$  and  $\mathbf{PS}$ , are non-empty, finite and disjoint.

**Definition 2** The set of terms over the signature  $\Sigma$ ,  $\mathbf{TE}^\Sigma$ , is the smallest set with the following properties: each variable is a term; each constant, ie a function symbol of rank 0, is a term; let  $f$  be a function symbol of rank  $k$  and  $t_1, \dots, t_k$  terms, then  $f(t_1, \dots, t_k)$  is a term.

A term is ground if it does not contain any variable.

**Definition 3** Let  $r$  be a predicate symbol of rank  $k$  and  $t_1, \dots, t_k$  terms, then  $r(t_1, \dots, t_k)$  is an atomic formula, or simply an atom. An atom is ground if it comprises only ground terms. Let  $\alpha$  be an atomic formula, then  $\alpha$  is also a positive literal and  $\neg\alpha$  a negative literal. We denote the set of atomic formulae over  $\Sigma$  by  $\mathbf{AF}^\Sigma$  and the set of literals over  $\Sigma$  by  $\mathbf{LIT}^\Sigma$ .

**Definition 4** A clause is a formula of the form  $\alpha_1 \vee \dots \vee \alpha_m \leftarrow \beta_1 \wedge \dots \wedge \beta_n$ , in which all variables are assumed to be universally quantified. Each  $\alpha_i$  in the head of the clause is an atom and each  $\beta_j$  in its body a literal. A clause is ground if it comprises only ground atoms. A clause is normal if  $m=1$ , it is a query if  $m=0$ . A normal clause is called a rule if  $n \geq 1$ , it is called a fact if  $n=0$ . A clause is range-restricted if each of its variables occurs also in a positive literal in its body. We denote the set of all range-restricted clauses over  $\Sigma$  by  $\mathbf{CL}^\Sigma$  and its subset of normal clauses by  $\mathbf{NCL}^\Sigma$ . ■

We assume in this paper that all formulae are range-restricted clauses.

cf Reiter (1984).

**Definition 5** Let  $X \subseteq \mathbf{CL}$  be a set of clauses, then  $\mathbf{Th}(X) \subseteq \mathbf{CL}$  denotes all clauses which can be (logically) derived from  $X$  (for a clause  $\varphi$ ,  $\varphi \in \mathbf{Th}(X)$  is also denoted as  $X \vdash \varphi$ ). The set of all literals in  $\mathbf{Th}(X)$  is denoted by  $F(X)$ , ie  $F(X) = \mathbf{Th}(X) \upharpoonright_{\mathbf{LIT}}$ .

### 2.2 Logic databases

**Definition 6** A DDB-scheme  $DB$  is  $DB = (\Sigma, C)$ , where  $\Sigma = (\mathbf{FS}, \mathbf{PS})$  is a signature and  $C \subseteq \mathbf{CL}^\Sigma$  a set of static integrity constraints; the present state of  $DB$  is denoted as  $db = I$ , where  $I \subseteq \mathbf{NCL}^\Sigma$ . The closure of  $I$  under the Closed World Assumption is denoted as  $\bar{I}$ , ie  $F(\bar{I}) = F(I) \cup \{\neg\alpha \mid \alpha \in \mathbf{AF} \setminus F(I), \alpha \text{ ground}\}$ . A state  $db = I$  is always consistent, viz  $C \subseteq \mathbf{Th}(\bar{I})$  holds.

The following definition is only indirectly referred to in this paper. We include it to round up our framework.

**Definition 7** Let  $\chi(C)$  denote the set of all consistent data sets with regard to  $C$ , ie

$$\chi(C) = \{I \subseteq \mathbf{NCL} \mid C \subseteq \mathbf{Th}(\bar{I})\}$$

and let  $db = I$  be the present state of  $DB$ . From a declarative viewpoint, a transaction  $\tau$  is a set  $X \subseteq \mathbf{NCL}$ . From an operational viewpoint, a transaction  $\tau = (\delta, \iota)$  alters the set  $I$  into  $X \subseteq \mathbf{NCL}$ .  $\tau = (\delta, \iota)$  is completely characterised through two components: the set of facts deleted from  $I$ ,  $\delta$ , and the set of facts newly included into  $X$ ,  $\iota$ , ie  $\delta \cap \iota = \emptyset$  and  $F(I) \setminus \delta = F(X) \setminus \iota$ . If  $X \in \chi(C)$ , then  $\tau$  is accepted and  $db = X$  is the new state of  $DB$ . ■

Moreover, we assume that the only way to communicate with a DDB is through an interface with the following properties:

- DDB's response to the command LIST is a complete listing of  $\Sigma$ ,  $C$  and  $I$ .
- DDB's response to a query is:
  - Syntax error if the query is not a valid query in the language over  $\Sigma$ .
  - Otherwise, a possibly empty set of ground substitutions which define a subset of  $F(\bar{I})$ .
- DDB's response to a transaction  $\tau$  is:
  - Syntax error if  $\tau$  contains a clause which is not in  $\mathbf{NCL}^\Sigma$ .
  - Accepted if  $\tau \in T(C)$ .

- Rejected if  $\tau \notin T(C)$ .
- DDB's response to any other input is Unrecognised command.

### 2.3 Databases with users and rights

The database presented above is an open one because it cannot tell one user from another – it answers any query and follows any valid transaction in the same manner. A database must be able to recognise the users if it is expected to treat them differently. Therefore we add to our database a set  $P$  of all users or persons who have access to it. We also introduce for each user  $p \in P$  the following rights:

- $RS_p \subseteq CL^{\Sigma_p^*}$  determines the clauses a person may see as an element of  $I$  or  $C$ .
- $RD_p \subseteq RS_p$  determines the clauses a person is allowed to delete.
- $RI_p \subseteq CL^{\Sigma_p}$  determines the clauses a person is allowed to insert.

Now we have arrived at a database which recognises different users and is able to behave in accordance with the stated rights. We call it a database with rights.

### 2.4 Personal database profiles

Let  $DB$  be a database with the scheme  $DB = (\Sigma, C)$  and the state  $db = I$ . The application of  $RS$ , the right to see, to  $DB$  provides for each user  $p$  his profile  $DB_p$  with the scheme  $DB_p = (\Sigma_p, C_p)$  and the state  $db_p = I_p$ .

One of the requirements to the profile is that it satisfies the confidentiality requirements for the user  $p$ . But there is more than this. Our starting point has been an open database. Then we have added users and rights to it. If a user possesses all rights, then his profile is identical to the whole database. Otherwise, his profile is different from it. Should the database semantics of the whole database or of a profile be allowed to vary depending on the actual settings of the rights? We maintain that the desirable answer is in both cases 'No'. We would like to look on a profile as an independent open database which respects the va-

\* For the moment it suffices to know that the sets of symbols of  $\Sigma_p$ , the signature of  $p$ , are subsets of the respective sets of  $\Sigma$ . The motivation for the removal of a symbol from  $\Sigma_p$  is given later.

lidity of the whole database. Thus we must determine the relationships between the original database and a profile, and between profiles.

First of all we must require that  $DB$  should always be valid and that validity of a state  $db = I$  depends only on the constraints  $C$ , ie  $C \subseteq Th(\bar{I})$ .

Secondly, a state  $db_p = I_p$  of the profile  $DB_p$  should also be always valid, and since  $DB_p$  should behave as if it were an autonomous database, its validity must not depend on anything else but the constraints of  $DB_p = (\Sigma_p, C_p)$ . Thus we require that  $C_p \subseteq Th(\bar{I}_p)$ .

Thirdly, a user's transaction can never violate  $C_p$ , but since  $DB$  is the ultimate authority on integrity, it must not happen that a transaction violates  $C$ , ie  $C_p \subseteq Th(\bar{I}_p)$  and  $C \not\subseteq Th(\bar{I})$ . Formally this can be translated into the requirement

$$C_p \not\subseteq Th(\bar{I}_p) \vee C \subseteq Th(\bar{I})$$

or equivalently

$$C_p \subseteq Th(\bar{I}_p) \rightarrow C \subseteq Th(\bar{I})$$

This decision is also supported by the following points.

- The user  $p$  has been granted access to his profile on condition that he is trusted to have it. To us it seems judicious to provide him with an explanation for the acceptance as well as for a rejection of his actions.
- We have considerable doubt whether it makes sense at all to talk of a database from  $p$ 's point of view when the part seen by him exhibits random behaviour. We could then omit  $C_p$  completely from his profile, since he would never know if a decision made by  $C_p$  is not overruled by some *invisible* authority.
- The formalism the database is based on would be of no use for the determination of the risks of disclosure. At present the user's autonomous profile gives him no opportunity of finding out any properties of  $C$ . In the other case, the database would not have the slightest idea of the information which  $p$  already has deduced and will deduce from its behaviour.

Finally, we require that the validity of two profiles is independent from each other. This means that a valid transaction executed by one user may not invalidate the profile of another user. The formal interpretation depends on the relationship between the data of two profiles. They are obviously independent if they do not share any data. We later investigate the case when one is a subset of the other, which is usually consid-

ered to hold in multilevel databases.

All these considerations show that it no longer makes sense to ask if a database with rights is valid when we have the definition of validity of an open database in mind. We therefore give a new definition of the validity of a database with rights  $DB$ . We still say that  $DB$  is valid, if the state  $db = I$  is valid. But we say that  $DB$  is locally valid for a  $p \in P$  if  $DB_p$  is valid, or simply that  $DB$  is locally valid if it holds for all profiles, and we say that  $DB$  is globally valid if  $db = I$  is valid and  $DB$  is locally valid, ie all profiles are also valid.

In this light the notion of global validity of a database with rights seems to be the matching counterpart to the notion of validity of an open database.

### 3 Formal semantics of confidentiality

In this section we present a summary of the results of Spalka (1994). An object of protection in a logic database is either a symbol of the signature, an atomic formula, ie a fact, or a clause, ie a rule. However, atomic formulae play here a central role.

#### 3.1 Confidentiality of symbols

Symbols of the signature cannot be directly manipulated. A symbol is only a part of a clause. To keep a symbol secret from a user can thus only mean that:

- This symbol does not appear in any clause of the user's data or constraints.
- The database responds with 'I don't understand', viz *Syntax error*, to a query or transaction of the user if it comprises this symbol.

Both points are immediately linked to the signature of the user-profile. They can be satisfied when the secret symbol is removed from it. One should however keep in mind that the removal of just one symbol from the signature can reduce the language by a considerable number of clauses.

#### 3.2 Confidentiality of facts

Let  $\alpha$  be a fact,  $I$  a set of clauses and  $\alpha$  is derivable from  $I$ , ie  $\alpha \in Th(I)$ . Let us also assume that  $\alpha$  should be kept secret from the user  $p$  with regard to  $I$ . As long as  $p$  does not mention  $\alpha$ , its secrecy is preserved. But what should the database answer when the user asks

Does  $\alpha \in Th(I)$  hold?

There are (at least) five possibilities:

- i) Yes.

- ii) Maybe.

- iii) No.

- iv) I don't know.

- v) I don't understand.

The first answer tells the whole truth and obviously does not preserve secrecy. But which of the remaining four possibilities preserve secrecy? The second answer is not a lie, but it is also not the whole truth. The database admits that it knows the truth but it is not going to tell it. The 'No'-answer is a blunt lie. In the fourth case, the database admits to understand the question, but it pretends not to know the answer. Finally, in the last case, the database pretends not even to understand the question.

In general, each answer except 'Yes' is suitable to keep the secret. However, depending on the circumstances, an answer can be too *weak* in a particular situation. We see that there is no unequivocal definition of secrecy. Some things can be more secret than other.

Each of the five answers gives the user a different amount of information on the secret. With respect to the above-given five points, it is:

- i) positive definite

- ii) indefinite

- iii) negative definite

- iv) indeterminate

- v) no information

on the secret. Since the amount of information is gradually decreasing with each point, we can say that each answer represents a degree of confidentiality. We take the view that the decision on the real secrecy of a secret or on the amount of information about a secret which a user may acquire must be made by an application. Thus it is necessary to assign a degree of confidentiality to a confidentiality requirement. But first we translate the informal answers into formal expressions in the context of a logic database:

G0:  $\alpha \in Th(\bar{I})$

G1:  $\alpha \vee \alpha' \vee \alpha'' \vee \dots \in Th(\bar{I})$

G2:  $\alpha \notin Th(\bar{I})$

G3:  $\alpha \notin Th(\bar{I})$  and  $\neg\alpha \notin Th(\bar{I})$

G4:  $\alpha \notin AF$

A confidentiality requirement for an atomic formula is now a statement of the form ' $\alpha$  should be kept secret from  $p$  at the degree  $G$ ' where  $G$  is one of G1 to G4.

G1 is the only degree of which we can say that it does not allow the database to lie to conceal a secret. It only provides him with a weaker information than it

is capable of, but this information is still true. If we contemplate the possible consequences of a lie from a practical and ethical point of view, then it seems preferable to give imprecise rather than false information. This preference is also underlined by the effort needed to enforce G2, which may require the maintenance of a consistent set of lies.

Finally, we note that the traditional definition of confidentiality as non-derivability is equivalent to the G1-degree in our formalism.

### 3.3 Confidentiality of rules

In principle, it would be possible to define the confidentiality of a clause in the same way as for an atomic formula. We believe that this is inappropriate. In our opinion, a reason for keeping a rule confidential is that it is used to derive confidential data. To give an example, let  $s(X) \leftarrow r(X)$  be a confidential rule and  $r(a)$  a fact. Then  $s(a)$  should also be kept secret.

We thus say that the requirement to keep a rule confidential, means that:

- i) This rule is not among the stored data or integrity constraints.
- ii) The data which can be derived by this rule should also be kept secret.

Since a fact is a rule with an empty body, this definition is a proper extension of the definition of confidentiality of a fact.

## 4 Confidentiality in multilevel databases

This section discusses the adaptation of BLP based on the MAC-model to multilevel logic databases.

### 4.1 The MAC-model

The MAC-model can be defined as

$$M_{MAC} = (O, S, SG, L)$$

$O$  is a set of objects, ie units of protection. The set  $S$  contains subjects which represent users that work with the objects.  $SG$  is a partially ordered set\* the elements of which are interpreted as security levels.  $L: S \cup O \rightarrow SG$  is a function which places a security mark on every subject and object. The value of  $L(o)$ ,  $o \in O$ , is interpreted as the object's degree of confidentiality, and the value of  $L(s)$ ,  $s \in S$ , as the subject's degree of trustworthiness.

\* Some authors define  $SG$  as a lattice.

The MAC-model is assumed to satisfy two properties. The Simple-Security-Property states for a file-orientated environment that  $L(s) \geq L(o)$  is necessary and sufficient in order that  $s$  may read  $o$ , and it is understood that any object which  $s$  may not read must be kept secret from him. The \*-property states that  $L(o) \geq L(s)$  is necessary and sufficient in order that  $s$  may create or write  $o$ .

Now we give an interpretation of the MAC-model for logic databases.

The objects of  $O$  are identified with

- symbols of the signature
- facts
- clauses

The subjects of  $S$  are identified with the users in  $P$  and the database commands.  $SG$  and  $L$  are adopted as new components of  $DB$ . The interpretation of the two properties depends on the object. Before we go into details, let us take a look at the original intention of both properties.

#### 4.1.1 The Simple-Security-Property

The function  $L$  enables us to relate an object and a subject. The Simple-Security-Property uses this relationship to express two points. Firstly, the property itself is the following implicit, generic confidentiality requirement: an object  $o$  should be kept secret from a subject  $s$ , if  $L(s) \geq L(o)$  does not hold. Secondly, this property shows us how to satisfy this confidentiality requirement in a file-orientated environment: if  $o$  should be kept secret from  $s$ , then  $s$  should not be given read-access to  $o$ .

In its original definition, both points are merged into one statement. This is appropriate for a file-orientated environment, but for a logic database we must consider both points separately.

#### 4.1.2 The \*-property

A subject can actively or passively acquire knowledge either by executing read-operations or by waiting until other subjects execute write-operations which are addressed to him. The Simple-Security-Property is concerned with the first case. The \*-property worries about other subjects' write-operations. Is this really something we need to worry about in a model?

The \*-property limits a user's ability to perform modifications of a system. It prevents him from modifying an object the security level of which is lower than his own. This restriction is hard to understand

when we keep in mind that a user is only assigned a specific security level if he is trusted to behave properly. Since the \*-property does not state anything about a user's trustworthiness, we must try to give a different interpretation to it.

If this property is concerned about a situation in which a user may be misled to use an untrustworthy command which pretends to be trustworthy, then it can be safely abandoned if the implementation of the commands can be trusted. In this case the \*-property does not belong to the model, but is rather an implementation requirement. If, on the other hand, its intention is that a system itself may not *write-down* any information not approved of by the Simple-Security-Property while it is processing a read-operation, then it is evidently not concerned about the possibility that the system will deliberately and intentionally violate the Simple-Security-Property. In our opinion, explicit modifications which violate the \*-property should be admissible on account of their implied trustworthiness.

To us the \*-property has only one meaningful interpretation: if two subjects, who may be users or commands, are able to communicate with each other, then a communication must be conducted in such a way that neither party will be provided with any *implicit* knowledge on information which should be kept secret from it and which is visible to the other party. If both subjects are users, then we can do nothing but to rely on their trustworthiness. If on the other hand a user is communicating with a database, then we must establish instructions for its behaviour. Yet in both cases we are forced to define the kind of implicit knowledge which may not be written down.

We advocate to choose an interpretation for the \*-property which agrees to the assumptions about a subject's trustworthiness expressed by the function  $L$ . In particular, we do not regard the \*-property as a restriction on explicit modifications, but only as a requirement to confine specific kinds of implicit information transfers.

In this light, in a theoretical model the \*-property is subsumed by our interpretation of the Simple-Security-Property, since the kind or degree of information which a subject is allowed to have on a secret can be expressed within a confidentiality requirement in our formalism.

## 4.2 Confidential symbols

When symbols of the signature are objects of protection, the situation resembles very much that in a file-

orientated environment.

Let  $a$  and  $b$  be two symbols and  $ph$  and  $pl$  two users such that  $L(ph) > L(pl)$ ,  $L(pl) = L(a)$  and  $L(ph) = L(b)$ . The signature of  $ph$  comprises both  $a$  and  $b$ , while according to section 3.1,  $b$  is not an element of  $pl$ 's signature.

Thus for the users  $ph$  and  $pl$ , the Simple-Security-Property induces an inclusion-relation on their signatures.

## 4.3 Confidential facts

Let  $ph$  and  $pl$  be two users with their database profiles  $DB_{ph}$  and  $DB_{pl}$  so that  $L(ph) > L(pl)$ . Let moreover  $\alpha$  be a fact from the data of the state  $db_{ph} = I_{ph}$  and  $L(ph) = L(\alpha)$ . The Simple-Security-Property tells us that  $\alpha$  should be kept secret from  $pl$  with regard to  $DB_{pl}$ . In section 3.2 we have shown that this requirement must be qualified with a degree of confidentiality, which can be G1, G2, G3 or G4.

### 4.3.1 G1

This weakest confidentiality-degree allows  $pl$  to have indefinite information on  $\alpha$ . Let us consider the following example. Let

$$\Sigma = (\mathbf{FS} = \{a\}, \mathbf{PS} = \{q, r, s\})$$

$$C = \{q(X) \vee r(X) \leftarrow s(X)\}$$

be a LDB-scheme visible to the user  $pl$ . Let moreover  $F(I_{ph}) = \{r(a), s(a)\}$ , and  $r(a)$  should be kept secret from  $pl$  at G1-degree.  $pl$  must not be able to derive  $r(a)$ . Thus we reduce  $pl$ 's set of positive data to  $F(I_{pl}) = \{s(a)\}$ . Now the trouble is that  $I_{pl}$  does not satisfy  $C$ , and we owe the user an explanation. We suggest to tell him that his profile is weakly consistent, that is:

- the integrity constraints in  $C$  are always satisfied by the data in  $db = I$
- his data may seem to violate  $C$  due to some secrets

Now the user is able to identify the violated constraint, and through a simple substitution he can find out that  $q(a) \vee r(a) \in Th(I)$  holds, viz either  $q(a)$  or  $r(a)$  true. Maybe  $r(a)$  is true, or maybe not. ■

We see that the interpretation of G1 in a LDB involves some interactions and new conventions. The general enforcement of G1 is based on the following method. Firstly, reduce the data in a user's profile so

that he can not derive the secret fact from it. Secondly, observe how the reduction affects the user's integrity constraints. If all constraints are satisfied, then the user cannot use them to derive any further information. If a constraint is violated, then all we can do is hope that it is an indefinite clause, viz it will only tell the user that a disjunction of some facts is true. However, if this constraint is a definite clause, then G1 cannot be enforced – in our opinion, in this case it simply does not make sense to require that this fact should be kept secret at G1-degree.

Since G1-requirements only reduce the data of a profile but do not introduce any data, the data of a profile are always a subset of the global database's data. For our users  $ph$  and  $pl$ , the Simple-Security-Property induces an inclusion-relation on their positive data, ie facts:

$$Th(I_{pl}) \subseteq Th(I_{ph}).$$

Does the same relationship also hold for their sets of integrity constraints? The answer is a definite 'No'. The properties of  $Th$  as a hull-operator, the validity of a profile and the subset relation on the sets of data yield only the following inclusions:

$$C_{pl} \subseteq Th(\bar{I}_{pl})$$

$$C_{pl} \subseteq Th(\bar{I}_{ph})$$

$$C_{ph} \subseteq Th(\bar{I}_{ph})$$

The relationship  $C_{pl} \subseteq C_{ph}$ , or more general  $Th(C_{pl}) \subseteq Th(C_{ph})$ , does not follow from the above inclusions. In our opinion, to state it as a requirement would only limit the database's expressiveness.

We believe that integrity constraints must only satisfy the semantics-preserving properties of a personal database profile.<sup>\*</sup> Here the independence of the profiles of  $pl$  and  $ph$  has two consequences. Firstly, the construction of  $C_{pl}$  and  $C_{ph}$  must ensure that  $pl$ 's valid transactions do not invalidate  $ph$ 's profile. Secondly, the transactions of  $ph$  are guaranteed to respect the validity of  $pl$ 's profile if they only affect data of his own level. However, based on  $ph$ 's trustworthiness, he can be allowed to execute any transaction which leads even to a weakly consistent profile of  $pl$  as long as no secret fact at G1-degree is disclosed.

#### 4.3.2 G2

Let  $\alpha$  be a fact which should be kept secret from the user  $pl$  at G2-degree. The database is required to en-

<sup>\*</sup> cf section 2.4.

sure that:

$$i) \alpha \notin Th(\bar{I}_{pl})$$

$$ii) C_{pl} \subseteq Th(\bar{I}_{pl})$$

The difference between G1 and G2 is that G1 allows a profile to become weakly consistent, whereas G2 does not. This is necessary in order to avoid the derivation of any information which cannot be derived from  $I_{pl}$ , ie the database must always answer with a convincing 'No'. Let us consider a variant of the example of the previous section.

$$\Sigma = (\mathbf{FS} = \{a\}, \mathbf{PS} = \{q, r, s\})$$

$$C = \{q(X) \vee r(X) \leftarrow s(X)\}$$

$$F(I) = \{r(a), s(a)\}$$

We require that  $r(a)$  should be kept secret from  $pl$  at G2-degree. Now we are not allowed to set  $F(I_{pl}) = \{s(a)\}$  since this gives  $pl$  indefinite information on the secret.

We see that there are two reasons for weak consistency:

- the secret  $r(a)$  is not derivable from  $I_{pl}$
- $q(a)$ , which is not secret, is not present  $F(I)$ .

Consequently there are two ways to make  $pl$ 's profile consistent:

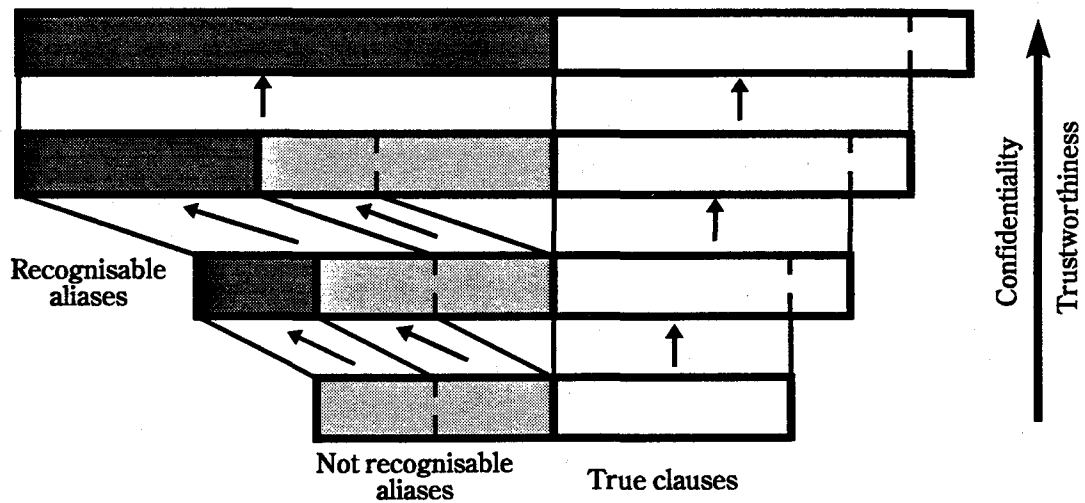
- Show  $pl$  the secret, viz insert  $r(a)$  into  $I_{pl}$
- Insert something else into  $I_{pl}$  which makes it consistent, ie insert  $q(a)$ .

This example shows that  $q(a)$  represents from the database's viewpoint a plausible lie for  $r(a)$ , ie it may serve as a cover story<sup>†</sup> for a secret fact. We say that  $q(a)$  is an alias for  $r(a)$ . In general, each fact from the violated constraint's head except the secret is a plausible lie.<sup>‡</sup> However, if this constraint is a definite clause, then it offers no aliases for the secret. In this case the constraint uniquely identifies the secret, and confidentiality at G2-degree cannot be enforced.

Since the alias is a member of  $F(I_{pl})$  but not of  $F(I)$ ,  $F(I_{pl})$  is no longer a subset of  $F(I)$ . For our users  $ph$  and  $pl$ , the Simple-Security-Property does not

<sup>†</sup> cf Garvey/Lunt (1991).

<sup>‡</sup> Brüggemann (1993) aptly points out that a good cover story is also expected to play down the covered secret as far as possible. Thus it would be advisable to measure the quality of a cover story with respect to a secret. Although we do not do it in this paper, our database can use some special predicates to express it, eg as an order on the possible plausible lies.



imply an inclusion of the sets of integrity constraints for the same reasons as for G1. Moreover, it can be no longer interpreted even as an inclusion on the sets of their data because G2-requirements may lead to a deliberate inclusion of false information into a user's profile. G2 provides a higher degree of confidentiality than G1, but aliases do not come without problems.

The next example motivates the interpretation of the Simple-Security-Property for G2-degree. Let us assume that the fact  $\alpha$  must be kept secret from  $pl$  and that G2-secrecy can only be enforced if the alias  $\beta$  is inserted for  $\alpha$  in  $pl$ 's data.  $pl$  cannot recognise  $\beta$  as an alias (it is placed in the light grey zone in the diagram above). Let us assume that  $\alpha$  is not secret to the user  $ph$  (it is located in his white zone). Now  $ph$  sees two different facts, which represent two different names for the same fact. How can  $ph$  recognise which of them is the true one, and which is an alias? If  $ph$  is considered trustworthy to see the truth, he must not be confused by false aliases.

We see that an alias inserted for a user at a low level can disturb the profile of a user at a higher level. Thus we must provide for the possibility to *move* an alias from the light grey into the dark grey zone, viz out of the profile's data.

For a user  $p$ , the set of facts  $\alpha$  which satisfy the condition  $L(p) \geq L(\alpha)$  can be partitioned into three subsets:

- i) true facts
- ii) aliases which are not recognisable as such at  $p$ 's security level  $L(p)$
- iii) recognisable aliases at  $L(p)$

Thus for G2-degree the Simple-Security-Property induces between two users with adjacent security levels an inclusion-relation on the true facts and on the ali-

ases which are not recognisable at both levels. For users with any two comparable security levels, the inclusion-relation holds only on the true facts.

#### 4.3.3 G3

A confidentiality requirement at G3-degree can be expressed in standard predicate logic. However, it is trivially not satisfiable in databases in which the Closed World Assumption is made. It tells us that for each atom  $\alpha$ , either  $\alpha$  or its negation  $\neg\alpha$  is derivable. This obviously contradicts the formal G3-requirement.

#### 4.3.4 G4

G4 is the strongest degree of confidentiality. It requires a database to give a user no information on a secret. According to section 3.2, this means that  $\alpha$  is not a valid fact in the user profile's language, ie

$$\alpha \notin AF^{\Sigma, \mu}$$

The only way to achieve it is to remove at least one symbol from the user's signature which he would need to construct the confidential fact. We see that confidentiality of facts at G4-degree can be reduced to confidentiality of symbols.

### 4.4 Confidential rules

The definition of confidentiality of a rule reduced to the rule itself requires that the rule should be neither an element of the data nor of the integrity constraints. Here further investigation is necessary in order to find out when and how this can be done without violating the database semantics.

## 5 Conclusion

In this paper we have presented a new approach to the definition of confidentiality in multilevel logic databases. An open deductive database has served as our starting point. With the introduction of users and rights we have defined the notion of global consistency and that of a personal database profile.

We have shown that secrecy has no unique meaning. We have given four possible definitions of secrecy, G1 to G4, which have been motivated by real-life situations. They correspond to the information which is contained in the informal answers 'Maybe', 'No', 'Don't know' and 'Don't understand', that is, they capture the various degrees of implicit information which a user may obtain on a secret. All definitions have been formalised within standard predicate logic. Three of them, G1 for indefinite, G2 for negative, and G4 for no information on secrets, are relevant in the presence of the Closed World Assumption. From the viewpoint of multilevel security, G1 to G4 provide a formal semantics of the Simple-Security-Property and the \*-property. In particular we have demonstrated that the traditional interpretation of these properties represents just a special case of our formalism. The presented approach is theoretically sound and completely embodied in standard predicate logic.

## References

Berson/Lunt (1987a)

Berson, Thomas A., and Teresa F. Lunt. 'Security Considerations for Knowledge-Based Systems'. *Third Expert Systems in Government Conference*. Reprint. 1987.

Berson/Lunt (1987b)

Berson, Thomas A., and Teresa F. Lunt. 'Multi-level Security for Knowledge-Based Systems'. *1987 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, 1987. pp 235-242.

Bonatti/Kraus/Subrahmanian (1992)

Bonatti, Piero, Sarit Kraus, and V. S. Subrahmanian. 'Declarative Foundations of Secure Deductive Databases'. Ed Joachim Biskup, and Richard Hull. *4th International Conference on Database Theory - ICDT'92*. LNCS vol 646. Berlin, Heidelberg: Springer-Verlag, 1992. pp 391-406.

Brüggemann (1993)

Brüggemann, Hans Hermann. *Private communication*. Hildesheim, 1993.

Burns (1990)

Burns, Rae K. 'Integrity and Secrecy: Fundamen-

tal Conflicts in the Database Environment'. Ed Bhavani Thuraisingham. *3rd RADC Database Security Workshop 1990*. Bedford, Massachusetts: Mitre, 1991. pp 37-40.

Cremers/Griefahn/Hinze (1993)

Cremers, Armin B., Ulrike Griefahn, and Ralf Hinze. *Deduktive Datenbanken*. Vieweg, 1993.

Cuppens/Yazdani (1991)

Cuppens, Frédéric, and Kioumars Yazdani. 'Logic Hints and Security in Relational Database'. Ed Carl E. Landwehr, and Sushil Jajodia. *Database Security V*. IFIP WG11.3 Workshop on Database Security 1991. Amsterdam: North-Holland, 1992. pp 227-238.

Denning et al (1988)

Denning, Dorothy E., Teresa F. Lunt, Roger R. Schell, William R. Shockley, and Mark Heckman. 'The SeaView Security Model'. *1988 Symposium on Security and Privacy*. IEEE Computer Society Press, 1988. pp 218-233.

Gallaire/Minker/Nicholas (1984)

Gallaire, Hervé, Jack Minker, and Jean-Marie Nicholas. 'Logic and Databases: A Deductive Approach'. *ACM Computing Surveys* 16.2 (1984):153-185.

Garvey/Lunt (1990)

Garvey, Thomas D., and Teresa F. Lunt. 'Multi-level Security for Knowledge Based Systems'. *6th Annual Computer Security Applications Conference*. IEEE Computer Society Press, 1990.

Garvey/Lunt (1991)

Garvey, Thomas D., and Teresa F. Lunt. *Multilevel Security for Knowledge Based Systems*. Technical Report SRI-CSL-91-01. Menlo Park, CA: SRI International, 1991.

Garvey et al (1992)

Garvey, Thomas D., Teresa F. Lunt, Xiaolei Qian, and Mark E. Stickel. 'Toward a tool to detect and eliminate inference problems in the design of multilevel databases'. Ed Bhavani Thuraisingham, and Carl E. Landwehr. *Database Security VI*. IFIP WG11.3 Workshop on Database Security 1992. Amsterdam: North-Holland, 1993. pp 149-167.

Gougen/Meseguer (1984)

Gougen, Joseph A., and José Meseguer. 'Unwinding and Inference Control'. *1984 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, 1984. pp 75-86.

Jajodia/Sandhu (1990)

Jajodia, Sushil, and Ravi Sandhu. 'Polyinstantiation Integrity in Multilevel Relations'. *1990 IEEE Symposium on Research in Security and Privacy*. IEEE



- Computer Society Press, 1990. pp 104-115.
- Jajodia/Sandhu (1991)  
Jajodia, Sushil, and Ravi Sandhu. 'Toward a multi-level secure relational data model'. *ACM SIGMOD International Conference on Management of Data 1991*. 1991. pp 50-59.
- Landwehr (1981)  
Landwehr, Carl E. 'Formal Models for Computer Security'. *ACM Computing Surveys* 13.3 (1981): 247-278.
- Lunt (1990)  
Lunt, Teresa F. 'The True Meaning of Polyinstantiation: Proposal for an Operational Semantics for a Multilevel Relational Database System'. Ed Bhavani Thuraisingham. *3rd RADC Database Security Workshop 1990*. Bedford, Massachusetts: Mitre, 1991. pp 26-36.
- Lunt (1991)  
Lunt, Teresa F. 'Polyinstantiation: an Inevitable Part of a Multilevel World'. *The Computer Security Foundations Workshop IV*. IEEE Computer Society Press, 1991. pp 236-238.
- Lunt/Millen (1989)  
Lunt, Teresa F., and Jonathan K. Millen. *Secure Knowledge-Based Systems*. Technical Report SRI-CSL-90-04. Menlo Park: SRI International, 1989.
- Meadows/Jajodia (1987)  
Meadows, Catherine, and Sushil Jajodia. 'Integrity Versus Security In Multilevel Secure Databases'. Ed Carl E. Landwehr. *Database Security*. IFIP WG11.3 Workshop on Database Security 1987. Amsterdam: North-Holland, 1988. pp 89-101.
- Michael et al (1992)  
Michael, Bret J., Edgar H. Sibley, Richard F. Baum, and Fu Li. 'On the Axiomatization of Security Policy: Some Tentative Observations About Logic Representations'. Ed Bhavani Thuraisingham, and Carl E. Landwehr. *Database Security VI*. IFIP WG11.3 Workshop on Database Security 1992. Amsterdam: North-Holland, 1993. pp 367-386.
- Morgenstern (1987)  
Morgenstern, Matthew. 'Security and Inference in Multilevel Database and Knowledge-Base Systems'. *1987 ACM SIGMOD Conference/ SIGMOD Record* 16.3 (1987):357-373.
- Qian (1994)  
Qian, Xiaolei. 'A Model-Theoretic Semantics of the Multilevel Relational Model'. Ed Matthias Jarke, Janis Bubenko, and Keith Jeffery. *Advances in Database Technology - EDBT'94*. LNCS, vol 779. Berlin et al: Springer-Verlag, 1994. pp 201-214.
- Reiter (1978)  
Reiter, Raymond. 'On closed world databases'. Ed Hervé Gallaire, and Jack Minker. *Logic and Data Bases*. New York: Plenum, 1978. pp 55-76.
- Reiter (1984)  
Reiter, Raymond. 'Towards a Logical Reconstruction of Relational Database Theory'. Ed Michael L. Brodie, John Mylopoulos, and Joachim W. Schmidt. *On Conceptual Modeling*. New York: Springer-Verlag, 1984. pp 191-238.
- Sandhu/Jajodia/Lunt (1990)  
Sandhu, Ravi, Sushil Jajodia, and Teresa F. Lunt. 'A new polyinstantiation integrity constraint for multilevel relations'. *The Computer Security Foundations Workshop III*. IEEE Computer Society Press, 1990. pp 159-165.
- Smith/Winslett (1992)  
Smith, Kenneth, and Marianne Winslett. 'Entity Modeling in the MLS Relational Model'. *18th VLDB Conference*. 1992. pp 199-210.
- Spalka (1994)  
Spalka, Adrian. 'Formal Semantics of Rights and Confidentiality in Definite Deductive Databases'. *IEEE Computer Security Foundations Workshop VII*. IEEE Computer Society Press, 1994. pp 47-58.
- Stickel et al (1993)  
Stickel, Mark E., Xiaolei Qian, Teresa F. Lunt, and Thomas D. Garvey. *Inference Channel Detection and Elimination*. Second Interim Paper. SRI Project 2528. Menlo Park: SRI International, 1993.
- Thuraisingham (1991)  
Thuraisingham, Bhavani. 'A Nonmonotonic Typed Multilevel Logic for Multilevel Secure Data/Knowledge Base Management Systems'. *IEEE Computer Security Foundations Workshop IV*. IEEE Computer Society Press, 1991. pp 127-138.
- Wiseman (1990)  
Wiseman, Simon. 'The Control of Integrity in Databases'. Ed Sushil Jajodia, and Carl E. Landwehr. *Database Security IV*. IFIP WG11.3 Workshop on Database Security 1990. Amsterdam: North-Holland, 1991. pp 191-203.
- Wiseman (1991)  
Wiseman, Simon. 'The conflict between confidentiality and integrity'. *IEEE Computer Security Foundations Workshop IV*. IEEE Computer Society Press, 1991. pp 241-242.

## Healthcare Information Architecture: Elements of a New Paradigm

Daniel J. Essin<sup>1</sup> and Thomas L. Lincoln<sup>1,2</sup>

### Abstract

An Electronic Medical Record (EMR) must simultaneously provide a secure, permanent archive for an individual's medical records and also function as a multi-purpose database that supports the complex, varied activities of patient care. Meeting these objectives requires unusual flexibility in how data are retrieved and processed. Semantic and referential integrity must be preserved both over time and as chunks of information are exchanged with other systems. To do this, the structure of an EMR system must support sufficient indirection in notation and access to information so that atomicity, authenticity and persistence of individual entries are preserved. These requirements imply a client/server approach in which generalized indirect access methods are extended into areas of application development that previously used low-level and/or proprietary access techniques, and in which relationships between data entries are determined dynamically based on actual events, rather than statically through application design. A modular information architecture is proposed that integrates these requirements for structure, content, and processing. Such increased linking requires that new forms of system security be incorporated into an EMR at a structural level, with an emphasis on the labeling of elements to be secured behind a security barrier, with audit trails to document necessary overrides and monitor for suspicious use.

---

<sup>1</sup> Clinical Information Systems, University of Southern California, Rm. 1L32, 1240 N. Mission Rd., Los Angeles, CA 90033, e-mail: [essin@usc.edu](mailto:essin@usc.edu)

<sup>2</sup> The RAND Corporation, 1700 Main Street, Santa Monica, CA 90407-2138, e-mail: [lincoln@rand.org](mailto:lincoln@rand.org)

## 1 - Introduction

To effectively reform healthcare, a paradigm shift will be required in healthcare computing. To meet new requirements, we will need new data management systems that are not merely a superficial rearrangement of existing hospital information systems.. Despite some computerization, the traditional paper-based medical record continues to serve all aspects of clinical care. It represents a kind of primitive blackboard system that passively organizes each patient's care and facilitates the solving of medical problems. In this sense, it both documents and communicates. Problems and their solutions are formulated on the chart, and various care providers consult it in order to coordinate the process. Thus some steps are procedural and some are cognitive. The paper chart also has some notoriously awkward characteristics. It is available in only one place when it is often needed in several simultaneously. It is fragmented, particularly with respect to imaging data, and is insufficiently indexed, with no single ordering satisfactory for all purposes. It is also often illegible.

Creating an electronic medical records system (EMRS) that can satisfy this same wide range of uses as the paper chart presents both a specific and a generic challenge to computing science. The task is to turn this classic paper source into one that will relieve the evident shortcomings without introducing new complications -- such as unwanted access -- all the while retaining the many advantages of the paper format. It is comfortably structured as a collection of documents, is able to encompass the variability and complexity of medical phenomena and health care practice, can be perused with minimal procedural navigation, it is portable to all venues, and it constitutes a single permanent legal document, appropriately signed by those responsible. This is a tall order, but we believe it to be possible using today's technology, given some decisions about certain policy parameters, plus some directed research and development.

To the present, attempts to create an EMR have fallen short. The most important reason for failure has been the assumption that clinical activities can be redirected into machine oriented formats and that the various rigidities introduced for the convenience of the computer will not interfere with clinical work. This assumption ignores the heuristic value of the approaches to information management embodied in the paper record. They are not arbitrary, but have been refined over time to deal with difficult issues. Thus, as advocated by Donald Norman in his book for a general audience: "Things That Make Us Smart: Defending human attributes in the age of the machine" [Nor93], success of an EMRS will depend upon supporting the flow of clinical work as it is most effectively accomplished by numerous participants, through a careful choice of data structures and of the underlying architecture.

## 2 - Requirements

The behavior an EMRS should exhibit is complex: 1) It must provide a rich method of representing information so that content, meaning and context are not obscured, insuring that the raw data is not prematurely replaced by interpretation or conjecture. 2) It must be "open" so that a wide range of information management appliances (applications), each with its own set of functional requirements, can use the information as a resource. 3) It must inform users about the nature of the information that it contains. 4) It must be able to selectively retrieve information, either for human viewers or to serve as knowledge sources for automated process- control and decision-support systems. 5) Since different groups of users each have their own agenda and preferences, there must be great flexibility in rendering the information for presentation. 6) It must store the data in ways that meet permanence regulations. 7) It must structurally address the issues of privacy, confidentiality and security.

The challenge to information scientists is to devise an information architecture that will address these requirements. The first step is to isolate basic properties that can be combined to create systems that exhibit the desired behavior (Table 1).

Table 1 Properties of Database Systems Designed to Store and Process Medical Records		
Atomicity	Semantic Integrity	Flexibility
Authenticity	Security	Processability
Persistence	Performance	Interoperability

### Atomicity

Each entry placed into EMRS should be self-contained, i.e., atomic. It must contain sufficient information to remain informative if removed from its host environment, and its authenticity must be preserved. Each entry must be registered using a time-base that is sufficiently fine-grained to allow an accurate chronology of events to be constructed. This is especially important when many participants are adding items concurrently in response to a single external event. In a certain sense an entry is an object.

### Authenticity

All entries must be unalterable [Pro92] and permanently archived. Each entry must be preserved, as it was entered, in order to meet medico-legal standards. Each document must be sealed with some type of encrypted checksum so that it can be verified that no changes have occurred since the document was committed to storage.

Updates are not permitted once documents have been committed. Corrections must be appended as new documents. Ordinary retrieval processes will only display those entries which, taken together, constitute the "official" correct record. Audit trails must be included, so that, with appropriate permission, the entire record can become visible, including those entries that have been superseded.

## Persistence

The period during which legal unalterability must be ensured is over 20 years in the case of records that document care to infants but may be shorter in the case of adults. With the current interest in a "lifetime medical record," individual documents may have to be maintained for over a century.

Database technologies that require that the data be periodically copied and/or reformatted as part of system maintenance and database restructuring would violate the unalterability requirement. However, as long as the original is never altered, working copies could be made freely since they could always be verified for accuracy against the original. This suggests the use of robust write-once media for the originals.

This requirement also implies that the data stores are external to and independent of any particular processing environment. Data stored internally to a specific application or platform cannot be accessed directly by others and even complicates modifying the original applications as their requirements evolve.

## Flexibility of Information Representation and Retrieval

The document structure must freely accept descriptive material of arbitrary length and it must be possible to qualify or annotate any or all quantitative items in the document.

Entries must accommodate fuzzy information such as approximate dates and times, information for which only qualitative definitions exist and statements of opinion.

Retrieval functions must produce useful results even if Information is missing.

Information may appear to be missing if, for security reasons, is unreachable in the absence of special access authorization.

The data contained within the persistent data store should be structured so that any conceivable query can be expressed as a first-order expression against such a database. The semantics of the data and the database must be explicitly recorded as part of the database and must be easily discoverable.

This is necessary because, although the typical database can be queried for a list of relation names, there is no way to determine their semantic nature or relationship [Kri91, Lit91], because traditional data management techniques hide the semantics of the database from the users. Today non-technical users are unable to query most databases because much of the knowledge of the meaning of individual attributes or relationships is implicitly embedded within the logic of the retrieval programs. Furthermore, there is no way to determine how many relations exist within the database that might contain information relevant to a particular inquiry. When role or relationship information is confounded by being present in the names of both relations and attributes, semantic heterogeneity increases. In order to avoid obscuring the semantics of the data, one has to consider the database as a whole [Lit91]. These authors assert that the first order normal form (1ONF) in which the database consists of a single relation and contains specific slots (i.e. attributes) that hold the information, would have been represented as by relation and attribute names if the database were in some traditional normal form, e.g. 3NF. They further state that any conceivable query can be expressed as a first-order expression against such a database. We take the matter even further, and assert that this concept can be applied to non-normal form databases (in which each entry is arbitrarily complex), provided that there is a mechanism to apply the first-order expressions to the output of intentionally defined functions that can be applied to the data.

Both developers and users need adequate tools to help them explore the semantics of the database and to determine what terms have been used before, and in what context. As the volume of stored data grows, discovering the semantics of past and present data models becomes an increasingly difficult task. But a lack of this capability leads to Keyword Drift [Ess87], a phenomenon whereby the semantics of an application wander over time. Users who do not have good information about what terms are currently active continually invent new keywords and new rules for categorizing and indexing the same information that they have coded before. As old data become unrecognizable

through this process, they become fossilized and unusable -- effectively non-existent for ordinary purposes.

### Semantic Integrity

Medical documents make frequent reference to data that are coded and/or maintained by ancillary systems. In a "properly normalized" relational database, a medical document would store only the appropriate foreign keys needed to join with the relations containing the explanatory detail. However, many coding schemes change from year to year and often retain the same code numbers even though the underlying definitions have been altered. It is not always possible to insure that the necessary systems (or versions of systems) will be on-line to satisfy a relational query at the time a document needs to be viewed or copied to an outside agency. Therefore, all information that is necessary to insure the semantic integrity of a document must be copied and stored in the document itself at the time it is committed to storage. The intent is to copy just enough information to preserve integrity (readability and context) of the individual entry.

### Interoperability

Documents transferred (or accessed) between sites, or used at the same site at different times, must be interoperable (processable at the recipient site and informationally equivalent). It must be possible to access the information content of documents, independent of the nature of the host system or in the absence of any sophisticated data manager (i.e. humans can read them with a low-level disk editor if all else fails).

### Processability

Each document must also include meta-information that describes its semantic content and organization. This information must be computable and accessible through queries. Existing documents may be candidates for inclusion in queries or new transactions on the basis of an arbitrarily large number of rule-based criteria. Similarly, the result sets



produced by arbitrarily complex transactions must be accessible through query languages and application programming interfaces (API) so that they can be used as input to other queries and processes.

### Performance

The speed with which database operations can be accomplished is always an important non-functional requirement. Slow responses commonly violate the cognitive tempo. In addition, there are many medical situations in which rapid access to information is critical.

### Security

In order for the healthcare process to be most effective, the medical record must contain accurate and complete information that reveals the details of people's lives and their medical histories, what was done for them and why and who was involved. In order to elicit the maximum detail, each participant must feel confident that the information will not fall into the wrong hands and be used against them. For this reason, just as there are legal requirements for record retention, there are legal and ethical requirements that the records be kept secure and confidential so that each individual's privacy is preserved.

### 3 - An Approach to Information Representation

None of the requirements or properties discussed above addresses the structure of the atomic unit of data storage. It is clear that in order to treat this disparate but highly inter-related data as a single resource it must be unified into a single structure that contains not only the data but a variety of semantic information (meta-data) to guide its subsequent retrieval and use. We theorize that the atomic unit of storage should be an encapsulated complex object with specific structural properties which we will now describe. We hypothesize that objects, so constructed, have the properties necessary to enable this unification. We call these objects Loosely Structured Documents [Ess93].

The term "loosely structured" refers to the fact that there may be wide variations in content and modest variations in structure within individual documents without obscuring their similarity to other documents of the same type.

The accumulated details that can be found in a collection of medical records exhibit complexity that is unbounded. The information may come in hundreds<sup>1</sup> of formats and the content differs widely depending on the domain from which these data originated. Viewed from a somewhat greater distance, the paper medical record is a collection of separate loosely structured documents [Ess93, Lin93]. Some data is highly quantitative, often organized in a tabular format. Some information is semi-quantitative data and is commonly collected using questionnaires and check lists. Records of interviews are almost entirely narrative. The most common records, those documenting ambulatory care encounters and admission to a hospital combine quantitative, semi-quantitative and narrative components into documents that have a loosely structured quality. Headers are in reality labels (or tags) that identify the content of different sections (such as Heart, Lungs, Impression, etc.). Some entries include logical links to physiological monitoring data and/or image data that are stored in other places. Within each type of form, flowsheet or document, some well established convention is used to structure the information. A variety of these forms are kept handy to that the users can easily switch between variants that organize the information differently or that impose more or less structure as each case dictates.

Structured documents have become a familiar convention. TEX and WordPerfect use internal markup to denote formatting and style regions<sup>2</sup>. CLOS (the Common Lisp Object System) and various frame-based knowledge representations define slots within objects. Boxer, a computational medium for elementary school students, creates structure with nested boxes [Sol93]. The Standardized Generalized Markup Language [Gol90] derives its openness and flexibility from the use of meta-level descriptors of

---

<sup>1</sup> A sales brochure for [Row85] advertised "800 useful nursing forms"

<sup>2</sup> Tex and other markup languages also include conventions for representing arrays and tabular data structures as streams of text with embedded tags to denote the position of each datum within the array.

document structure. Each of these markup conventions is intended to introduce a structure into data in order to enhance its ability to be processed computationally.

The internal structure of each document type found in the medical chart has many of the characteristics of the machine processable structures mentioned above, i.e. the structure usually is (or can be) indicated by topic headings inserted into the text. Tags such as CC: (chief complaint), and PMH: (past medical history) are immediately familiar to all practitioners and isolate specific regions of content. In effect, these tags constitute a markup language that emphasizes medical content. Missing tags imply the absence of significant material (in the opinion of the original observer). Other tagged sections may be optionally or conditionally inserted into specific documents in much the same way that a paper record may contain an annotation in the margin. More importantly, with appropriate tagging, highly structured tabular data can be represented using the same conventions.

[Day87] discusses documents as an example of complex objects and identifies a number of requirements for managing data objects with a complex internal structure. Complex objects are "highly structured objects that are composed of other objects." For example: "a document may be composed of sections ... and the sections themselves may be composed of section headings, paragraphs of text, and figures." In this sense, medical charts, and their component entries, are clearly complex data objects. "In many applications these complex objects are the units for storage, retrieval, update, [and] integrity control.... The most fundamental requirement of a complex object is that the user be allowed to manipulate it as a whole." Attempting to store medical records in conventional (e.g. relational) databases results in each object being reduced to a number of tuples scattered among a variety of tables. Because "there is no way to specify to the DBMS [database management system] that all of these linked tuples form a single complex object" operations on complex objects require complex sequences of relational commands.

Since objects can be arbitrarily complex <sup>3</sup>, the potential number of relationships between objects is potentially large [Day87]. Therefore, Dayal suggests that databases provide a general facility for specifying relationships between complex objects and/or their components in terms of functions defined over sets of complex objects instead of being limited to a small number of distinguished relationships with fixed semantics as is common in relational databases.

Objects, whether simple or complex, may have attributes that are not recorded directly within them but which must be derived indirectly from other data. This implies that data models in general should be extended to include the capability to return information by inference (but, in certain instances, also to block it). In other words, the results of database queries may include data that is not ever stored in the database but is derived dynamically from indirect sources or that is computed by arbitrary procedures. Scientific and medical databases have a corollary requirement - the ability to view complex objects at different levels of abstraction. This capability can be obtained by defining views over the output of retrieval functions alone or in combination with values derived from extensionally defined functions that are stored within the database.

[Day87] notes that "in some cases, it is too expensive to compute every intensionally-defined function on demand (i.e. at query execution time). It may be cheaper to precompute and cache its values instead. For querying purposes ... the function may be treated as being an extensionally-defined function. However, updates to the function's arguments may cause the cached values to become obsolete, requiring propagation of the update."

---

<sup>3</sup> Dayal's term for unbounded complexity.

## 4 - The Proposed Architecture

### Structure

The above requirements emphasize the need to treat the persistent data store as a discrete entity, separate from any application. In order to translate those requirements into an implementation a convention for structuring the documents must be adopted that can 1) accommodate variations in complexity, 2) allow application and knowledge evolution, 3) provide interoperability and open, self-describing semantics and 4) allow a wide variety of domain specific applications share, and be applied to, the same data. One candidate for a structuring convention is HyTime - the Hypermedia/Time-based structuring language <sup>4</sup> [New91]. It is built on the Standard Generalized Markup Language (SGML) <sup>5,6</sup> and introduces two abstractions that together provide a notation for defining a generalized hierarchy of occurrence types and a means of recording them. Using SGML, the internal structure of documents are specified by Document Type Definitions (DTD) - formal, computable statements that describe how documents will be structured and what mandatory and optional components will be present. The first level of abstraction is the DTD itself. The syntax of DTD's is expressed as a nested set of elements. Each element has its own generic identifier, an optional set of attributes and attribute data types, and a BNF-like production stating what sort of data can be placed inside each element or level of the element hierarchy [New91]. The second level of abstraction is provided by HyTime's architectural forms. Architectural forms are element meta-declarations that define the elements that can appear in DTD's or meta-DTD's.

Architectural forms define the class hierarchy of documents that can be entered into the data store and thus, in this case, distinguish a system as a medical system. At the

---

<sup>4</sup> ISO/IEC DIS 10744 (International Organization for Standardization / International Electrotechnical Commission Draft International Standard 10744)

<sup>5</sup> (ISO/IEC International Standards 8879-1986) [Go190]

<sup>6</sup> At least one MEDIX (IEEE P1157) prototype, built on the CMU-IBM Andrew Toolkit, has suggested the possibility of incorporating the SGML into a multi-media medical document application [McL90].

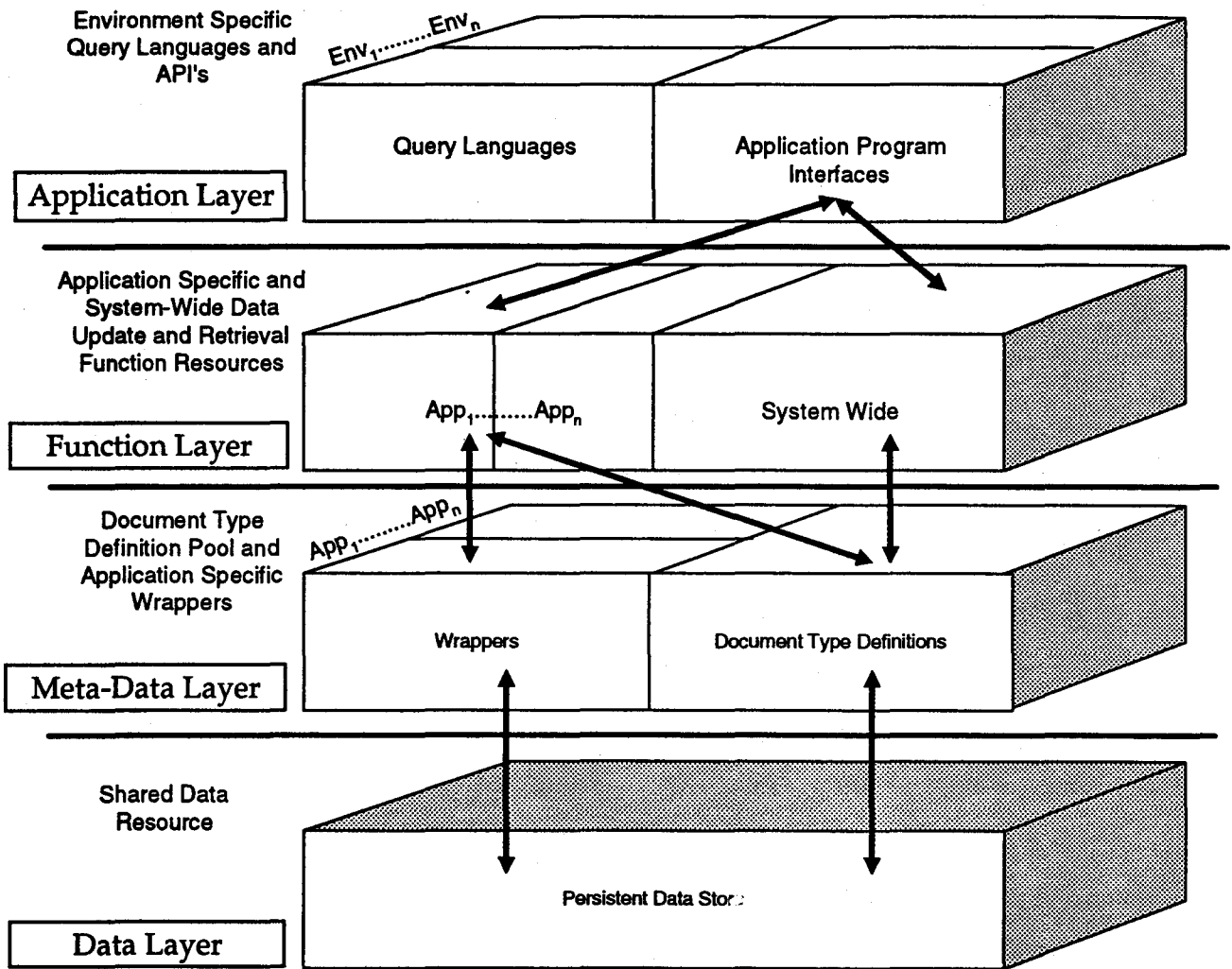
architectural form level, developers can specify the structure of the various components of a document, i.e. "who," "what," "where," etc. These elements can then be assembled as necessary to create the DTD's that will actually control what information is collected and how it is rendered (displayed). An architectural form specification defines the minimum information that must appear, any anticipated but optional information that may appear, and how any additional notations should be "marked up" so that they can be located and classified. It must specify what rules in the knowledge envelope of the system can be used to validate input and which rules define the syntax that can be used to enter and flag nonconforming data and annotations. A given architectural form may be used by zero, one, or many DTD's. Forms that are implemented by zero DTD's function as abstract types from which subclasses can be derived.

#### Application Independent Resources

It is not sufficient for the semantics of documents to be open. For a given domain, e.g. the EMRS, all applications accessing these documents must apply consistent logic during processing in order to maintain semantic integrity. This requires an explicit mechanism for creating data transformation and retrieval functions. This must be done at the domain level so that all applications in the domain can share them. There are a growing number of systems that do this. Hypercard and a variety of other Macintosh applications can share XCMD's. Dynamic Link Libraries in Windows, NT, and OS/2, are language independent and can be shared any application capable of calling them. Stored procedures in SQL databases and Remote Procedure Calls in various UNIX systems address the same need for application independent, system-wide resources. All applications using such resources achieve consistent behavior and, as a consequence, consistent semantics.

Under this model, application development would have two components. 1) The persistent data store – the document types and their semantics and the layer of function resources must share an evolutionary development path. 2) User-interfaces – query languages, API's and wrappers (temporary encapsulations of process-related data in

non-document form) may be application-specific. The relationship between these components is represented diagrammatically in Figure 1.



Modular and Layered Structure of the EMR  
Illustrating Data Flows to a Specific Application

Figure 1.

## Application Independent Database Structure

The requirement for interoperability anticipates that future systems will rely heavily on distributed processing. Workstations will perform computationally intensive tasks that are departmentally or functionally specific in nature. Logically, this implies that portions of the database will be accessed frequently by some applications and rarely (or never) by others. Security, confidentiality and network efficiency will each be promoted by logically partitioning the database and distributing certain portions to the site of most frequent use. Federations of application specific systems will replace the monolithic information systems of today. If the requirements for atomicity and processability are met, it will be possible to aggregate the data when necessary.

Meeting the atomicity and persistence requirements separates the traditional problem of database concurrency control into two parts. Since no updates to existing entries are allowed, all users are free to add new records at will. Entries that are intended to correct other entries may produce user views that only display the most current information.

The atomicity requirement also supports fault-tolerant, high-performance designs. Since existing records are never physically updated or deleted, the process of replicating the data to remote locations can be approached in a more leisurely fashion. It will be possible to queue transactions requiring replication, establish priorities, and even temporarily suspend the process if there is a physical disturbance on a portion of the network. Parallel processing [Car89] and blackboard systems [Eng88] are almost accident byproducts. Resilient medical systems have high availability requirements. Many are expected to be "up" continuously. This requirement is incompatible with the current generation of DBMS and operating systems that require periodic "down-time" for maintenance and the installation of new software versions. Externalizing the persistent data store offers a wide range of new opportunities to design methods that can provide continuous access to the data when various applications, or system components, are taken off-line for testing, modification or repair.



## Creating an Open Environment for Application Development

The layered architecture allows application development to proceed asynchronously and in parallel on many fronts overcoming a traditional bottleneck. To allow this parallel activity without elaborate coordination, applications will use the DTD's and other explicit representations of database semantics as the control mechanisms. Because properly constructed DTD's are computable, this approach should detect and eliminate designs or actions that would violate system integrity. Semantic checks can occur both in compilation, for the static elements, and during execution for the dynamic constructs. Once such tools are in place, it will be possible to engage end-users into the application development process without a loss of control. This scenario is compatible with both the desire for better engineered software, a more productive less error-prone development methodology, and the changes that are occurring in the way organizations and work are managed [Tap93].

### 5 - Security Issues.

Constructing security for an information architecture such as the one described here is a multidimensional problem. The appropriate security level for individual pieces of information is not stable over time and is frequently context dependent. As Ware has emphasized<sup>7</sup>, that security technology will always fall short, and that the greatest risk is unauthorized use by authorized users. Confidentiality and privacy must be considered to be at ongoing risk even when data systems themselves are otherwise secure. Complicating matters further, the very techniques that one hopes to use to improve patient care, namely aggregating data and by drawing inferences from it in order to gain diagnostic and therapeutic insights, are considered threats in other settings.

The architecture is modular and layered rather than monolithic (Figure 1). This provides the basis for systems in which the components are mutually distrustful

---

<sup>7</sup> Ware, W: personal communication.

[Nrc91]. Separating applications from data makes it possible to model work processes and construct data flows that clearly define boundaries of trust, for example, no one ordering supplies to restock the warehouse should ever be connected to any data source containing patient specific information. Each layer has specific security related tasks to perform.

The security behavior of the data layer must be adaptive, internally controlled and self-protective. It must decide whether or not to release information and it must control the permanent filing of new entries. It should also generate audit trails of database access (whether it stores then or not). The decision to release or accept information may be total or partial and it may be independent or mediated via trusted interactions with other system components. Loosely Structure Documents provide a mechanism to encapsulate security related information within them that can drive this activity. The approach is to tag those areas of content that have special security implications, such as the identities of the author and patient, the circumstances of document creation and any areas of the content that have a higher or lower level than the document as a whole. The default behavior of the persistent data store would be to only release information to the creator of the information, the individual to whom the information referred, or to properly cleared system administrators - unless there were additional restrictions encapsulated within a particular document that blocked this process.

The meta-data layer contains the information that defines the formatting and content architecture of the documents stored in the data layer. This layer also contains application specific wrappers. Wrappers are temporary encapsulations of process-related data in non-document form. This is an ideal place to assemble the information needed to drive access-control in a production environment as well as to maintain working copies of work in process and the knowledge bases needed to support production applications. In part, access can be controlled by creating application specific wrappers that only maintain working copies of a limited amount of data. Applications that only have access to these abstracts, but not the data layer, cannot

violate it. The volume of information will be too great and the number of users too large to create specific authorization matrices. Most access control to the data layer will have to be handled on the basis of role information. Some roles can be defined statically, others are defined by prior events. In this model, role information would be supplied to an access controller by a wrapper (Figure 1). This wrapper might (among other things) construct association tables based on:

1) role assigning events

Dr. Smith is credentialed as a member of the active staff for 2 years and has privileges in general surgery.

Dr. Garcia is credentialed as a member of the active staff for 2 years and has privileges in pulmonary medicine.

Nurse Adams has an valid license is hired by the facility.

2) administrative events

Nurse Adams is assigned to the Surgical Floor.

Mrs. Jones is admitted to the Surgical Floor by Dr. Smith

Mr. Jackson is admitted to the Medical Floor by Dr. Garcia

Dr. Smith requests a pulmonary consultation

The access control function would infer that:

Dr. Smith and Dr. Garcia can read all records and create entries relating to Mrs. Smith.

Nurse Adams can read and create entries relating to the current admission of Mrs. Smith as well as her history for the past year.

Mr. Jackson has a cardiac arrest. Dr. Smith and Nurse Adams respond to the emergency. They assert that it is an emergency and have full access to the records for the duration of the event. They both have subsequent read-access to any entries that they made during the event.

If the facility was informed that Dr. Cohen, also on the staff, had joined Dr. Smith in practice, Dr. Cohen would have access to Mrs. Jones' records.

After Mrs. Jones is discharged Nurse Adams and Dr. Garcia no longer have access to Mrs. Jones' records.

The relationship between any access controller and the data-layer is clearly a trusted one.

Another wrapper might keep a working copy of the last week's vital signs and lab results on hospitalized patients for rapid retrieval and manipulation and an index of the data available on those patients that could be retrieved from the data layer. The difficult trade off is to decide how much information to disclose - too little and patient care be compromised, too much and the potential for an inferential attack is increased.

At the function layer and the application layer, the implementation of security will depend on the approach taken to creating the access controllers. While existing techniques may be applicable there are some challenging clinical requirements at the application layer to consider. One such challenge is presented by the need for virtual sessions. In a fast-paced chaotic environment like a trauma center, a physician may need to start work on several patients simultaneously and have the ability to continue the work on any patient from any available workstation. This calls for some type of virtual session manager that keeps all database connections alive, saves the state of all visual displays and can restore the operational state of the program on any terminal when requested by the initiator of the event or by another authorized individual.

Access control has different meanings depending on context and time. As described in the scenario above, in an emergency context a wider range of individuals are allowed access. The value of some data is time limited. For example, the number ounces of liquid that Mrs. Jones consumed on her first day in the hospital day typically has a low security during the hospital stay and the level decreases steadily after discharge. Although the data must be retained for a legally prescribed length of time, the likelihood that this data will ever be retrieved is extremely low.

Several other security questions must be addressed that have little to do with the information architecture presented here but remain as open issues in the healthcare domain. The first relates to authorized copying of data. Various groups and the federal government would like to have access to various portions of the medical record to support a variety of research and planning activities. Should copies of this information be released or should these organizations be required to use it under secure conditions? If copies are released how should they be tracked? Can the systems controlling the data layer automatically apply transformations to the data as it is released to prevent the use of aggregation techniques to reestablish the identify of individuals? Is it possible to produce specially encrypted copies with built-in expiration dates on the decryption keys? Can data be released in an active form so that it can detect if it has been removed from a controlled environment and "self destruct". Can data be released while maintaining control over the retrieval functions by allowing users a remote sites to "borrow" functions via remote procedure calls.

## 6 - Conclusion

The model presented in this paper suggests an approach to the development of medical records databases that focuses on creating tools: 1) to establish and maintain a persistent store of data that is external to all applications, 2) to allow those involved in medical events to accurately and efficiently document what has occurred, 3) to allow individuals and processes access to the accumulated information, and 4) to address at a structural level the need to insure that the database is permanent and secure.

Some of the requirements described here raise fundamental research issues that will need further study. Others, especially the reliance on raw text searching (even if assisted by content delimiting tags) and the assumption that security and open access are not contradictory are frequently perceived to present overwhelming obstacles. Many of these apparent obstacles are being overcome in the research lab, some have already been implemented and others are in search of new paradigms in system security.

## References

- [Car89] Carriero N and Gelernter D: Linda in Context. *Commun. ACM*, 32, 4, (April 1989), 444-459.
- [Day87] Dayal U, Manola F, et al: "Simplifying Complex Objects: The Probe Approach to Modeling and Querying Them," *Proceedings of German Database Conference, Burg Technik and Wissenschaft-87*. reprinted in Zdonik, S. and Meyer, D. *Readings in Object-Oriented Database Systems*, Morgan Kaufman Publishers, San Mateo, CA 1990.
- [Eng88] Nii HP, Feigenbaum EA, Anton JJ and Rockmore AJ: Signal-to-Symbol Transformation: HASP/SIAP Case Study. in: Englemore R and Morgan T. *Blackboard Systems*. Addison Wesley 1988.
- [Ess93] Essin, DJ: Intelligent Processing of Loosely Structured Documents as a Strategy for Organizing Electronic Health Care Records. *Methods of Information in Medicine*, in press.
- [Ess87] Essin, DJ: Unpublished material. 1987.
- [Gol90] Goldfarb C: "The SGML Handbook," Oxford University Press, 1990.
- [Hri90] Hripcsak G et.al.: "The Arden Syntax for Medical Logic Modules," 14th Annual Symposium on Computer Applications in Medical Care, IEEE Computer Society Press, (November 1990), 200-204.
- [Kri91] Krishnamurthy R, Litwin W, Kent W: "Language Features for Interoperability of Databases with Schematic Discrepancies," *Proc. of ACM-SIGMOD Conf. SIGMOD Record*, 20, 2, (June 1991), 40-49.
- [Lin93] Lincoln, TL, Essin, DJ and Ware, WH: The Electronic Medical Record: A Challenge for Computer Science to Develop Clinically and Socially Relevant

Computer Systems to Coordinate Information for Patient Care and Analysis.  
The Information Society, Vol. 9, No. 2 (Apr-Jun 1993), 157-188.

- [Lit91] Litwin W, Ketabchi M, Krishnamurthy R: "First Order Normal Form for Relational Databases and Multidatabases," SIGMOD Record, 20, 4, (December 1991), 74-76.
- [McL90] McLinden S, Carlos G, and Oleson C: "The Evolution of a Standard for Patient Record Communication: A Case Study," 14th Annual Symposium on Computer Applications in Medical Care, IEEE Computer Society Press, (November 1990), 239-243.
- [New91] Newcomb S, Kipp N, and Newcomb V: "The 'HyTime' Hypermedia/Time-based Document Structuring Language," Commun. ACM, 24, 11, (November 1991), 67-83.
- [Nor93] Norman D: "Things That Make Us Smart: Defending human attributes in the age of the machine," Addison-Wesley, 1993.
- [Nrc91] Computers at Risk: Safe Computing in the Information Age. National Research Council. National Academy Press, 1991.
- [Pro92] Prosser RL: "Alteration of Medical Records Submitted for Medicolegal Review" JAMA Vol. 257, No. 19, May 20, 1992, pp. 2630-2631.
- [Row85] Rowland HS: Nursing forms manual. Aspen Systems Corp., Rockville, Md. 1985
- [Sol93] Soloway E: Reading and Writing in the 21st Century, Commun ACM Vol. 36, No. 3, May 1993, pp. 23-30.
- [Tap93] Tapscott D and Caston A: "Paradigm Shift: The New Promise of Information Technology" McGraw-Hill, 1993.

# Communication, Information Security and Value

John Dobson

Department of Computing Science  
University of Newcastle  
Newcastle NE1 7RU  
United Kingdom

## 1. Introduction

Information is one of the most dangerous substances known to humankind. Its use, or misuse, can bring down governments, destroy organisations, and cause untold personal misery. No wonder it needs to be handled safely and securely.

But this does not mean that the only protection must be afforded by access control. Information is of value, both positive, as when it is used as an organisational resource to help an organisation achieve its goals, and negative, as when it is used detrimentally in the wrong hands. Protection must also allow for an appropriate balance of values; and protection adds value to information.

For example, information privacy of medical records is not just a matter of preventing information getting into the wrong hands; anonymity also allows the protection of individuals so they can do their job or fulfil their role better, whether as patient or doctor. The negative side of this is that it can also be used to cover up instances of medical malpractice or deception by the patient.

So any thinking about security must start from an understanding of the relevance of the information to what the organisation or relationship using the information is trying to achieve, produce a theory of information which is a value- and relevance-based theory, and see information protection as a value-adding or value-protecting process.

Very few, if any, current theories of security are capable of reasoning about the value of the objects that the security policies are designed to protect. The assumption is that access to the objects is allowed, or not allowed, and that is the end of it. A corollary usually is that if access is to be prevented, it must be prevented at all costs, and hence the need for the provable correctness of an implementation of the access control policy.

But the "at all costs" assumption is unrealistic. In practice, an organisation has the choice of the following options:

- protect the object by reducing the vulnerabilities in the system and ensuring that the access control system works (fault<sup>1</sup> avoidance)
- reduce the threat by containing the enemy so that the very possibility of access is prevented (fault prevention)
- reduce the risk to exposure by so arranging things that a single attack cannot result in total loss (fault tolerance)
- ensure that if loss occurs, some recovery or compensation is available (fault recovery)
- accept the risk and hope for the best (fault acceptance).

---

<sup>1</sup> a fault here is a weakness in the system that might possibly result in a security breach.



Each of these options has an associated cost and risk. Risk management will consider these, and the value of the object to be protected, and the direct and consequential losses that might accrue, and the cost and effectiveness of countermeasures, and come up with a *security management policy*, which states how a fixed budget is to be allocated between the various fault management options identified above.

So although access control is a good set of mechanisms for fault avoidance, it is not the whole story. A new approach to security must enable reasoning about the costs and benefits of fault prevention, tolerance, recovery and acceptance as well. It is unlikely that controlling access to objects is a suitable conceptual basis for these in the way that it is for fault avoidance, because in none of these is access the real issue. What do seem to be the issues is summarised in the following table:

Strategy	Issues	Mechanisms
avoidance	what are the objects to be protected and who is allowed access to them? if access is granted or taken, what further information might be deduced?	access control information flow control
prevention	what other agents are there in the world and what is the disposition of their forces? what are their capabilities and budgets?	attack, i.e. causing faults in the enemy environment reducing the number of attackers or their budgets
tolerance	where are the single points of failure and concentrations of value?	distribution (fragmentation and scattering) redundancy
recovery	what are the available options for forward and backward error recovery? for compensation?	insurance compensation
acceptance	what is the probability of loss and direct and consequential costs?	

There is not a single all-embracing concept which can do justice to the modelling of all these strategies and enable comparison between them. There are at least four different kinds of analysis that are involved:

- **vulnerability analysis:** what are the weaknesses in the system from a security point of view? (In conventional terms, this is analogous to fault analysis.)
- **threat analysis:** what agents or events in the outside world could enable a vulnerability to be exploited so as to result in a loss? (In conventional terms, this is analogous to failure mode analysis.)
- **countermeasure analysis:** what countermeasures to vulnerabilities and threats are available, and what are their costs and effectiveness?
- **risk analysis:** is protection worth it if the countermeasure is costly and perhaps not very effective?

Each of these kinds of analysis will require its own set of models, concepts and methods.

This paper addresses the problem of analysing an information system for security flaws or vulnerabilities in a way that is analogous to the analysis of a safety-critical system. In particular, instead of adopting the approach that security is a property that must be proved to hold (fault avoidance), it shows how to analyse a system for possible security failures so that fault prevention, tolerance, recovery or even fault acceptance techniques can be chosen where appropriate. The justification for this approach is that fault avoidance may not always be desirable, for example for reasons of cost. Sometimes it may be better to insure against loss than to try to prevent it; and this applies to computer security too.

We start from two simple definitions, one of a safe system and one of a secure system:

A **safe** system is one that will not harm me or cause me loss, *even if it fails*.

A **secure** system is one that will not give others the means to harm me or cause me loss, *even if it fails*.

Of the many points that may be elaborated from these definitions, we wish to concentrate on four:

- 1) The failure modes of a system are at least as important as the normal operational modes, and need at least as much analysis. It is very striking how conventional approaches to safety case presentation concentrate on failure mode analysis in order to show how the safety mechanisms (or their alternates) will behave in the presence of failure, whereas this aspect seems lacking from security case presentation, which concentrates on showing that failures will not occur (or simply makes this assumption). If a security case amounts to saying "This is secure provided *that* is reliable" then there are further questions to be answered.
- 2) Safety is defined in terms of direct consequence, whereas security is defined in terms of indirect consequence: somebody ("my enemy") must receive something to my possible disadvantage.
- 3) Both safety and security are relative to a particular observer or stakeholder ("me").
- 4) "Loss" is a value term; it can be quantified in terms of some abstract value system (money, or peace of mind, or national security for example).

So any method of analysing a system for security vulnerabilities must be able to satisfy the following requirements:

- 1) It must be able to define, and recognise instances of, failure modes;
- 2) It must be able to accommodate the notion of someone receiving or obtaining something (this is what distinguishes a method of security analysis from methods of safety analysis, which do not have this requirement);
- 3) It must be able to accommodate the notion of relativity to a stakeholder;
- 4) It must be able to accommodate the notion of value.

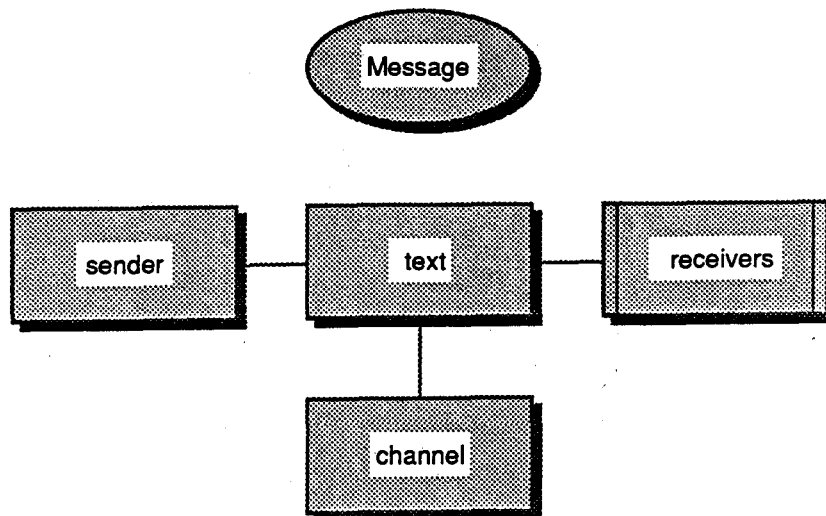
In this paper such a method of security analysis is proposed. It is based on modelling a computer system as a message-passing system, whose purpose is to facilitate human communication. (We shall say that message-passing is the *perspective* of the model. The perspective of a model is what the model concentrates on representing.)

## 2. The Conceptual Basis: Messages and Communication

The strategy we shall adopt is, in outline, as follows:

- i) We shall define the abstract syntax of a message, and of a communication. A computer system will be seen as a means of enabling communication through the passing of messages. This deals with requirement 2) above. It also deals with requirement 3) since communication will be defined in terms of stakeholders.
- ii) We shall provide a complete enumeration of possible failure modes of messages and communications. Security analysis then consists of identifying all the instances of messages and communications in a system (this is the hard part!) and analysing the defined failure modes for each instance. This deals with requirement 1) above.
- iii) We shall indicate an approach to attaching the notion of value to a communication so that standard methods of transaction chain analysis can be employed. This deals with requirement 4) above.

The abstract definition of a message is: some **text** passed from a **sender** to a set of **receivers** over a **channel**. No further elaboration of the primitive terms (in bold) will be provided here. We shall leave the definition of communication until later.



This definition allows us to enumerate the possible failure modes of a message:

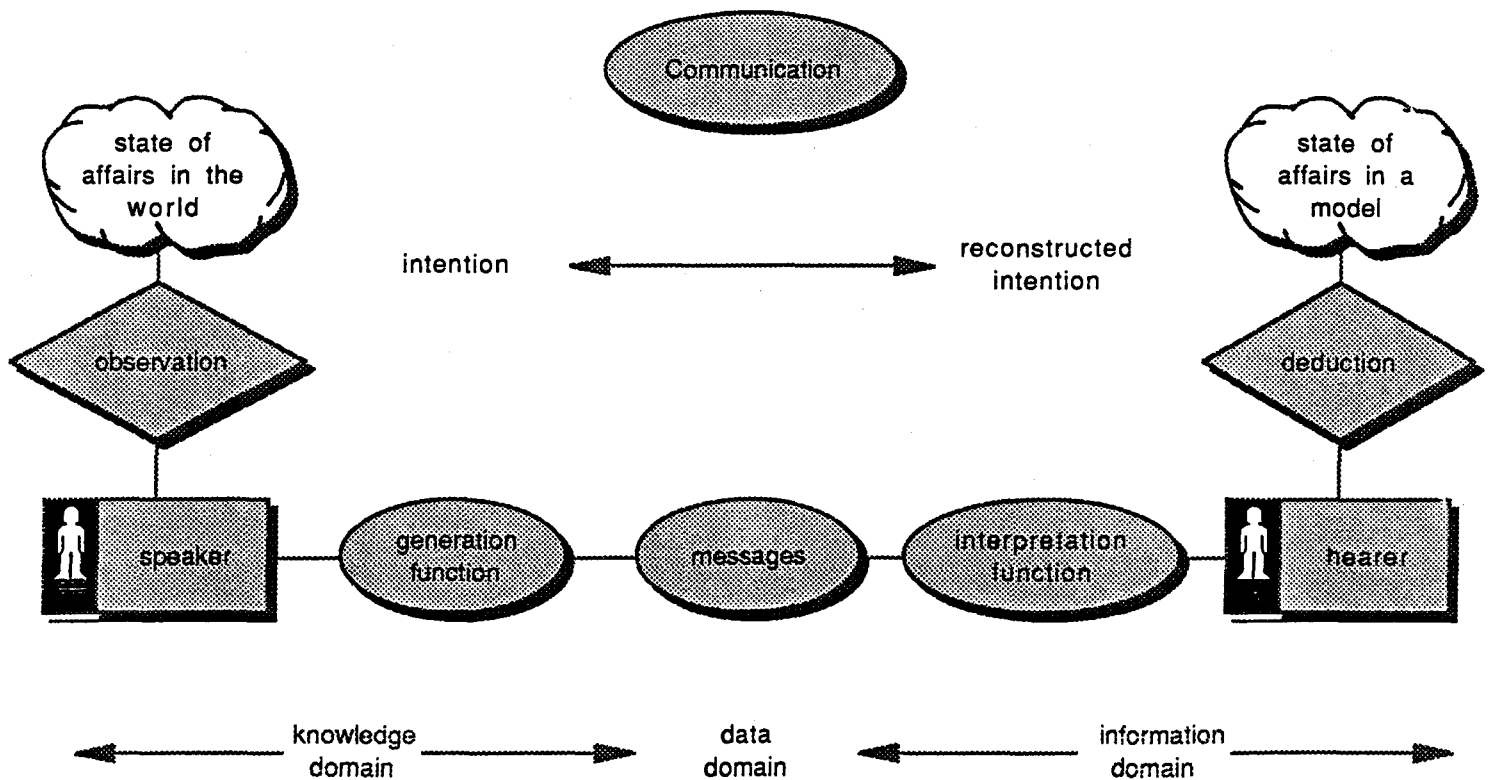
- The apparent sender (as seen by a particular receiver) might not be the same as the real sender.
- The set of real receivers might not be the same as the set of receivers intended by the sender: some intended receivers might not receive the message and some unintended ones might.
- The text received by a particular receiver might differ from the text intended by the sender.
- There are a number of authorisation failure modes, all of them being some form of the sender not being authorised to send that text to a particular receiver.

- There are a number of sequencing errors over an ordered set of messages: message loss, message duplication, message permutation.
- The communication channel might block.
- The communication channel might suffer from a number of timing faults (messages delivered too late or too early).

Our claim is that the above enumeration is complete, in the sense that any failure of an instance of a message (as defined) in a system can usefully be put into one of the above categories. The word 'usefully' implies that sometimes there may be a choice of which category to use.

Communication is a more subtle notion. The basic form of communication is an intention (i.e. a human interest, that which is to be communicated) being mapped by a particular stakeholder (the **speaker**) using a process we shall call **generation** onto a set of messages, which are then sent to a set of other stakeholders (**hearers**) who use individual processes of **interpretation** to reconstruct the original speaker's intention. Again no further elaboration of the terms in bold will be provided. For example, encryption can be considered one form of generation and decryption as the corresponding interpretation.

But there is more to communication than that, since we have to explain these unanalysed intentions. Our model is that the speaker's intention arises as a result of an **observation** of states of affairs in the speaker's world, and that a particular hearer's reconstructed intention results in the hearer adjusting the state of affairs in *the hearer's model of the speaker's world*. This model may be computational, or physical, or cognitive. Sometimes it may be the same as the speaker's world itself, but this is not always the case. We shall call this latter process of adjustment a **deduction** process.



This allows us to enumerate the possible failure modes of a communication, other than those that can be categorised as message failures:

- The reconstructed intention might not be the same as the original intention. Sometimes (but not always) this can be identified as a failure in generation (the messages do not carry the intention) or a failure in interpretation (the messages carry the intention but this does not get through to the hearer). Sometimes the generation and interpretation functions might not be mutual inverses.
- The original observation might be incorrect (not correspond to reality in the speaker's world).
- The intention might not capture the original observation correctly ("What I said was ... and this was mapped onto the messages correctly, but what I *meant* was ...").
- The deduction process might be faulty: the hearer makes inappropriate adjustments in the hearer's model.
- The hearer's model might be inappropriate: the hearer has chosen the wrong selection of state variables to select for representation or to ignore in constructing the model of the speaker's world.

We can now draw up a template which will be used for the categorisation of possible message failures, as follows:

	DATA DOMAIN FAILURES	
<u>message failures</u>	<u>sequence failures</u>	<u>channel failures</u>
<i>real/apparent sender mismatch</i>	<i>lost message</i>	<i>blocked channel</i>
<i>real/intended receiver mismatch</i>	<i>duplicate message</i>	<i>timing error</i>
<i>sent/received text mismatch</i>	<i>permutation error</i>	
<i>authorisation errors</i>		

Similarly we can set up a template of communication failure modes, as follows:

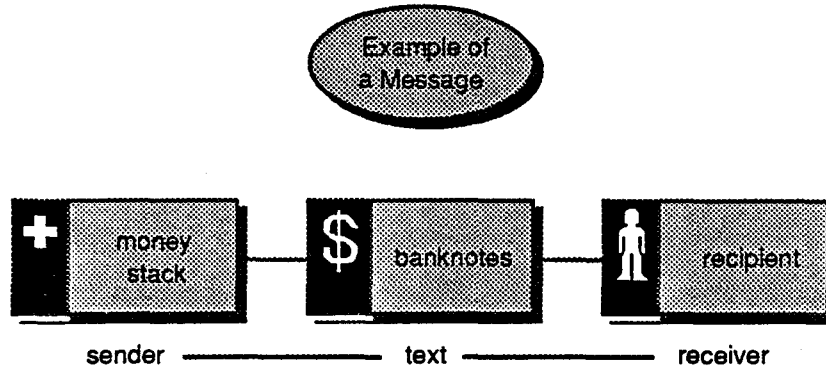
KNOWLEDGE DOMAIN FAILURES	INFORMATION DOMAIN FAILURES
<i>observation errors</i>	<i>deduction errors</i>
<i>speaker intention errors</i>	<i>hearer reconstruction errors</i>
<i>generation errors</i>	<i>interpretation errors</i>
<i>generation not inverse of interpretation</i>	<i>interpretation not inverse of generation</i>
	<i>modelling errors</i>

### 3. Two Examples

We shall take two very simple examples chosen especially to illustrate the ideas presented. Neither should be taken as examples of real world actuality.

Firstly, an example of a message:

*At the final stage of an automated teller machine (ATM) transaction, some money is passed from a money stack through a chute to a grasping hand. This can be considered a message. The money stack is the sender, the chute the channel, the monetary notes the text, and the grasping hand the receiver.*



Applying our template, we can fill it in as follows. The numbers refer to subsequent paragraphs in which an example of possible security flaws of that category is given.

	DATA DOMAIN FAILURES	
message failures	sequence failures	channel failures
<i>reall/apparent sender mismatch</i> (1)	<i>lost message</i> (5)	<i>blocked channel</i> (8)
<i>reall/intended receiver mismatch</i> (2)	<i>duplicate message</i> (6)	<i>timing error</i> (9)
<i>sent/received text mismatch</i> (3)	<i>permutation error</i> (7)	
<i>authorisation errors</i> (4)		

(1) How does the recipient know that the money has actually come from the bank? This might not matter of course; but consider that a bogus ATM might have been set up in a shopping mall which dispenses real money in response to accepting, and stealing, clients' card numbers and identification codes.

(2) How does the bank know that the hand that grasps the money belongs to the person authenticated in previous messages? (It might not care of course.) Consider the opportunity for a thief who waits for a client to make a valid transaction and then grabs the money as it comes out of the chute.

- (3) How do the bank and the client know that the money stack contains notes of the right denomination? Suppose the money stack contains grocery coupons? Suppose the chute tears all the banknotes in half as it delivers them?
- (4) Questions of authorisation are supposed to have been dealt with during previous messages of this transaction.
- (5) How do we know that the number of notes counted out by the money stack is the same as the number grasped by the hand? Is there a secret trapdoor in the chute that secretes every tenth banknote into a special cache for the benefit of the maintenance engineer, for example?
- (6) Or does the money stack count "one for the client, one for the engineer, two for the client, two for the engineer...?"
- (7) It probably doesn't matter in what order the notes are given out. But in other contexts, the exact sequence of messages might matter.
- (8) This corresponds to the vandal who fills the mouth of the chute up with SuperGlue (™, probably).
- (9) Suppose the chute only delivers the notes an hour after the money stack has been activated to deliver them. What would happen?

Now for an example of communication failure analysis.

*The Prime Minister of Machiavellia suspects a plot among her colleagues to place her in a position of some political difficulty. She responds by secretly leaking a sensitive document to a journalist, so disguising things that it appears that the document has come from a colleague whom she wishes to embarrass first. (Leaking a sensitive document is, of course, a matter of embarrassment for the apparent leaker. Resignation will be demanded.)*

Here, the intention is clear — to embarrass a colleague. The message generated and interpreted is, of course, not just the sensitive document itself but more importantly the apparent source of the leak.

KNOWLEDGE DOMAIN FAILURES	INFORMATION DOMAIN FAILURES
<i>observation errors</i> (1)	<i>deduction errors</i> (5)
<i>speaker intention errors</i> (2)	<i>hearer reconstruction errors</i> (6)
<i>generation errors</i> (3)	<i>interpretation errors</i> (7)
<i>generation not inverse of interpretation</i> (4)	<i>interpretation not inverse of generation</i> (8)
	<i>modelling errors</i> (9)

- (1) The Prime Minister might be in error in suspecting a plot.
- (2) The document might not be sufficiently sensitive and embarrassing (its leaking must be a resignation issue), so it must be carefully chosen.

- (3) The journalist might not understand that this is a deliberate leak (and, for example, return the document unread on the grounds that a simple mistake has been made).
- (4) The Prime Minister must be assured that the source trail followed by the journalist, and any subsequent investigation of the leak, does in fact clearly point back to her colleague. Subverting (and possibly blackmailing) her colleague's Press Officer might do the trick — but again it might not. An apparent computer audit trail might be better if it could be arranged, but this might not be possible if the computer software is sufficiently "correct", i.e. not in accordance with the real requirements.
- (5) The journalist might not recognise the document and the apparent source of the leak.
- (6) The journalist might not realise the apparent purpose for which the document has been leaked.
- (7) The journalist might not believe that the apparent source is the true source (dangerous, this one!).
- (8) The journalist might simply misread the identification of the apparent leaker.
- (9) The journalist might not have an adequate model of Machiavellian cabinet politics.

Perhaps some of the above assignments are a bit arbitrary, or could have been otherwise categorised. This does not really matter. What matters is that a systematic way is found of trying to generate as many different failure modes as can be conceived. To repeat, what we are advocating is a method which

- defines a model of messages and a model of communication;
- defines possible failure modes in terms of those models;
- instantiates the models wherever they can be found in the system to be investigated;
- for each instance, decides on suitable interpretations of the previously identified failure modes;
- for each interpretation of each failure mode, decides whether the security risk exposed should be prevented or the threat removed, masked (e.g. by insurance), or accepted.

#### **4. Communication as a Means of the Social Construction of Reality**

Perhaps an unusual feature of our approach is that we have done our vulnerability analysis in terms of the messages that are passed between entities in a computer system, and the communications that these messages encode or represent, whereas most approaches to security start from a basis of the entities involved (divided, perhaps, into 'subjects' and 'objects'). There are good reasons for this.

Firstly, as we explained earlier, our definition of a secure system means that we are interested in the ways in which someone might acquire something. Direct access is one such means, but interpretation is another. If I am concerned that my enemy X might get to know about my precious object P whose total protection is beyond my means, then I want to know who X is talking to and what about. Whether or not it is about P, or whether X is trying to access P, doesn't really matter. This is the basis of telephone tapping.

More importantly, however, security is but one example of a wide class of concerns such as safety, performance, maintainability and so on, all of which are characterised by the fact that their definition and analysis has to take place as much in the social domain as in the technical



domain. The origin and ownership of security policies, strategies for security management, the context of the protection mechanisms, and ultimately the very meaning of 'security' itself, are all social issues which have to be resolved in the organisational environment of the information system. This means that any method for analysis of an allegedly secure system has to be a method of analysis that can be applied equally well to social and to technical systems. Many methods for representation and analysis of organisational systems, loosely called 'enterprise modelling', exist and the best of these agree in seeing the structure and functioning of an organisation in terms of a social construct based on various forms of relationships built through social communication: co-operation, negotiation, competition, power struggles, downright enmity, and other more complex forms. If an organisation is to be understood in these terms, and if we are right in seeking a common set of concepts in which to describe both the social and technical aspects of the security perspective, then the concept of communication seems the best starting point, with the technical system being seen as the bearer of the messages which enable communication to take place. After all, a database is only a particular form of message channel supporting communication between an information source and an information enquirer.

## 5. The Addition of Value

What we have just presented is, however, more than just a neat way of performing a security analysis of a system. The modelling of a computer system in terms of abstract messages and communications, rather than in terms of abstract objects, allows us to fulfil another of our objectives, that of explaining how objects in a computer system acquire value, and so might require protection. In some cases (not, of course, all), the computation of value might be sufficiently realistic to allow a security management policy to decide to what extent the object is worth protecting anyway.

There are many drivers of the value of an object in the world, which we do not propose to analyse. This paper is concerned with the security of things in a computerised information system, and the way the value of those things arises.

It is our model of communication that gives rise to the (simplified) theory of value that we propose. The object of value that is to be protected is taken to be the hearer's model of the speaker's world which incorporates a particular state of affairs. Referring back to the picture of communication, we can see that the ways in which value can come to be associated with such an object is through the cost of acquisition and the cost of ownership and the benefit that may accrue through subsequent use. Also the messages themselves may carry a value either in the text (as in electronic funds transfer) or simply by their existence.

Costs of acquisition include the initial cost of observation, the cost of the generation functions, the cost of transmission of messages, the cost of the interpretation functions, and the cost of deductions. Costs of ownership include cost of maintenance of the model and possibly cost of decommissioning of the model.

Benefits of use of the model arise in two separate ways. Firstly, interpretation of a message takes place in a context, this context including the current state of affairs in the model. Secondly, in an information value-adding market, the model in one link of the value-adding chain is often taken as the world of observation in the next link of the chain. So the costs of observation in the next link provide the benefits of use in the previous link.

This will be illustrated by three simple examples of cases where naïve access control is insufficient to express the organisational policies, which require a theory of value and change in value for their full expression.

- **Press releases.** No access before the release time, unlimited and positively encouraged access thereafter. The information has changed in value.
- **Need-to-know.** Sometimes, due to the contingencies of war, high-level information is to be made available to low-level personnel, contrary to MAC, without either downgrading the level of the information or upgrading the level of the personnel. The information becomes

of value to the personnel so that they can correctly interpret any subsequent communications that are passed to them.

- **Resource-constrained access.** At busy times in certain South American telephone systems, people who pay more — business lines, usually — get dial tone sooner than ordinary residential lines<sup>2</sup>. Here, the theory of value dictates that the protection policy (of valuable resources, namely service access) is mapped not onto access control policies but onto resource queuing policies.

In fact there are number of mechanisms onto which a protection policy could be mapped: access control policies, resource queuing policies, flow control policies, regulatory policies and so on. Which of these is used is determined by the structure of the organisations and the context of organisational relationships in which they operate. What is common to them all, however, is that the protection policies operate in a context of relationships mediated by communications of the kind we have described, and it is in the breakdown of these value-adding communications that most of the opportunities for detrimentally manipulating value are to be found.

## 6. What can be Formalised? What should be Implemented?

The theory of messages presented above is trivially formalisable. Formalisation of the theory of communication runs into difficulties mainly because of the properties of the interpretation function, which is hearer-dependent. Consider, for example, the difficulties arising from system error messages, which carry a communication from the system designer to the system operator or user, and a result of which the user is expected to adjust a faulty model of the system designer's world. It is notoriously hard to come up with an set of error messages which are immediately clear to all users equally.

The theory of value is not yet sufficiently developed. It is not even yet clear whether it is composable. However, if combined with a suitable form of utility theory, it might provide a basis for ways of thinking about such things as the true economic costs of computer security. This is for further research.

What has been presented is a means of analysis, not a proposed new security protection policy. So what could be implemented is some automated support for the analysis. For example, in an object-oriented application, it would be useful to have records of messages passed to and from the objects of interest (the 'subjects' and 'objects' of the protection policy, for example), so that they could be analysed in the way proposed. What would also be of interest is to see how the messages related to the communications involved, assuming that there was some way of identifying or determining the latter. A prerequisite for this would be a decent enterprise model of the organisational environment in which the communication was taking place, since it is the enterprise model that allows definition of the types of communication that might take place..

## 7. What Else?

It would be a mistake to think that the perspectives of messages and communication which we have presented are the only perspectives on an information security system from which a vulnerability analysis could be performed. There are at least three other perspectives for which models need to be developed for a full security analysis of a system: behaviour, structure, and enterprise relationships (and possibly substance might be a fourth). In our previous work in this area, we suggested that from the point of view of analysis of security vulnerabilities, behaviour might best be modelled by some form of Petri net and structure was best considered in terms of a

---

<sup>2</sup> or at least this used to be the case. I don't know whether it still is.

composition of trusted and untrusted components. We have also previously dealt with the enterprise relationship perspective at some length. But revisions of these might be for other papers.

### **Acknowledgements**

Some of this paper is a revision and reworking of ideas and methods developed while the author was funded by RSRE Malvern (now known as DRA) during the period 1986-1989. Most of this paper has benefitted from close association over the years with Mike Martin. I am very grateful to the University of Connecticut for affording me the time and space to get these ideas down on paper in this revised and hopefully improved form and to Steve Demurjian for his helpful comments.

**FUZZY PATTERNS IN DATA**  
**-Anomaly Detection**

T. Y. Lin  
Mathematics and Computer Science  
San Jose State University  
San Jose, California 95192  
tylin@sjsumcs.SJSU.EDU  
Tel 408-924-5121(Voice)  
408-924-5080 (Fax)  
U.S.A.

**Abstract**

A computer is a finite discrete machines, the set of real numbers is an infinite continuum. So the representation of numbers in computers is an approximation. Rough set theory is the underlying mathematics. A "computer" version of Weistrass theorem states that every sequence, within the radius of error, repeats certain terms infinitely many times. In terms of applications, the theorem guarantees that the audit trail has repeating data. Examining further, based on fuzzy-rough set theory, hidden fuzzy relationships (rules) in audited data are uncovered. The information about the repeating data and fuzzy relationships reflect "unconscious patterns" of user's habits. They are some deeper "signatures" of users, which provide a solid foundation to detect the abuse and misuse of computer systems. A sliding window information system is used to illustrate the detection of a hypothetical virus attack. The complexity problem is believed to be controllable via rough set representation of data.

## 1. Introduction

What is a pattern? Does it exist? One could approach "hard patterns" from algorithmic information theory. Unfortunately, algorithm information theory asserts that almost all finite sequences have no patterns [Lamb90], [LiVi88]. This says that there is no theory for "hard patterns" in finite sequence. However, "soft patterns" do exist. In this paper we develop two types of patterns, one is repeating records (within the radius of error), the other is fuzzy relationships among data. In the area of intrusion detection, we believe users exhibit "unconscious patterns" [Lunt90], [Lunt91]. In this paper, we continue our earlier efforts on the fundamental questions of anomaly detection: Do patterns exist in audit trails? What types of patterns are there? [Lin93a,b]. Some experimental results based on DataLogic software will be reported in the future paper. Datalogic is a software system developed by Reduct Inc based on Rough Set Theory.

Let us say few words about the "new" computing and mathematical concepts that will be used in this paper. Recently Zadeh organized a soft computing program at Berkeley, and spoke about soft computing at SIMTEC'93 (Simulation Technology), [Zade93], [Wild94]. Independently, Pawlak has proposed an all-embracing soft set theory at RSKD'93 (Rough Sets and Knowledge Discovery) [Pawl93]. The notion of soft sets is a unified view of classical, rough, and fuzzy sets. Rough sets and fuzzy sets are complementary generalizations of classical sets. Fuzzy sets allow partial set memberships to handle vagueness, while rough sets allow multiple set memberships to deal with indiscernibility. According to Zadeh, soft computing includes, at least, fuzzy logic, neural network, probabilistic reasoning, belief network, genetic algorithms, and parts of learning and chaos theories. We believe that the notion of soft sets and many works developed by Pawlak school are also part of soft computing. Soft computing will be our main computing techniques.

Computers are finite discrete machines, however, the set of real numbers is an infinite continuum. So the representation of real numbers in computers must be an approximate representation. Are there mathematical theories behind such approximations. Pawlak' rough set theory turns out to be the right mathematical model for such representations [Pawl82], [Pawl91].

In this paper, first we examine the properties of numbers represented in computers from the point of view of mathematical analysis. Earlier, we have obtained a "computer" version of Weistrass theorem [Lin93a], which states that every sequence in a closed interval repeats, within the radius of error, certain values infinitely many times. In terms of our applications, the theorem implies that in the "infinite" input stream of records, there are repeating patterns. We can interpret the audit trail as an infinite input stream of records of a database. So the theorem guarantees that

- (a) there are repeating records.

These repeating data are not necessarily the only patterns. Some relationships among these input data may repeating themselves "infinitely" many times. So based on rough set theory again, we examine further the hidden repeating fuzzy relationships among these data. These relationships are often the reflection of some unconscious patterns of user's habits [Lunt90]. The fuzzy-rough set methodology allow us to find more elaborate hidden phenomena in the audit trail, namely,

- (b) The repeating fuzzy relationships(rules).

The information about the "repeating records" and "unconscious habits" are often the deeper facts about users. Thus provide us a foundation to detect the abuse and misuse of computer systems.

## 2. Rough Sets and Numbers in Computers

As remarked earlier, real numbers is an infinite continuum., while computer memory is finite in size. How could we represent real numbers in computers?

Let  $X$  be an interval  $X=[a, b]$  which covers the range that we need. The computer's representation of  $X$  is a finite set of points lying between the real numbers  $a$  and  $b$ .

$$a \approx a_1, a_2, \dots, a_n \approx b$$

More precisely,  $X$  is partitioned into half-open intervals

$$[a_1, a_1+\epsilon), [a_2, a_2+\epsilon), \dots, [a_n, b=a_n+\epsilon]$$

such that each sub-interval  $s_i=[a_i, a_i+\epsilon)$  is mapped (truncated) into the left-end point  $a_i$ , where  $\epsilon$  is a small positive number.  $a_i$  is a truncated number. Such partition defines an equivalence relation  $R$  on  $X$ . The pair  $(X, R)$  is called approximation space by Pawlak [Paw82], [Paw91]. The equivalence relation,  $x R y$ , means that  $x$  and  $y$  are truncated into the same number. Geometrically, it means that  $x$  and  $y$  are in the same sub-interval. We will call such  $R$  an indiscernibility relation of radius  $\epsilon$ . The quotient set  $X/R$  is a set of sub-intervals that are often represented by their left-end points. We will call  $\epsilon$  the radius of truncation.

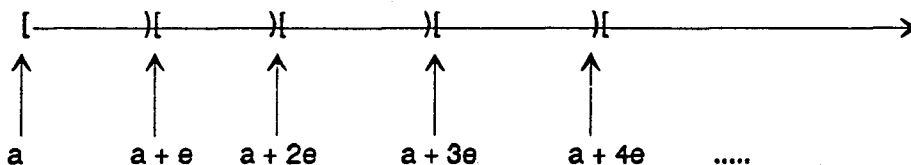


Figure 1

Let  $S$  be a sequence in  $X$ .  $S$  determines a sequence  $[S]$  in  $X/R$ . Theoretically,  $[S]$  is a sequence of sub-intervals, or, in practice, a sequence of truncated numbers.  $[S]$  will be called, in either sense, the image sequence of  $S$ .

### 3. Sequences of Real Numbers in Computers

In mathematical analysis, Weistrass theorem states that a sequence in a closed interval  $X$  has a convergent subsequence, say converge to the point  $p$ . In other words, given an  $\epsilon$ -neighborhood of  $p$ , the sequence will repeatedly fell into this  $\epsilon$ -neighborhood of  $p$  infinitely many times. If we truncate more than  $2\epsilon$ , then the sequence will repeat certain value (the truncated  $p$ ) infinitely many times. This conclude that an infinite sequence has a repeating pattern.

**Theorem** Every sequence of a finite interval has a repeating subsequence, when it is represented in computers.

As we have observed in Section 3, there are only finite points in this interval, which are represented in computers. So an infinite sequence certainly will repeat itself infinitely many times at (at least) one of those points.

The same idea can be applied to high dimensional Euclidean space. The high dimensional "interval" is a (high dimensional) cube. So we have

**Theorem.** Every sequence of vectors in a closed (high dimensional) cube has a repeating subsequence, when the sequence is represented in computers.

### Applications

One can view audit trail as a sequence of vectors or records. We will regard the vector as tuples in a relational database (to be more precise, an information system). So the components of vectors will be referred to as attributes. Note that all data in an audit trail are in computers (so they are truncated data)

Theorem. If the audit trail is long enough, then there is repeating records.

The repeating records are part of user's "signature".

## 4. Fuzzy Information Systems

Our main focus is on audit trail, which can be viewed as a relational database or information system with continuous input. Since we will be more interested in the data, information systems are better framework than databases. The information system has been studied intensively by Pawlak school [Paw82]. Our contribution in this paper is extending Pawlak's methodology to fuzzy rough sets [DuPr90], [Lin92]. Based on fuzzy view of rough sets, instead of exact rules, we obtain fuzzy rules. In audit trails, we need fuzzy rules, because of constant updating. Exact rules are too expensive to update. Our approach is a "fuzzy" variation of Ziarko's work [Ziar93]. In our case, each supporting case is weighted, or from the point of view of fuzzy sets, each case has a partial membership. We view an audit trail as a "dynamic" information system; the records are constantly inserted and faded away (aging). An information system in audit trails is a sliding "window".

### 4.1. Pawlak Information Systems

A Pawlak information system is a 4-tuple

$$S = (U, T, V, \rho)$$

where

U is the set of objects of S.

T is a set of attributes.

V = the union of all the sets  $V_a$  of values of attributes a.

$\rho : U \times T \rightarrow V$ , called description function, is a map such that

$\rho(x,a)$  is in  $V_a$  for all x in U and a in T.

Let B be a non-empty subset of T. Let x, y be two objects. x and y are indiscernible by B in S, denoted by

$$x \equiv y \pmod{B} \text{ if } \rho(x,q) = \rho(y,q) \text{ for every } q \in B.$$

Obviously,  $\equiv$  is an equivalence relation, it will be called indiscernibility relation  $IND(B)$ . The partition induced by B is called a classification of U generated by B. For a non empty subset B of T, an ordered pair  $A = (U, B)$  is an approximation space. A definable set X will be called B-definable [Paw82].

An information system  $(S, T, V, \rho)$  is called a decision table if  $T = C \cup D$  is a set of attributes, where C and D are disjoint non-empty subsets [Pawl91]. The elements in C are called conditional attributes. The elements in D are called decision attributes.

A relation/view instance is a snap shot of a relational database, which represents user's instant perception of entities or objects represented in the database. An information system is such an instance. We should also note that the attributes in the information systems may be a proper subset of attributes of databases.

Example

A relation Table-1

ID#	LOCATION	TEST	POLL	LEVEL	NEW	CASE	RESULT
ID-1.	Houston	1	0	0	11	1	1
ID-2.	San Jose	1	0	0	11	1	1
ID-3.	Santa Clara	1	1	1	11	1	1
ID-4.	New York	0	1	1	10	0.7	1
ID-5.	Chicago	0	1	1	10	0.7	1
ID-6.	Los Angeles	0	1	1	10	0.7	1
ID-7.	San Franscico	0	1	1	10	0.7	1
ID-8.	Seattle	0	1	1	10	0.7	1
ID-9.	Philadelphia	0	1	1	10	0.7	1
ID-10.	Atlanta	0	1	1	10	0.7	1
ID-11.	St Louis	0	1	1	10	0.7	1
ID-12.	Cincinnati	0	1	1	10	0.7	1
ID-13.	Washington	0	1	1	12	1	2
ID-14.	New Orleans	1	1	0	12	1	2
ID-15.	Baltimore	1	1	0	12	1	2
ID-16.	Boston	1	1	0	12	1	2
ID-17.	San Diego	1	1	0	12	1	2
ID-18.	Palo Alto.	1	1	0	23	1	3
ID-19.	Berkeley	1	0	0	23	1	3
ID-20.	Davis	1	0	0	23	1	3
ID-21.	Austin	1	0	0	23	1	3

From this relation, we will form two information systems, more precisely, two decision tables; they are adopted from (with changes) [Ziar93]

Example 1. Exact Rules

(4.1) We will consider an equivalence relation defined by the attribute RESULT, called decision attribute.

$$ID-i \equiv ID-j \text{ iff } ID-i.RESULT=ID-j.RESULT,$$

We have the following three equivalence classes, called decision classes

$$\begin{aligned} DECISION1 &= \{ID-1, ID-2, \dots, ID-12\} = \{1\}, \\ DECISION2 &= \{ID-13, ID-14, \dots, ID-17\} = \{2\}, \\ DECISION3 &= \{ID-18, ID-19, \dots, ID-21\} = \{3\} \end{aligned}$$

(4.2) For the conditional attributes (NEW, CASE), we consider the following equivalence relation

$$ID-i \equiv ID-j \text{ iff } ID-i.NEW=ID-j.NEW, ID-i.CASE=ID-j.CASE,$$

Then we have the following three equivalence classes, called condition classes.

$$ID-i \equiv ID-j \text{ iff } ID-i.NEW=ID-j.NEW, ID-i.CASE=ID-j.CASE,$$

Get four condition classes.



#1CASE1={ID-1, ID-2, ID-3},  
 #1CASE2={ID-4, ID-5,....., ID-12 },  
 #1CASE3={ID-13, ID-15,.....ID-17},  
 #1CASE4={ID-18, ID-15,.....ID-21}

Later, we will consider the case that each conditional class is a fuzzy set.  
 Comparing condition & decision classes, we get the dependencies

#1CASE1----->DECISION1  
 #1CASE2----->DECISION1  
 #1CASE3----->DECISION2  
 #1CASE4----->DECISION3

Or in other words, it discovers the following exact rules:

If NEW=11 and CASE=1, then RESULT=1  
 If NEW=10, and CASE=0.7, then RESULT=1  
 If NEW=12, and CASE=1, then RESULT=2  
 If NEW=23, and CASE=1, then RESULT=3

#### 4.2. Fuzzy Pawlak Information Systems

##### Example 2. Fuzzy Rules

In stead of giving an fuzzy information system, we give a fuzzy view of the information system. The equivalence classes are regarded as fuzzy sets, and hence we have derived fuzzy rules. Our results can be viewed as fuzzy version of [Ziar93]. The decision attributes be the same as in (4..1)

(4,.3) We will consider the equivalence relation defined by conditional attributes {TEST, POLL, LEVEL}

$ID-i \cong ID-j$  iff  $ID-i.TEST=ID-j.TEST$ ,  $ID-i.POLL=ID-j.POLL$ ,  $ID-i.LEVEL=ID-j.LEVEL$ ,

Then we have the following three condition classes

#2CASE1={ID-1, ID-2, ID-19, ID-20, ID-21},  
 #2CASE2={ID-3},  
 #2CASE3={ID-4, ID-5,.....ID-13}

Comparing the condition classes with decision classes, we found

(4.3.1) one exact inclusion

#2CASE2  $\subseteq_{(0)}$  DECISION1,

So, it discovers the exact rule

If TEST=1, POLL=1, and LEVEL=1, then RESULT=1------(R1)

(4.3.2) fuzzy inclusions (see Appendix 7.3)

The equivalence class is a classical set, we treat it as a fuzzy set, namely, it is represented by its characteristic function with real values in 0 or 1. The fuzzy inclusions are represented by the inequalities of membership functions. Further, we allow certain errors as long as they are within the radius  $\epsilon$  of tolerance(errors). In fact, we will call such inclusions  $\epsilon$ -fuzzy inclusions, denoted by  $\subseteq_{\epsilon}$  [Lin93b],

In this example, let us choose  $\epsilon=0.1$ . Then, we have an  $\epsilon$ -fuzzy inclusion other than 4.3.1

$$\#3\text{CASE3} \subseteq_{(0.1)} \text{DECISION1}.$$

To see the  $\epsilon$ -fuzzy inclusion, write

$$Y=\text{DECISION1}, X=\#3\text{CASE3}, Z=X \cap Y=\{\text{ID-4, ID-5, .....ID-12}\}$$

Let  $FZ = FX \cap FY$ , and  $FW = FX \cup FY$ , which express the relationships of  $Z = X \cap Y$  and  $W = X \cup Y$  in terms of characteristic functions (membership functions). Then

$$(Eq-1) \quad \sum_{u=u_1}^{u_{21}} |FX(u)/\text{Card}(FW) - FZ(u)/\text{Card}(FW)| \leq$$

$$\sum_{u=u_1}^{u_{21}} |FX(u)/13 - FZ(u)/13| = 1/13 \leq \epsilon$$

- where (1)  $u_i = \text{ID-}i, i=1, 2, \dots, 21$ , are the records  
 (2)  $u$  is a variable that varies through the records,  $u_1, u_2, \dots, u_{21}$   
 (3)  $\text{Card}$  is the (fuzzy set theoretical) cardinal numbers [Kand86].

The first sum (Eq-1) is called **deviation number**.

So, the  $\epsilon$ -fuzzy inclusion discovers the following approximate rules

$$\text{If TEST}=0, \text{ POLL}=1, \text{ and LEVEL}=1, \text{ then (approximately) RESULT}=1 \text{ --- (R2)}$$

In conclusion, the fuzzy view of rough set methodology gives us two fuzzy rules (one exact, one fuzzy). We should like to comment that one could take the attitude that the two fuzzy membership functions  $FX$  and  $FZ$  are the different representations of the same fuzzy set (both are admissible membership functions). In next computation, we will take the aging into account.

### 4. 3. Sliding Window Information System (SWIS)

**Aging Rule:** Assume the record id is numbered by the time of its arrival. For example, ID-1 arrived at time 1 and ID-2 arrived at time 2, and so forth. The aging rule is described by an aging function which is function of time. In this example, the "age" of the newest record is 1, the next 20 records are 0.9, the 21st (in reverse chronological order) is 0.1, the 22nd record and so on are 0.

We will present two examples here to illustrate the idea

#### Ex3. SWIS-Ex. 1

The Sliding Window Information System is a fuzzy information system (an instance of relational database)

$$(\text{Id-1}, 0.0), (\text{Id-2}, 0.1), (\text{Id-3}, 0.9), (\text{Id-4}, 0.9) \dots (\text{Id-21}, 0.9) \text{ plus a new data } (\text{Id-22}, 0.9), (\text{Id-23}, 1)$$

where the pair denote the record id and its "age" (the degree of membership). The new data is:

ID-22.	San Macro	1	0	0	23	1	3
ID-23.	Hayward	1	0	0	23	1	3

The decision attributes be the same as in

(4.1) but the values have changed

$$ID-i \cong ID-j \text{ iff } ID-i.RESULT=ID-j.RESULT,$$

We have the following three equivalence classes, called decision classes

$$\begin{aligned} \text{DECISION1} &= \{ID-1, ID-2, \dots, ID-12\} = \{1\}, \\ \text{DECISION2} &= \{ID-13, ID-14, \dots, ID-17\} = \{2\}, \\ \text{DECISION3} &= \{ID-18, ID-19, \dots, ID-21, ID-22, ID-23\} = \{3\} \end{aligned}$$

(4.3.3) We will consider the equivalence relation defined by conditional attributes {TEST, POLL, LEVEL}

$$ID-i \cong ID-j \text{ iff } ID-i.TEST=ID-j.TEST, ID-i.POLL=ID-j.POLL, ID-i.LEVEL=ID-j.LEVEL,$$

Then we have the following three condition classes

$$\begin{aligned} \#3\text{CASE1} &= \{ID-1, ID-2, ID-19, ID-20, ID-21, ID-22, ID-23\}, \\ \#3\text{CASE2} &= \{ID-3\}, \\ \#3\text{CASE3} &= \{ID-4, ID-5, \dots, ID-13\} \end{aligned}$$

In this example, let us choose  $\epsilon=0.1$ . Then, we have an  $\epsilon$ -fuzzy inclusion other than (4.3.1)

$$\#3\text{CASE3} \subseteq_{(0.1)} \text{DECISION1}.$$

To see the  $\epsilon$ -fuzzy inclusion, write

$$Y = \text{DECISION1}, X = \#3\text{CASE3}, Z = X \cap Y = \{ID-4, ID-5, \dots, ID-12\}$$

Let  $FZ = FX \cap FY$ , and  $FW = FX \cup FY$ , which express the relationships of  $Z = X \cap Y$  and  $W = X \cup Y$  in terms of aging functions (membership functions).

In such case the value of  $FX(u)$  in (Eq-1) is the "age" of the record  $u$ . So the formula of (Eq-1) is reduced to

$$\sum_{u=u_1}^{u_2} |FX(u)g(u)/\text{Card}(FW) - FZ(u)g(u)/\text{Card}(FW)| \leq \epsilon$$

Note that

$$\text{Card}(FW) = 0.9 \cdot 12 + 1 = 11.8$$

$$\sum_{u=u_1}^{u_2} |FX(u)g(u)/11.8 - FZ(u)g(u)/11.8| = 0.9/11.8 \leq \epsilon$$

$$u=u_1$$

Note that  $FX(u)g(u)$  is the membership function of the record  $u$ . Recall that the left-most sum is the deviation number. If the deviation number of a rule is fluctuated within the tolerance, such as  $\epsilon$ , and other "signature" data (repeating records) are unchanged, then the system can proceed normally, otherwise there is "intrusion". We will report full experimental results in the near future. For now, let us examine the case which has intrusion.

**Ex 4. SWIS-Ex. 2.** The example of "blind append" virus

In this example, we examine the case when a virus blindly repeat "infinitely" many times of a user's last command. In other words, the same record repeatedly enter the audit trail.

Let us first recall the aging rules. The "age" of the newest record is 1, the next 20 records are 0.9, the 21st(in reverse chronological order) is 0.1, the 22nd record and so on are 0.

The Sliding Window Information System is a fuzzy information system (an instance of relational database)

(Id-1, 0.0) (Id-2, 0.0), ... (Id-16, 0.1) (Id-17, 0.9),..... (Id-36,0.9) (Id-37,1)

where the pair denote the record id and its "age" (the degree of membership). The new data from Id-22 to Id-28 are the "same":

ID-22.	San Macro	1	0	0	23	1	3
ID-23.		1	0	0	23	1	3
			:				
ID-37.		1	0	0	23	1	3

The decision attributes be the same as in

(4,.1) but the values have changed

$$ID-i \cong ID-j \text{ iff } ID-i.RESULT=ID-j.RESULT,$$

We have the following three equivalence classes, called decision classes

$$\begin{aligned} \text{DECISION1} &= \{ID-1, ID-2, \dots, ID-12\} = \{1\}, \\ \text{DECISION2} &= \{ID-13, ID-14, \dots, ID-17\} = \{2\}, \\ \text{DECISION3} &= \{ID-18, ID-19, \dots, ID-37\} = \{3\} \end{aligned}$$

(4,.3.3) We will consider the equivalence relation defined by conditional attributes {TEST, POLL, LEVEL}

$$ID-i \cong ID-j \text{ iff } ID-i.TEST=ID-j.TEST, ID-i.POLL=ID-j.POLL, ID-i.LEVEL=ID-j.LEVEL,$$

Then we have the following three condition classes

$$\#3\text{CASE1} = \{ID-1, ID-2, ID-19, ID-20, ID-21, \dots, ID-37\},$$

#3CASE2={ID-3},  
 #3CASE3={ID-4,ID-5,.....ID-13}

In this example, let us choose  $\epsilon=0.1$ . Then, we have an  $\epsilon$ -fuzzy inclusion other than (4.3.1)

(Inc-1) #3CASE3  $\subseteq_{(0.1)}$  DECISION1.

(Inc-2) #3CASE1  $\subseteq_{(0.1)}$  DECISION3

To see the first  $\epsilon$ -fuzzy inclusion (Inc-1), write

$$Y=DECISION1, X=\#3CASE3, Z=X \cap Y=\{ID-4, ID-5, \dots, ID-12\}$$

Let  $FZ = FX \cap FY$ , and  $FW = FX \cup FY$ , which express the relationships of  $Z = X \cap Y$  and  $W = X \cup Y$  in terms of aging functions (membership functions).

In such case the value of  $FX(u)$  in (Eq-1) is the "age" of the record  $u$ . So the formula of (Eq-1) is reduced to

$$\sum_{u=u_1}^{u_37} |FX(u)g(u)/Card(FW) - FZ(u)g(u)/Card(FW)| \leq$$

Note that

$$Card(FW) = 0.0$$

$$\sum_{u=u_1}^{u_37} |FX(u)g(u)/0.0 - FZ(u)g(u)/0.0| = 0.0/0.0 \quad ?? \quad \epsilon$$

(Note that  $FX(u)g(u)$  is the membership function of the record  $u$ ). (Eq-1) no longer stay within the radius of tolerance. The fuzzy inclusion is no longer true. So the fuzzy rule disappears from the sliding window. However, a new rule is appearing.

To see the second  $\epsilon$ -fuzzy inclusion (Inc-2), write

$$D=DECISION3, C=\#3CASE1, Z=C \cap D=\{ID-4, ID-5, \dots, ID-12\}$$

Let  $FZ = FC \cap FD$ , and  $FW = FC \cup FD$ , which express the relationships of  $Z = C \cap D$  and  $W = C \cup D$  in terms of aging functions (membership functions).

In such case the value of  $FC(u)$  in (Eq-1) is the "age" of the record  $u$ . So the formula of (Eq-1) is reduced to

$$\sum_{u=u_1}^{u_37} |FC(u)g(u)/Card(FW) - FZ(u)g(u)/Card(FW)| \leq$$

Note that

$$Card(FW) = 0.1 + 0.9 * 20 + 1 = 19.1$$

$$\sum_{u=u_1}^{u_2} |FC(u)g(u)/19.1 - FZ(u)g(u)/19.1| = 0.1/19.1 + 0.9/19.1 + 0.9/19.1 \leq \epsilon$$

(Note that  $FC(u)g(u)$  is the membership function of the record  $u$ ). (Eq-1) satisfy the radius of tolerance. The fuzzy inclusion become a new rule (or a new pattern). So the "signature" of a user definitely changed, so an intrusion is occurring. We will not address the complexity problem. However, as we have discuss in the beginning part of this paper, we have shown that , based on rough set theory, there are only finitely different many records in a sequence of records. We believe that the complexity problem can be controlled via rough set representation of data. We will discuss in near future.

## 5. Applications to Audit Trails

From Section 3, we are assured that, we can find the repeating records for each user. We could keep a log on the following information:

### (a) The repeating records, and its frequency, or the occurrence patterns

After we have a sufficient collection of data on a user, we can make a data analysis (as in Section 4), and find some hidden

### (b) The fuzzy repeating relationships(rules) in the incoming data.

We will keep these information, fuzzy rules and the deviation number on each rules (see Ex. 2) in the system log.

Now as the data are continuously collected and faded away (aging), as the sliding window slides. The fuzzy rules may stay constant, although the deviation number may fluctuate within the tolerance level. However, any significant changes on the data (a) or (b) are a signal of abuse or misuse. So this methodology provides us a foundation for anomaly detection.

## 6 Appendix- Rough Sets

### 6.1. Equivalence Relation

A binary relation is an equivalence relation iff it is reflexive, symmetric and transitive. For every equivalence relation there is a partition and vice versa. Let  $R$  be a given equivalence relation over  $U$ . The family of all equivalence classes is a set, it is called quotient set and denoted by  $U/R$ . There is a natural projection from  $U$  to  $U/R$ .

$$NQ: U \longrightarrow U/R$$

defined by  $NQ(u) = [u]$  (read as natural quotient), where  $[u]$  is the equivalence class containing  $u$ . We should note here that  $[u]$  has dual roles; it is an element, not a subset, of  $U/R$ , but it is a subset of  $U$ . In [2], elements in  $U/R$  are called names of equivalence classes.

Let us denote the complete inverse image of  $NQ$  by

$$INV.NQ(q) = \{u : NQ(u) = q\} = [u]$$

or more generally, for a subset  $X$  of  $U/R$

$$\text{INV.NQ}(X) = \{u : \text{NQ}(u) \text{ is in } X\}$$

Note that  $\text{INV.NQ}(q)$  is an equivalence class and  $\text{INV.NQ}(X)$  is a union of equivalence classes.

Example 1. Let  $Z$  be integers. Let  $R$  denote the equivalence relation called congruence mod  $m$ . That is,

$$x R y \text{ if } x - y \text{ is divisible by } m.$$

Let  $m = 4$ . Then the equivalence classes are

$$[0] = \{\dots -8, -4, 0, 4, 8, \dots\}$$

$$[1] = \{\dots -7, -3, 1, 5, 9, \dots\}$$

$$[2] = \{\dots -6, -2, 2, 6, 10, \dots\}$$

$$[3] = \{\dots -5, -1, 3, 7, 11, \dots\}$$

In other words,  $[0], [1], [2], [3]$  is a partition for the integers  $Z$ . The quotient set of this equivalence relation is denoted by  $Z_m$ .  $Z_4 = \{[0], [1], [2], [3]\}$ .

## 6.2. Rough Sets

Let  $U$  be the universe of discourse. Let  $R\text{Col}$  be a finite Collection of equivalence Relations  $R$  over  $U$ . In general we will use Pawlak's terminology and notations. An ordered pair

$$K = (U, R\text{Col})$$

is called a knowledge base over  $U$  (In most cases, there is only one equivalence relation  $R$  in  $R\text{Col}$ , so  $K = (U, R)$ ). A subset  $X$  of  $U$  is called a concept. For an equivalence relation  $R$ , an equivalence class is called  $R$ -elementary concept,  $R$ -elementary set,  $R$ -basic category or  $R$ -elementary knowledge (about  $U$  in  $K$ ). The empty set is assumed to be elementary. A set which is a union of elementary sets is called  $R$ -definable or  $R$ -exact. A finite union is called composed set in  $U$ . The set of equivalence classes is the quotient set  $U/R$ . There is a neat correspondence between the elementary sets of  $U$  and the quotient set  $U/R$ . Each elementary set in  $U$  corresponds to an element in  $U/R$ .

Let  $S\text{Col}$  be a nonempty SubCollection of  $R\text{Col}$ . The intersection of all equivalence relations in  $S\text{Col}$ , denoted by  $\text{IND}(S\text{Col})$ , is an equivalence relation and will be called an indiscernibility relation over  $S\text{Col}$ . The quotient set  $U/\text{IND}(S\text{Col})$  will be abbreviated by  $U/S\text{Col}$ . Equivalence classes of  $\text{IND}(S\text{Col})$  are called basic categories (concepts) of knowledge  $K$ . A concept  $X$  is exact in the knowledge base  $K$  if there exists an equivalence relation  $R$  in  $\text{IND}(K)$  such that  $X$  is  $R$ -exact, where  $\text{IND}(K)$  is the collection of all possible equivalence relations in  $K$ , that is,

$$\text{IND}(K) = \{\text{IND}(S\text{Col}) : \text{for all } S\text{Col}'\text{'s in } R\text{Col}\}.$$

For each  $X$ , we associate two subsets, upper and lower approximation:

$$L\_APP(X) = \{u : [u] \text{ is a subset of } X\}$$

$$U\_APP(X) = \{u : [u] \text{ and } X \text{ has non-empty intersection}\}$$

A subset  $X$  of  $U$  is definable iff  $U\_APP(X) = L\_APP(X)$ . The lower approximation of  $X$  in  $U$  is the greatest definable set in  $U$  contained in  $X$ . The upper approximation of  $X$  in  $U$  is the least definable set in  $U$  containing  $X$ .

As Pawlak pointed out that the equivalence classes form a topology for U (it will be called Pawlak topology). So we can rephrase the upper and lower approximations as follows:

$$\begin{aligned} L\_APP(X) &= \text{Interior point of } X \\ &= \text{The largest open set contained in } X \\ U\_APP(X) &= \text{Closure of } X \\ &= \text{The smallest closed set containing } X. \end{aligned}$$

Rough set theory serves two functions: one is a generalization of the equality which leads to classification, the other is the approximation in Pawlak topology.

## 7. Appendix -Fuzzy Sets

The theory of fuzzy sets deals with subsets where the membership function is real valued, not boolean valued. Intuitively the fuzzy subsets have no well defined boundaries in the universe of discourse. Let U be the universe of discourse. Then a fuzzy set FX is an ordered pairs:

$$FX = (U, FX)$$

where  $FX: U \rightarrow [0,1]$  is a function.. If both  $FX(0)$  and  $FX(1)$  are nonempty, we call the fuzzy set normal [Zimm90]. Note that FX is a fuzzy set and  $FX()$  is a membership function of FX. When context is clear, we may use FX both as the fuzzy set or the membership function. If the membership function assumes only real values 0 and 1, the fuzzy set is a classical set. An element x is said to be fuzzily belonged to FX if  $FX(x) > 0$  and x is said to be absolutely not belong to FX if  $FX(x) = 0$ .

### 7.1. Quasi Classical Sets

Let X be a classical set. We would like to consider the membership function

$$c*X: U \rightarrow [0,1]$$

defined by  $(c*X)(u) = c*(X(u))$  for constant c, where \* is the multiplication of real numbers. Then  $c*X$  is a special type of fuzzy set, we will call it quasi classical set. The meaning of such quasi classical set is that an object x in U is either not in X or the degree (possibility, probability) of its membership is c. We also would like to consider the "union" of quasi classical sets:

$$(a*X \cup a*Y)(x) = \text{MAX}(a*X(x), b*Y(x))$$

The union of quasi-classical sets are the so-called "step functions"

### 7.2. Fuzzy Rough Sets

Let R be an equivalence relation over U. Let  $FCol(U/R)$  be the Collection of all Fuzzy sets over  $U/R$ . Then the natural projection induces a subfamily of fuzzy sets on U.

$$\begin{array}{ccc} NQ & FX & \\ U \rightarrow & U/R & \rightarrow [0,1] \end{array}$$

$$\text{SubFCol}(U) = \{NQ*FX: FX \text{ is in } FCol(U/R)\}$$

where \* is the composition of functions. This subfamily  $\text{SubFCol}$  is the family of all R-exact fuzzy sets.



SubFCol is precisely, the "step functions" We would like to have more explicit description of this SubFCol of fuzzy sets on U. Let the membership function of the equivalence classes (R-elementary sets) be

$$EC_i: U \longrightarrow [0, 1], i = 1, 2, \dots, n.$$

Since  $EC_i$  (i-th equivalence class) is a classical set, its membership function assumes 0 and 1 only; it may be referred to as classical equivalence class.

A fuzzy set in U

$$FX: U \longrightarrow [0, 1]$$

is R-definable iff FX is in SubFCol(U). That is, FX is constant function on every  $EC_i$ . In other words, FX is a linear sum of classical sets. Using functional notations, FX is R-definable iff

$$FX = c_1 * EC_1 + c_2 * EC_2 + \dots + c_n * EC_n.$$

The R-definable fuzzy set may also be called R-exact. A fuzzy set (concept) is R-undefinable iff it is not R-definable; it may also be called R-inexact.

For each FX, we associate two subsets, upper and lower approximation:

$$\begin{aligned} U\_APP(FX) &= \inf\{FY: FX \leq FY \text{ for all } FY \text{ in } CQE\} \\ L\_APP(FX) &= \sup\{FY: FX \geq FY \text{ for all } FY \text{ in } CQE\} \end{aligned}$$

Such pairs are called fuzzy rough sets.

### 7.3. Real World Fuzzy Sets

Let  $U = \{u_1, u_2, \dots, u_n\}$  be the universe. For a given small number  $\epsilon$  (called radius of tolerance/error), Let FX and FY be two membership functions. Then both functions are said to be representing the same real world fuzzy set, if

for given  $\epsilon$ ,

$$\sum_{u=u_1}^{u_n} |FX(u) - FY(u)| / \text{Card}(FW) \leq \epsilon$$

where  $FW = FX \cup FY$ , and  $\text{Card}(FW)$  is the cardinality of fuzzy set FW. Roughly, the "total difference" is relatively small compared to "the total measure" However, this admissibility is *not* an equivalence relation.

### References

- [DuPr90] Didier Dubois and Henri Prade. Rough fuzzy sets and fuzzy rough sets. International Journal of General Systems, pages 191-209, 1990.
- [Kand86] Abraham Kandel (1986), Fuzzy Mathematical Techniques with Applications, Addison-Wesley, Reading Massachusetts, 1986
- [Lamb90] Michael van Lambalgen, The Axiomatization of Randomness, The Journal of Symbolic logic, Vol. 55, No 3, Sept., 1990.

- [LiVi88] Ming Li and Paul Vitanyi, Two decades of applied Kolmogorov Complexity, Proceeding of third IEEE Structure in Complexity theory Conference, 1988.
- [Lin92] T.Y. Lin, Topological and Fuzzy Rough Sets, Kluwer Academic Publishers, 1992 (A chapter of Decision support by Experience - Application of the Rough Sets Theory, R. Slowinski (ed.)
- [Lin93a] T. Y. Lin, Rough Patterns and Intrusion Detection Systems, Journal of Foundation of Computer Sciences and Decision Supports, 1993.
- [Lin93b] T. Y. Lin, Coping with imprecise information – "fuzzy logic", Downsiaing Expo, Santa Clara, Aug. 4-6, 1993.
- [Lunt90] T. F. Lunt and Ann Tamaru, F. Gillman, R. Jagganathan, C. Jatali, H. Javitz, and A. Valdes, and P. Neumann, A real-time Intrusion Detection Expert System. SRI technical report, 1990
- [Lunt90] H. Javitz, A. Valdes, T. F. Lunt and Ann Tamaru, Next Generation Intrusion Detection Expert System. SRI technical report, 1993.
- [Pawl82] Z. Pawlak , Rough sets. Int. J. Computer and Information Sci. 11, 341-356, 1982
- [Pawl90] Z. Pawlak, Rough sets - Theoretical Aspects of Reasoning about Data, Kluwer Academic Publishers, 1990.
- [Ziar93] W. Ziarko, 1993, Variable Precision Rough Set Model, Journal Computer and System Science, 39-58, 1993

**The Development of  
Generally Accepted System Security Principles (GSSP)  
NIST's Approach**

The National Performance Review (NPR) which Vice President Al Gore has actively supported has recommended as part of the National Information Infrastructure (NII) that the National Institute of Standards and Technology develop Generally Accepted System Security Principles (GSSP) for the federal government. NIST is working under the auspice of the Information Systems Security Association (ISSA) in coordination with OMB and with technical assistance from NSA to plan and coordinate the development of generally acceptable security principles. These principles are to be applied in the use, protection, and design of government information and data systems, particularly front-line systems for electronically delivering service to citizens.

Chair:           Marianne Swanson  
                  National Institute of Standards and Technology

Panelists:

**Will Ozier, ISSA GSSP Committee Chair**

For the past 18 months, ISSA has led an international group of security experts in developing the GSSP. Within this short timeframe, the committee has developed a preliminary GSSP, begun cataloging IT security foundation documents and determining the relationship to other IT security initiatives. These projects along with their status will be described.

**Marianne Swanson, National Institute of Standards and Technology**

NIST has been an active player in the ISSA GSSP Committee since its inception and it is with this effort already underway, that NIST will carry out the recommendation made in the NII Report. NIST's progress in developing the pervasive principles will be discussed.

**Ed Roback, National Institute of Standards and Technology**

The draft NIST IT Security Handbook will play an integral part in the GSSP. The Handbook's audience, intended function and contents will be described in detail by one of the principle authors.

**Barbara Guttman, National Institute of Standards and Technology**

The key role that the NIST IT Security Handbook will play in the GSSP process will be discussed. How the Handbook ties in with many other NIST IT security documents will also be presented.

# **Product and System Certification in Europe**

**Chair: Mr. Klaus J. Keus, BSI, Germany**

## **Introduction / Summary**

**Mr. Klaus Keus, BSI, Germany**

The European Evaluation and Certification and its application schemes are working successfully since several years, by apply national and -since 3 years- the European harmonized IT-Security Evaluation Criteria (ITSEC) for product and system evaluation, and act on a common evaluation methodology (ITSEM).

Different users in government and private institutions are asking for certified products in a wide variety of application areas. Solutions for operating systems, databases, network components or applications, implemented in SW, firmware or HW, satisfy different security requirements such as confidentiality, integrity and availability. The usage of certified products and systems is not restricted to government and military confidentiality anymore. It expanded to new public and private areas such as telecommunications, banking and insurance, traffic control, medical systems and nuclear power stations, including the aspects of IT-Safety and dependability.

As the range of certified products expands and their usage in different applications increases, the number of involved parties and nations is becoming larger. New experienced partners, e.g. TNO as a representative of the Netherlands, will contribute their longtime experience as testing laboratory for IT. The large experience using the ITSEC -in combination with the common methodology- for SW-evaluation allows the Europeans to extend its applicability for HW- and system evaluation, and platform independency, as well as SW portability and interoperability. The evaluation of an IT-System as a composition of different -evaluated and certified- components and products is based on a relationship model in respect with correctness and effectiveness aspects.

The actual European scheme for product and system evaluation is mainly based on the ITSEC. With the harmonization of the different IT-security evaluation criteria into international harmonized ones, e.g. the Common Criteria (CC), new alternatives or enlargements concerning the scheme have to be discussed. The integration of IT-security evaluation and certification into the existing general IT-development and validation process has to be checked. First constructive approaches of vendor declaration or evaluation as a complement to third party evaluation / certification (e.g. performed by an independent body (e.g. government body)) have to be considered.

The practical usage and the advantages of presently installed quality assurance / management system for IT-development, such as ISO 9001, ISO 9000 part 3 and other quality standards will be presented and the benefits of combining product-oriented IT-security criteria requirements with process-related quality standards will be explained.

## **Status of European Certification Schemes and Mutual Recognition**

**Mrs. Angelika C. Jennen, BSI, Germany**

The European Certification Schemes have been working for several years and have gained experience in applying criteria and procedures to many areas of IT-security covering product and system evaluation for government and private use. The trends are: transition from classical operating systems

and confidentiality aspects to application based security, including integrity and availability requirements, inclusion of telecommunication, traffic control, medical applications with a growing focus on safety aspects. The criteria used have proven their applicability to all mentioned areas. The increasing number of re-evaluations / -certifications of new product releases has demonstrated the suitability of the decomposition concept "security enforcing - relevant - non relevant". Several recognition agreements were signed or are close to signature. A common understanding of the equivalence of evaluation procedures and results has been achieved.

**Certification Maintenance under ITSEC**  
**Mr. Jeremy Wilde, Logica, UK**

The presentation will address the current approach to certification maintenance in the UK, drawing on examples of products which have undergone multiple evaluations. The paper will identify the main requirements of a maintenance scheme, and will address the requirements on both sponsor and evaluator to ensure quick, cost-effective reevaluations. It will then go on to suggest possible changes to the current procedures, with a view to harmonising European and American approaches under the Common Criteria.

Finally the paper will consider the wider implications of maintaining certificates through a move from one set of criteria to another - an issue which will become key for developers as the Common Criteria become the established standard.

**Security Evaluations in the Netherlands - An evaluators view on globalisation of elvaluations**  
**Dr. Paul L. Overbeek - TNO Physics and Electronics Laboratory, The Netherlands**

The paper talks about the experience in trial evaluations of security in IT products against international criteria, performed by a well experienced laboratory in The Netherlands, called TNO (TNO Physics and Electronics Laboratory).

They started with ITSEC trial evaluations in 1993. In the introduction TNO will share the misery and joy in setting up these evaluations and will explain the experience TNO had so far. The paper will concentrate on the implications of the current "globalisation" of security evaluations including issues as:

- 1 Changing positioning and role of "national authorities"
- 2 Wider audience for security evaluation criteria:  
incorporation of day-to-day business needs
- 3 Developments in IT imply changing needs for security evaluations
- 4 Affordable security: low and cheap entry for evaluations

**Effectivness in French Evaluations**  
**Laurent Borowski, CR2A, France**

This evaluation was conducted by the french governmental evaluation facility CESSCE (Centre d'Evaluation de la Sécurité des Systèmes informatiques Commerciaux) which sub-contracted the main part of the technical work to CR2A, a company which has applied to be an ITSEC.

The target of evaluation is composed of a PC electronic board and of an optical electronic card used for identification and authentication. The main interest of this work is to assess the suitability of ITSEC criteria to evaluation of hardware components.

### **The relation between Correctness and Effectiveness in System Composition**

**Mr. Mats Ohlin**

**Swedish Defense Materiel Administration (FMV)**

**Electronic Systems Directorate, Sweden**

Traditionally assurance is described as the combination of correctness in the implementation of the security functions on one hand and the effectiveness of the combination of those functions. Also the (minimum) strength of mechanism is assessed (this specific aspect is discussed separately later in the paper).

In the ITSEC view the correctness evaluation must be completed before the effectiveness of the TOE can be finally established.

When evaluating a complex TOE (such as a multiuser, timesharing OS) it is natural to regard the TOE as being composed by smaller components. In a generalized system view these components may be built up a composition of internal, "smaller" components. Ultimately, there is a level where further decomposition is no longer possible. We denote these components as basic components.

This paper talks about the relationship between the correctness and the effectiveness aspects in a system composed by different -evaluated and certified- products.

### **Evaluation of Platform Independence**

**Mr. Peter Cambell-Burns, Admiral Management Services Limited, UK**

In the UK, the need for cost effective development and evaluation has resulted in a trend towards the use of evaluated commercial-off-the-shelf (COTS) products in secure systems. However, a product's certificate will only be valid for a restricted set of hardware platform/operating system combinations. This poses a problem for the product developer who must decide for which platform or platforms the product is to be evaluated. This decision must be balanced by the cost of the evaluation which will increase with the number of platforms. The user of a secure system needs to be able to match the products available to the system requirements. These requirements will include not only the functionality of the product, but also the environment in which the product is intended to operate. If the operational requirements cannot be met by an existing evaluated product, then the user will have to rely on bespoke software or let the security requirements dictate the solution to the non-security requirements.

Software developers and system integrators have long recognised the benefits of software portability and interoperability. Towards the goals of portability and interoperability, a range of well defined standards have evolved which enable software to be developed with an ever increasing degree of

platform independence. It is important therefore that software evaluation is able to keep pace with these developments. For example, a developer may be able to demonstrate that a particular assurance level applies to a product when it runs on any platform which satisfies a given specification. The practicability of evaluating a claim of platform independence under the ITSEC scheme has been assessed. This has required a detailed examination of issues such as reuse of evaluation results and impact analysis. This paper introduces the concept of a platform independence evaluation and proposes an approach for developing and evaluating platform independent products.

**Vendor Assurance vs. 3rd Party Evaluation: A Constructive Approach**  
**Dr. Heinrich Kersten, BSI, Germany**

The majority of existing security evaluation criteria is based on 3rd party evaluation, i.e. any evaluation result is achieved by labs not participating in or contributing to the product's development. A deeper analysis of e.g. the ITSEC criteria reveals that there are several "evaluator's actions" not corresponding to the specific product to be evaluated but relate to the development and quality assurance processes at the vendor's site. These process requirements are also objectives in ISO 9000 certifications and other general product quality standards. Therefore, it is an obvious question how ISO 9000 procedures existing at a vendor's development lab interfere with a product evaluation and certification according to ITSEC.

A constructive approach is presented combining the benefits of the product-oriented security criteria and the process-related quality standards, reducing evaluation efforts but maintaining an adequate level of assurance.

## **New Concepts in Assurance Panel**

### **Abstract**

This panel session will discuss new concepts in the area of assurance for IT security products and systems. The panel presentations will include the results of two recent workshops on assurance and new approaches to gaining assurance from evaluations and process.

### **Panel Chair:**

Pat Toth, NIST

### **Panelists:**

Lynne Ambuel, National Security Agency

Ms. Ambuel will discuss the results of the Invitational Workshop on Information Technology (IT) Assurance and Trustworthiness which was held March 21-23, 1994 in Williamsburg, Virginia.

Deitra Kimpton, CSE - Canada

This panel presentation will provide an overview of the proceedings of the International Invitational Workshop on Developmental Assurance which was held June 16-17, 1994 in Ellicott City, Maryland.

Ken Rochon, National Security Agency

Mr. Rochon will present innovative experimental evaluation approaches that are being considered by the Trusted Products Evaluation Program (TPEP). These innovative approaches to evaluation present a departure from the traditional methods of evaluation.

Karen Ferraiolo, ARCA Systems

Ms. Ferraiolo will discuss how assurance is viewed today, the need to look at assurance as multi-dimensional, the relevance of process assurance and the Security Engineering Capability Maturity Model's contribution to improvements in assurance production and measurement.



**PANEL**  
**New Challenges for C&A:**  
**The Price of Interconnectivity and Interoperability**

<b>Chairs:</b>	Ellen Flahavin NIST Building 224, Room 245 Gaithersburg, MD 20899 301-975-3871 flahavin@csmes.ncsl.nist.gov	Joel Sachs ARCA 10320 Little Patuxent Pkwy., Suite 1005 Columbia, MD 21403 410-715-0500 sachs@arca.md.com
----------------	--	--

**Panelists:** Annabelle Lee, MITRE  
Ellen O'Connor, IRS  
Hector Ruiz, DISA  
Steven Schanzer, CIA  
Ed Springer, OMB

Several key trends have emerged in terms of our future use and reliance on technology. Most significant is the drive for interconnectivity and interoperability within and across information systems, which are best exemplified in the movement from stove-pipe systems to a consolidated infrastructure, e.g., the DII, GII, NII, and III. Technology itself continues to evolve at rapid rate. As a result of continuously changing competitive world, we now see that the missions and organizations, which are associated with these systems, are also evolving, e.g., corporate re-engineering and continuous process improvement. All of these trends result in major and new challenges for the certification and accreditation.

This panel will examine such challenges as well as alternatives to address them. It will prove informative to those individuals who need to perform certification and accreditation today and plan for tomorrow. The panelists will address a number of specific questions associated with certification and accreditation in a highly interconnected and interoperable world. This will be done from a variety of Government perspectives, including civil, defense, intelligence, and multi-agency.

Questions will focus on what is done today, what needs to be done in the near-term, and what needs to be done in the distant future. They include:

- **C&A Orientation:** Should we a) continue to focus on individual systems with attention to their external connectivity or b) focus on the entire infrastructure with emphasis on its entities?
- **Risk Management:** Should we a) continue a risk avoidance philosophy or b) adopt a risk tolerance one?
- **C&A Scope:** Should we a) continue view C&A as only certification and accreditation activities or b) expand it to all activities that support certification and led to accreditation?
- **C&A Flexibility:** Should we a) continue to allow C&A to be conducted with flexibility and discretion or b) mandate a rigid process?
- **C&A Methodology:** Should we a) leave the implementation of C&A to the services and agencies or b) require a uniform set of procedures based on assurance needs?
- **C&A Level of Effort:** Should we a) leave the implementation of C&A to the services and agencies or b) require a minimum effort based on assurance needs?
- **C&A Expertise:** Should we place minimum standards on certifiers and accreditors? By individuals or organizations? With licensing?
- **C&A Tools:** Should we invest in tools to a) assist in the execution of C&A, b) automate C&A activities, or c) abandon tools altogether?
- **C&A Coordination:** Should we establish some form of coordination for C&A? Centrally?

The Department of Defense Goal Security Architecture  
W. Timothy Polk, Chair  
National Institute of Standards and Technology  
wpolk@nist.gov

The Department of Defense Goal Security Architecture (DGSA) is a generic architecture for secure distributed processing. The DGSA is derived from the DoD Information System Security Policy and reflects requirements for the support of multiple security policies, distributed information processing, connectivity by common carrier, users with different security attributes, and resources with varying degrees of security protection. Mission-specific security architectures derived from the DGSA form the basis for implementing secure distributed systems.

Increased interoperability through standards development is one of the benefits projected as a result of the DGSA. NIST is working with DISA and NSA to develop a standards-based transition strategy for the development of systems conforming to the DGSA. NIST is also examining the DGSA to evaluate the DGSA's applicability to civilian security requirements.

*The Department of Defense Goal Security Architecture (DGSA)*  
Richard McAllister, National Security Agency

The DGSA is a generic security architecture, offering guidance and structure to those developing specific architectures for particular missions. The DGSA views the system as *Local Subscriber Environments* (LSEs) and *Communication Networks* (CNs.) The DGSA is based upon a strategy for allocating security services to these components and several fundamental security concepts.

*The DGSA Overall Transition Strategy*  
Carl Deutsch, National Security Agency

The DGSA Overall Transition Strategy is a plan for migrating from currently available solutions those meeting the architectural principles of the DGSA. This strategy encompasses nine transition teams addressing standards, product development, research, security management, local subscriber environments, communication networks, certification, policy, and training.

*Security Standards for DGSA-based Architectures*  
Janice Schafer, Defense Information Systems Agency

DISA is leading the Security Standards Transition Team's development of a standards-based transition strategy for the development of systems conforming to the DGSA. Development and implementation of DGSA-conforming standards will provide a cost-effective incremental upgrade path from current systems to the functionality specified in the DGSA.

*DGSA's Applicability to non-DoD Environments*  
Jim Coyle, Booz-Allen & Hamilton

The DGSA encompasses principles and common sense concepts applicable to non-DOD (civilian government and commercial) security environments, as well as DoD classified environments. This talk will highlight the importance of security contexts and security associations and show how they are bound by security management. System developers can leverage these principles and enhance the security of non-DoD environments by developing mission-specific target architectures consistent with the DGSA and migrating to those architectures.

Panel Title: MULTILEVEL SECURITY (MLS) - CURRENT APPLICATIONS,  
FUTURE DIRECTION

Length: 3 hours (2 panels)

Panel Summary:

This panel covers applications and use of multilevel security (MLS) solutions fielded at the US Unified Commands by the Department of Defense MLS Program, and an overview of the NSA Multilevel Information System Security Initiative (MISSI). MLS applications highlighted include the Operations/Intelligence Interface, the Two-Level Workstation, and the Standard Mail Guard. Presentations given by panelists will cover requirements satisfied by MLS applications, operational utility, accreditation issues, and management of residual risk. The MISSI overview will cover how DoD will progress from these current applications to more extensive MLS capabilities.

Panel Members and Statements (NOTE: Panel members invited but who have not confirmed noted with INVITED. If the specific person cannot attend, someone else from their organization will):

Chair: COL John J. Sheldon, DISA. MLS technologies provide a significant operational benefit to warrior command and control systems. Introductory presentation will briefly cover the DoD MLS Program, the common, high-priority requirements of the US Unified Commands, the near-term solutions being fielded, and research and development efforts leading to future solutions.

Mr. John Wiand, USSOCOM (INVITED). Implementation and utilization of the Operations/Intelligence Interface and the Standard Mail Guard at USSOCOM from a user's perspective.

Mr. Russ Myers, USACOM. Operations/Intelligence Interface fielding at USACOM: operational benefits and lessons learned during USACOM Exercise Agile Provider 94 and the Joint Warrior Interoperability Demonstration (JWID)-94.

Ms. Emily Klutz, USACOM (INVITED). The Two-Level Workstation: user's experience in bridging the Top Secret WWMCCS LAN and ACOM's Secret-level Command and Control LAN.

LTC Tom Surface, USPACOM. MLS Fieldings in USPACOM: lessons learned on the Operations/Intelligence Interface in the Joint Intelligence Center, Pacific, and the Command and Control Releasability Guard in US Forces, Korea.

Maj Kevin Newland, USSPACECOM. Utility, risks, and accreditation issues in fielding the Standard Mail Guard in USSPACECOM.

Mr. Paul Woodie, NSA. MISSI offers technologies that respond to the requirements for secure EMail and messaging. This overview will cover how DoD will progress from current applications to more extensive MLS messaging capabilities.

Mr. Charles West, DISA. Today's technologies lay the groundwork for tomorrow's solutions. This presentation will address how DoD is responding to requirements, and the solutions being addressed for future fieldings.

Mr. Woodie will provide an overview of a family of compatible network security components being developed by the NSA under an umbrella called the Multilevel Information Systems Security Initiative (MISSI). These components can be applied to networks as a type of "security overlay" to provide a feature known as "writer-to-reader" security for existing data communication networks.

This session will explore the concept of "writer-to-reader" security, including how it is achieved and applied to provide an increasing set of both security functionality and security assurance. Included in the MISSI are direct security provider components both at the workstation and at network boundaries (e.g., between a LAN and a WAN). These include workstation security cards, the Secure Network Server, and NES network encryption products.

The MISSI also includes a family of compatible software components to allow more efficient and automated security management for the overall network. These components are collectively called Network Security Management. These products are: 1) Local Authority Workstation, 2) Audit Manager, 3) Rekey Manager, 4) Directory Server, and 5) Mail List Agent.

Included in the session will be a report on the overall status of the MISSI and the products that have been fielded to date.

**Panel Title:** Prominent Industry-Sponsored Security Architectures Currently Under Development

**Panelist:** Michael McChesney, SecureWare, EGSA  
Roger Schell, Novell, GSA  
Bill Dwyer, Hewlett-Packard, DCE

**Panel Summary:**

This panel consists of representatives from three companies which are proactively implementing security architectures to meet their customer's expanding global network security requirements: SecureWare's EGSA (Extended Global Security Architecture), Novell's GSA (Global Security Architecture), and Hewlett-Packard's DCE (Distributed Computing Environment). The goal of this panel is to discuss why such additional security services are needed, and explore how each of these new security architectures is meeting the increasingly critical security requirements of customers.

Enterprises of all types, whether commercial, non-profit, or government related, are becoming more dependent upon distributed networks of computers and other information processing equipment for their mission critical applications. Sometimes these networks develop over time in an ad hoc manner as groups within the enterprise purchase equipment to meet their own specialized needs and then attempt to tie that equipment into the enterprises' backbone network. Sometimes these networks develop in a controlled, top down manner as the enterprise carefully plans to "downsize" their applications from mainframes to a distributed system. Regardless of how their network evolved, most enterprises with distributed computing systems are currently experiencing common problems which require expanded security services to solve. These common problems include:

a.) Cohesive Distributed Computing Infrastructure

Large enterprise networks are often constructed from a variety of different system types, such as DOS, Windows, and Macintosh PCs, Unix workstations, mini computers, mainframes, etc... The lack of a common, cohesive infrastructure for distributed computing limits the interoperability and integration that can be achieved between the different systems, and makes the development of cross-platform applications difficult.

b.) Administration and Management

It is difficult and very labor intensive to administer and manage the user accounts and system resources available on the individual computers throughout the network because of the distributed nature of the network and the vendor-specific mechanisms for administering them.

c.) Identification, Authentication and Unitary Login

Most types or brands of computers expect to be directly responsible for identifying and authenticating any user to which they grant access to their resources. If a user desires access to a resource or service on some other host, he must perform an additional "login" operation to authenticate himself to that host. There is no single authority or mechanism for uniquely identifying and authenticating a user to all computers throughout an enterprise such that the user need perform just a single, "unitary login", operation.

d.) Security Audit and Analysis

In the distributed environment it is difficult to detect and analyze attacks against an enterprises' information and resources. Doing so requires that audit records from all hosts throughout the network be centrally collected and analyzed by sophisticated, automated tools. Processing such a vast quantity of information in a timely manner requires a hierarchical collection and analysis infrastructure capable of collecting and processing audit records from all hosts within the network.

e.) Access Controls

Each type or brand of computer has a different set of capabilities that can be granted to a user, and different mechanisms or capabilities to restrict access to its resources based upon those user authorizations. Thus a heterogeneous network of computers might provide inconsistent or incorrect enforcement of an enterprises' Information Control Policies (ICPs) -- those policies specified by the enterprise for controlling access to and dissemination of sensitive or valuable information.

f.) Encryption and Integrity

Currently available systems do not provide appropriate mechanisms or security policies to enforce the Information Control Policies that are often required by commercial enterprises. Discretionary Access Control (DAC) by itself is often insufficient. The Mandatory Access Control (MAC) mechanism based upon Sensitivity Labels used by trusted products for enterprises within the Department of Defense is often inappropriate or overly restrictive for commercial use.

**Panelist Statements:**

**Michael McChesney, SecureWare**

SecureWare has spent significant effort studying the security requirements of Commercial and Government customers to determine the future direction of our security technology. One thing that was apparent is that although the term Information Security (INFOSEC) has been popularized to describe the joining of Computer Security (COMPUSEC) and Communication Security (COMSEC), a commercial architecture which combines COMPUSEC and COMSEC to provide a more secure system has not been implemented. Our analysis indicated that a true INFOSEC architecture which combines COMPUSEC features, such as access controls, and COMSEC features, such as cryptography, is necessary to provide the security services needed to meet customer's expanding global network security requirements.

Before designing changes to SecureWare's current technology to implement an improved security architecture, existing and forthcoming security technologies were examined to determine where existing technologies could be applied. Significant security features of technologies such as Novell's Global Security Architecture(GSA), OSF's Distributed Computing Environment (DCE), MIT's Kerberos, and ECMA (European Computer Manufacturers Association) SESAME were examined.

The real-world market forces, which in a large part determine which technologies will be adopted in the global market, were also considered when designing improvements to SecureWare's computer security technology. In other words, we looked at the companies in the computer industry which own most of the market share, and we considered which security technologies they were adopting. The result of our analysis is SecureWare's Extended Global Security Architecture (EGSA), which rationalizes customer security requirements with emerging technologies and real-world market forces. Based on

extensive research, SecureWare has designed EGSA as an extension to Novell's Global Security Architecture (GSA). EGSA extends Novell's GSA to provide additional security services in the areas of administration / management, identification / authorization, audit, access controls, and encryption / integrity. EGSA is also designed to be compatible with the goals of the Department of Defense's Goal Security Architecture (GSA).

### **EGSA Infrastructure**

EGSA uses a directory services infrastructure, similar to Novell's X.500-based NetWare Directory Services (NDS), as a global, hierarchical system for naming and referencing objects and attributes in a directory information database. EGSA extends this logically centralized database infrastructure to store not only administrative information about enterprise resources, but also security attributes. The information stored in the database for each resource (user, computer, printer, application, etc...) includes cryptographic information used to identify and authenticate that resource, credential information specifying what it is permitted to do with other resources, and additional information that is dependent upon the specific type of resource (e.g., user name, E-Mail address, etc... for users). The database is partitioned to allow multiple domains of control and administration, and is replicated to ensure robust, responsive operation.

### **Administration/Management**

The centralized database provides a convenient mechanism for centralized administration and network management. The hierarchical nature of the database makes it easy for users, hosts and applications to locate the information they need, such as E-Mail addresses, the public-key "certificates" used to verify the digital signatures on E-Mail or EDI documents, or the location of an employee, application or printer.

All hosts within the EGSA make use of the centralized database for accessing administrative information, identifying and authenticating users, and establishing user credentials. As it will inevitably be necessary to support legacy systems that are unaware of the EGSA and its centralized database, the link between the Directory Service and network management functions of the database can be used to automatically update the administrative information on legacy systems using SNMP, CMIP or dedicated agents. Thus the EGSA can achieve centralized administration and network management even when incorporating legacy systems.

### **Identification/Authentication**

The directory services database is also a repository for cryptographic information used to centrally identify and authenticate all users, hosts and applications, and credential information used to establish user credentials. This ensures uniform enforcement of an enterprise's Information Control Policies (ICPs), such as "single login", throughout the distributed system. Both the authentication and credential information are extendible. The EGSA supports multiple, configurable I&A mechanisms, and works particularly well with Smart Card technologies. EGSA provides strong security mechanisms for authenticating subjects, and propagating a subjects identity in a trusted manner throughout a distributed enterprise.

### **Audit**

A secure audit service determines whether transactions are accurately processed and information is securely maintained by ensuring that all actions are accountable throughout a distributed system. Coordination of the volumes of audit data produced by individual systems throughout an enterprise is necessary to intelligently and efficiently analyze audit data. EGSA includes a hierarchical audit collection mechanism with a centralized analysis processor to provide intelligent and efficient enterprise-wide audit.



In the EGSA design, each distributed audit element collects and condenses its own audit data before passing it up the audit element hierarchy where filters are used to further condense the audit data until it reaches the central audit analysis processor. A real-time filter component also monitors audit elements for critical events for timely forwarding to a higher-level audit analysis processor. The EGSA audit architecture thus allows critical events, such as system crashes and security intrusions, to be reported to a security officer in near real-time while also allowing more detailed analysis of information, like failed login attempts, to be efficiently performed as a background process.

### **Access Controls**

EGSA includes a generic security policy switch which can be configured to implement an enterprise's Information Control Policies (ICPs) -- those policies specified by the enterprise for controlling access to and dissemination of sensitive or valuable information. Currently available systems do not provide appropriate mechanisms or security policies to enforce the ICPs that are often required by commercial enterprises. Discretionary Access Control (DAC) by itself is often insufficient. The Mandatory Access Control (MAC) mechanism based upon Sensitivity Labels used by trusted products for enterprises within the Department of Defense is often inappropriate or overly restrictive for commercial use. EGSA's generic security policy switch allows a system to be configured to implement the set of security policies needed by the enterprise to protect its data. EGSA uses the security attribute information stored in the directory service for system resources, such as files and printers, the user/group's command authorizations/rights, and the security policy rules to enforce an enterprise's ICPs.

### **Encryption/Integrity**

A key feature of EGSA is that it integrates COMSEC cryptographic services with COMPUSEC security policy enforcement. Tying the cryptographic services directly to the configurable security policies is quite powerful. An application such as E-Mail or EDI can call the cryptographic services directly to protect their sensitive transactions, or encryption can be triggered automatically by the security policies when sensitive information is written to a removable media, sent over a modem, or transmitted over a network. Automatic cryptographic protection can be applied by the host initially exporting the sensitive data, or can be applied by an intermediate gateway when it becomes necessary to transfer the data over an unprotected network.. The EGSA cryptographic services are configurable to support different combinations of software or hardware algorithms.

### **EGSA Summary**

Novell is currently pursuing a joint development effort with SecureWare to implement NetWare Directory Services (NDS) on standard commercial Unix versions and make NDS the basis of the SecureWare's Extended Global Security Architecture (EGSA) infrastructure. EGSA extends Novell's Global Security Architecture (GSA) technology to implement additional security services.

The EGSA is a powerful architecture for building distributed secure systems. Its security features and mechanisms are configurable, allowing an enterprise to tailor the system to match its unique security requirements. Its central database with Directory Service and Management interfaces creates a powerful, versatile infrastructure that provides:

1. centralized network management and system administration.
2. centralized I&A with unitary login.
3. consistent enforcement of user authorizations and Information Control Policies.
4. an information resource that will expand user productivity and facilitate the development of distributed applications.

5. interoperability and integration of:
- different platforms from PCs to Unix workstations, minicomputers and mainframes.
  - systems from different vendors.
  - systems with differing security policies and levels of assurance.
  - legacy systems.

### **Roger Schell, Novell:**

Novell has announced that it is working with customers, industry partners, developers and security experts in the US and Europe to define and deliver a multi-vendor, interoperable solution that will provide customers with a widely trusted network computing environment.

### **Network Security Foundation**

Novell continues to lead the industry in providing systems with security functionality allowing customers to build barriers against intrusion of their information networks. These barriers help prevent unauthorized individuals from logging into the network, accessing and modifying bindery information, and tampering with sensitive data contained in system directories or files. In addition to providing multi-layered security, NetWare provides businesses with the highest level of reliability through numerous fault tolerant features. NetWare provides customers with security services in the areas of administration, authorization, audit, access control, and assurances.

### **Network Directory Services Security**

NetWare Directory Services (NDS) is a global, hierarchical system for naming and referencing objects and attributes in a directory information database. The administration tools in NetWare Directory Services facilitate the implementation and management of enterprise security. The Directory Services objects and associated attributes are the focal point for security in the NetWare 4 product line.

The security functionality for Directory Service objects and attributes is implemented using access control, inheritance and security equivalence. Access control and inheritance are governed by the Access Control List (ACL) attribute. The ACL attributes specifies what objects have rights to access and modify an object and its associated attributes. The ACL attribute also governs the inheritance of rights to objects and their attributes.

The Directory Services utilities provide administrators a simplified way to grant and manage the security privileges of global network users.

### **Administration**

Over the last ten years, Novell has developed an operating system that helps network administrators and users build systems with security functionality. NetWare operating systems contain embedded security controls providing a secure network foundation. These controls are administered with tools to facilitate network administrators in user and account setup. This allows both users and accounts to be controlled based on the rights and relationships setup with the administration tools. The setup can be based on sound organizational policies and procedures. It is this capability which allows organizations to more efficiently manage users on a server.

### **Authentication Services**

Authentication services verify the validity of each user for every login or access to other network services. In addition, the combination of Directory and authentication services provide the mechanism for a "single login" capability to the network.

The NetWare Directory authentication services uses RSA public key/private key encryption technology. The authentication mechanism, which is a critical part of login security, uses the private key attribute to verify a user's identity. Ongoing (background) authentication services are transparent to network users and take place as required when access other services. Only during login (ID and password exchange) is the user aware of authentication. The remainder of the session is authenticated as a network service.

### **Audit Services**

Auditing is the process of examining an organization's records to ensure that transactions are accurate and that confidential information is secure. System auditing records and reports significant events which occur on a system. The collection of records is referred to as an "audit trail." NetWare 4 audit services allow individuals to act independently of network supervisors, administrators, or users in auditing both past and present transactions on the network.

Auditors can monitor Directory Services transactions related to security such as logins, logouts, creation of Directory objects, changes to Directory attributes, trustee modification, and equivalence alteration. File system transactions, such as file and directory creations, deletions, modifications, reads, and writes can also be monitored.

### **Access Controls**

Access control are integral to the NetWare file structure. Access control help determine who the users are and what functions they can perform. Users and groups needing access to resources, such as data and programs that reside in files and directories, can be controlled. Also, all the objects at the server level can be protected from unauthorized access. Rights and attributes for users and groups are easily controlled and assigned in NetWare. There are directory, file and trustee rights. Together with the assigned attributes, a user's access can be restricted to specific directories, files, print queues, and job queues. In many environments, this set of trustee rights and attribute assignments is called an Access Control List (ACL).

### **Encryption Services**

NetWare Core Protocol (NCP) packet signature is a security features that protects servers and clients using the NetWare Core Protocol countering packet forgery. If NCP packet signature is not installed, a network client may be able to pose as a more privileged client and send a forged NCP request to a NetWare server. By forging the proper NCP request packet, an intruder could gain "SUPERVISOR" rights and access to all network resources.

NCP packet signature counters packet forgery by requiring the server and the client to "sign" each NCP packet. The packet signature changes with every packet. If NCP packet signature is installed correctly on the server and on all of its clients, it is difficult to forge a valid NCP packet.

### **NetWare 4 Class C2/E2 Evaluation**

Novell continues to aggressively pursue a Class C2 evaluated solution and has selected NetWare 4 as the platform for this process. Novell's proposal to the NCSC was accepted in September 1992, at which time work began on meeting the NCSC's rigid requirements for a "Trusted NetWare" product.

Novell's solution is significantly different from other vendor's approaches to meeting the Class C2 requirements. Novell recognizes that one can build a trusted network using trusted components, and has concluded that the Trusted Network Interpretation (TNI: NCSC-TG-005) is the only Network security evaluation document in place with a history of technical soundness in network evaluation. It poses a standard for evaluation networks - commercial or public sector.

### **NetWare/UnixWare Security Integration**

Novell has an ongoing commitment to provide the industry with secure, open system products which are designed to protect vital information and resources. NetWare 4, UNIX System V Releases, and UnixWare meet this commitment by providing a high degree of base security. As these products evolve to address industry needs, Novell will continue to define a security architecture for the 90's and beyond.

The NetWare/UnixWare security strategy is to provide security functionality for data and applications throughout an enterprise system. The system may be composed of multiple hardware platforms providing a diverse range of security features and services. As an important step for this strategy, Novell is currently pursuing a joint development with SecureWare to port NDS to run on standard commercial and Multi-Level Secure (MLS) UNIX versions.

### **Future Direction**

The current products are a significant step along Novell's path of expanding security services for existing, as well as for emerging advanced computer technology environments. Based on this foundation, additional steps are implemented to provide multi-level security for the assurance customers need to protect against deliberate or hostile attacks such as Trojan horses, and against intentional or unauthorized modification or disclosure.

While market place requirements today primarily respond to the security problems customers have seen in the past, this is just the tip of the iceberg; Certainly the threat to security in networks will increase in the next several years. Unfortunately, security problems will increase as connectivity increases exposure and the dependence of business and public sectors on a networked information infrastructure rapidly grows.

The problems of malicious software and deliberate attack, scarcely considered today beyond the relatively simple problem of computer viruses, is likely to become the dominant problem - and it is a technical problem that is essentially impossible to meaningfully address unless the proper foundations are already included in the design of our products. Novell is taking a proactive stance in initiating development of the multilevel security and encryption support, which over time, significantly increases assurance, and can be selectively applied for carefully architected elements of future networks. This plan initiates serious exploration of the security foundation for this future success.

### **Bill Dwyer, Hewlett-Packard:**

"DCE or Distributed Computing Environment allows for easier and more transparent access to information and resources that exist across the network. How is such an environment protected to insure that only those persons authorized have access to the information and resources? The security mechanisms of Hewlett-Packard's Distributed Computing Environment and their strengths will be discussed."

# Can Your Net Work Securely?

## Panel Session

### 17th National Computer Security Conference

#### Chairman:

Peter G. Neumann, Computer Science Lab, SRI International

#### Panelists:

Earl Boebert, Secure Computing Corporation

Whitfield Diffie, Sun Microsystems

Andy Goldstein, Digital Equipment Corporation

Clifford Neuman, USC--Information Sciences Institute

Attaining securely networked distributed systems often must rely on components whose trustworthiness cannot be assured. This panel will explore a variety of relevant topics, such as the following:

- \* The impact of vulnerabilities in existing networks of systems --- for example, flawed operating systems, limitations of fixed passwords in distributed environments, problems in authenticating users and systems, and hidden dependencies on untrustworthy components
- \* The need for nontrivial, pervasive user and system authentication in distributed systems (including the relative merits of certificates, token authenticators, Kerberos, the Digital DDSSA proposal, Tessera)
- \* System and network architectural issues such as these:
  - Are commercial operating systems heading in the right direction? Are secure servers enough? What promising research directions are being pursued? What is still missing?
  - Are multilevel - secure user systems (e.g., workstations, CMWs necessary in order to achieve multilevel - secure systems and networks?
  - What are appropriate roles for cryptography? What problems have been encountered? What is still missing?
  - Can we avoid having to trust sublimated (unrecognized) components? For example, can we learn anything from fault tolerance and systems designed to withstand Byzantine or other nonbenign fault modes?
  - What about Trojan horses in systems and network software?
  - What must be done to strengthen the existing evaluation criteria?
  - Is there a narrowing of commercial hardware chipsets? If so, is it an intrinsic limitation, or is it irrelevant to the needs of secure systems? Are advanced-hardware systems like LOCK still necessary?
- \* Expectations for the future

# How to Trust a Distributed System

**B. Clifford Neuman**  
**University of Southern California**  
**Information Sciences Institute**

Deciding how much trust to place in a distributed system is not easy, especially when the system crosses organizational boundaries. In the past year we have heard a great deal of talk about the information infrastructure on which the distributed systems of tomorrow will be built (this infrastructure is often referred to as the Information Superhighway, the National Information Infrastructure, or simply the NII). Such systems will lack many of the characteristics that improve security in centralized systems. Among the characteristics typically lacking are a protected communication channel between parts of the system, and a single authority that sets policy for the system. Technology exists and has been deployed to address the first problem; work is still needed on the second.

## **Protected Communication Between Parts of the System**

When a network extends beyond a physically secure perimeter it becomes possible for an attacker to tap the network, monitoring and in some cases introducing messages on the network. When computers outside a physically secure perimeter are legitimately connected to the network, such attacks become almost trivial. The presence of such attacks affects the security of the communication between different parts of a distributed system. When those communications are between otherwise trusted parts of the system, or when the data should not be disclosed to others, measures are needed to ensure that messages cannot be read or altered by an attacker.

Solutions to this problem rely on cryptographic techniques to protect transmitted data from disclosure to other than the intended recipient, and to provide assurance that the data received is what was sent by the claimed originator. When the communicating components of a distributed system are assumed to be trusted, the claimed originator may be the computer system itself, in which case cryptographic techniques are used to protect communication between hosts and the identity of the user is assumed to be correctly asserted by the host itself.

When the host computer is under the complete control of the user, mechanisms like Kerberos [4] can be applied that use cryptography to authenticate the user of the system. When the user does not completely trust the component of the system through which he or she interacts, such techniques can be combined with the use of token authenticators and smartcards to limit the period for which the system can claim the identity of the user. Issues related to trust of the software through which one interacts with the system are discussed at length in the proposed Digital Distributed System Security Architecture [1].

## **Absence of a Single Authority**

While the techniques described above can provide assurance that one is interacting with the intended agent in a distributed system, they say little about whether one should trust the agent with important data or critical functions. This is less of an issue in a small system where system services are provided by a single organization that is assumed to be trusted and competent, or at least where administrative sanctions can be applied if that trust is violated. Such will not be the case on the NII.

On the NII, users will regularly interact with service providers about which they have little prior knowledge. Methods will be needed through which users can assess whether a service provider is trustworthy and competent, and what recourse will be available in case that trust is violated. This need is not unique in distributed systems; it is just as important for society in general. In the "real world" such assurances are provided through licensing, endorsements, surety-bonding, and liability insurance.

Analogues to these mechanisms are needed for the NII [2,3]. Users would identify licensing authorities, endorsers, and insurance companies whose statements they trust, and would specify the exposure to risk that can be tolerated. Applications would apply those rules to decide whether to use a server, and the client could be queried if exceptions were required (and authorized by the user's organization).

### **Conclusion**

It is difficult to determine the level of trust one should place in a distributed system. Part of the difficulty can be addressed through the use of encryption and authentication methods that are readily available today. These methods ensure the privacy and integrity of data communicated between different parts of a system, increasing its security. Unfortunately, even once these methods are applied, there are problems inherent from the lack of a central authority that are harder to deal with. Reliance on endorsements, licensing, and insurance can make it easier for users to quickly determine whether a service should be trusted, and may provide recourse if that trust is violated. While online interactions with other organizations will always carry some risk, tomorrow's systems will make it easier to intelligently control one's exposure.

### **References**

- [1] M. Gasser, A. Goldstein, C. Kaufman, and B. Lampson. The Digital Distributed System Security Architecture. In *Proceedings of the 1989 National Computer Security Conference*, pages 305--319, 1989.
- [2] Charlie Lai, Gennady Medvinsky, and B. Clifford Neuman. The Role of Insurance, Licensing, and Endorsements in Evaluating Trust of Distributed System Services. Submitted for publication, May 1994.
- [3] B. Clifford Neuman. Protection and Security Issues for Future Systems. In *Proceedings of the Workshop on Operating Systems of the 90s and Beyond*. July 1991.
- [4] J. G. Steiner, B. C. Neuman, and J. I. Schiller. Kerberos: An Authentication Service for Open Network Systems. In *Proceedings of the Winter 1988 Usenix Conference*. pages 191-201, February 1988.

# Internet Firewalls

## Panelists

**John Wack**, National Institute of Standards and Technology, Chair

**Marcus Ranum**, Trusted Information Systems

**Brian McConnell**, The Mitre Corporation

**Others**, TBD

Many organizations are in the process of connecting their internal networks to the Internet to take advantage of Internet services and resources. Businesses and agencies are now using the Internet for a variety of purposes, including for exchanging electronic mail, for distributing information to the public, and for conducting research. However, Internet access is not necessarily a good thing for organizations that do not already have strong security procedures and practices in place.

There are significant security problems associated with the Internet that often are not obvious to new (and existing) users. Intruder activity, in particular, has been difficult to detect and discover, has been costly in terms of damage caused and lost productivity, and has been highly embarrassing to the organizations involved.

This panel will focus on firewalls and how they can be used to implement security policies to protect networks connected to the Internet. Firewall systems are highly effective for improving site security and providing general protection from Internet-borne threats. A firewall can be viewed as the technical implementation of a network security policy. It is NIST's recommendation that agencies and organizations use firewalls at their Internet gateways to implement their network policies.

This panel will discuss how firewalls work, policies that can be implemented by firewalls, and updates on different firewall configurations to support restricted access.



## **Panel Title: Proven Detection Tools For Intrusion Prevention**

In the last 36 months a number of tools have reached a point of maturity that when combined with security conscious system administrative practices has resulted in a substantial capability to protect and detect against the most common attack profiles. In this panel experts from government and commercial industry will discuss the use of, implementations, features, and lessons learned of protection tools including the Security Profile Inspector (SPI), TIGER, COPS, TRIPNIRE, and TCP/IP Wrappers. The panel will take the audience through detection scenarios, tool specification to address the environmental threats, and the actual lessons learned from operational implementation of these solutions.

### **Organizational affiliation:**

The chair will be **Michael Higgins** Deputy Director for INFOSEC Countermeasures, Center for Information Systems Security, Defense Information Systems Agency (703) 756-7934.

### **Panel Members:**

**Ed Dehart**, Computer Emergency Response Team/Coordinator Center, Software Engineering Institute, Carnegie Mellon University

**Steve Weeber**, Computer Incident Advisory Capability, Lawrence Livermore National Laboratory, Dept of Energy

**Frederick Avolio**, Trusted Information Systems Inc.

**David Slade**, Bellcore Security Information Exchange Bell Communications Corporation

## **PANEL: MLS System Solutions - A Continuing Debate Among The Critical Players**

Joel E. Sachs  
Arca Systems, Inc.  
10320 Little Patuxent Pkwy., Suite 1005  
Columbia, MD 21044  
410-715-0500

### **Panel Overview**

Acquiring and developing an MLS (multilevel) system solution that results in an accreditable secure solution is not simple; moreover, there is debate and confusion as to what should be specified during the initial phases of an acquisition that will help all parties involved throughout the life of the program. Several MLS system acquisitions have already been deemed less than successful. A number of reasons have been suggested: integration of MLS products is not straight forward, defining mission requirements and mapping them to security and system solution requirements is difficult, and certification and accreditation is difficult and not consistently applied.

This panel is a continuation of similar panels conducted at the last two National Computer Security Conferences that focused on these issues. In past years, the panel discussed and debated a spectrum of issues along the life-cycle timeline associated the acquisition, integration/development, certification and accreditation, operation and maintenance of a MLS system solution. This was achieved through role-playing of the critical players in the acquisition process, as opinions varied depending on one's position within the process. Each of the seven panelists acted on the behalf of an identified role with which they were experienced. These roles included: End-User Organization, Program Management Office, Advising Security Agency / Certification Body, Designated Approving Authority, Systems Integrator, Security Engineering Subcontractor, Vendor.

This year's panel will use the role-playing technique again, will focus on five specific issues, and will address each, one at a time. The issues are:

- What should be done to address assurance, its definition, development, certification, and accreditation under different acquisition strategies, including object-oriented, rapid prototyping, evolutionary development, and incremental development?
- What are the advantages and disadvantages with differing views under consideration today, including:
  - defense information infrastructure view versus single system with external connectivity view;
  - process-based certification versus result-based certification;
  - centrally executed versus centrally coordinated versus decentralized certification;
  - centrally executed versus centrally coordinated versus decentralized accreditation;
  - certification of individuals versus certification of organizations?
- How should key developmental items associated with security (both pre-RFP and post-RFP) be represented, for example, in many separate security documents, in system documents, in one single document?

Information is provided below which describes the roles of the critical players along with example issues and concerns for each critical player. A list of 25 questions and issues associated with pre-draft RFP, pre-RFP, pre-award, and post award milestones regarding specifying, procuring, and accrediting MLS System Solutions can be found in last year's panel description in the 1992 National Computer Security Conference Proceedings.

## **Panel Roles, Descriptions, and Areas of Concern**

### ***End-User Organization***

The end user organization has a requirement for a system solution. The results of this procurement will be delivered to this organization for their use.

The main concerns of the organization are how to ensure that the end-users get what they want and need, that the system solution will be accreditable, that it will fall within its budget and development and delivery schedule. End-user organizations usually understand functional requirements reasonably well but usually do not understand security and assurance requirements and security issues.

### ***Program Manager's Office [PMO]***

The PMO is the acquisition agency responsible for writing the RFP, awarding the contract, and supervising its execution. (Typically, a separate organization might be used to develop a system specification for the Statement of Work [SOW]. For the purposes of this panel, the player developing the specification will be considered merged with the PMO.)

The PMO's main concerns are system specification, cost, schedule, measuring the prime contractor's progress and compliance, and assuring steps towards accreditation are being taken. The PMO understands the functional requirements as communicated by the end-users, but is not likely to fully understand the security requirements, issues, and assurance needs that result from the mission and threat context.

### ***Advising Security Agency / Certification Body***

The Advising Security Agency is the End-User's and/or PMO's security arm. This agency helps monitor the progress of the program to ensure that security within the program is adequately addressed. The Certification Body gathers the assurance evidence and performs risk analyses on the system. (For the purposes of this panel, these two roles have been combined as often happens in practice.)

The main concern of both of these organizations is whether the delivered system meets the security requirements specified in the RFP and provides the required security functionality and assurance. The certification body must provide enough evidence to allow the accreditor to make a proper decision regarding the system's accreditation.

### ***Designated Approving Authority [DAA]***

The DAA is the individual responsible for the operational aspects of the system. It is this individual's responsibility to approve the system for operation.

The DAA's main concern is whether the system meets its operational requirements and its operational risk has been reduced to an acceptable level. Based on the evidence provided during the certification process, the DAA must make a decision whether the operational risk is acceptable given the evidence provided and the system's mission, and accredit or fail the system for operation. The DAA's accreditation of the system is his indication that he feels the risk is operating the system is low enough or the operational need is high enough to allow the system to operate.

### ***Systems Integrator***

The Systems Integrator is responsible for the development and integration of the end-system as well as the management of all the subcontractors involved in the effort.

The main concerns of the system integrator are how to provide the required functionality, security, and assurance within the budgetary and time constraints stipulated in the integrator's proposal. Other areas of concern include how to manage the security engineering effort to produce a functional and usable

system as well as how to handle the potential impact of requested changes to the end-system on system operations, security, and assurances.

*Security Engineering Group/Subcontractor*

Security Engineering is responsible for the security portion of the overall system development. This team is composed of internal systems integrator personnel, a security subcontractor, or a combination of both.

This team's main concerns are: how to relate component policies to the overall system policy, the trust requirements for each component, how to integrate trusted and untrusted systems, how to integrate multiple products into a single secure solution, and how to provide required assurance evidence. They may also be involved in determining the security requirements and policy, determining the appropriate assurance level, and how to provide assurance evidence.

*Vendor*

Vendors provide products that are used as part of end-user system solutions.

Their main issues are: how to relate their product features to the desired functionality and assurances needed within an MLS system solution and how to advise the systems integrator on the best use of these features and assurances.

**PROGRAM ENTRY**

**PANEL: Debate of Critical Player Perspectives on MLS System Solution Acquisition Topics**

- Chair: Joel Sachs, ARCA Systems
- Panelists: John Adams, SecureWare  
Michael Askew, GTE  
Gary Evans, ARCA  
Penny Klein, DISA  
Ann Leisenring, NSA  
Kathy Thompson, USACOM  
John Seymour, Joint Staff

Role-playing will be used to explore current issues and challenges associated with the acquisition, development, and accreditation of MLS systems solutions. Topics will include: establishing assurance under acquisition/development strategies, process-based versus result-based certification, single system versus infrastructure security.

## Panel: Trusted Systems Interoperability Group

Mr. W. Stan Wisseman, Chair  
Arca Systems, Inc.  
2540 North First Street, Suite 301  
San Jose, CA 95131  
wisseman@arca.ca.com

Mr. Jeffrey A. Edelheit  
The MITRE Corporation  
7525 Colshire Dr.  
McLean, VA 22102-3481  
edelheit@mitre.com

Mr. Ron Sharp  
AT&T Bell Labs  
67 Whippany Rd  
Whippany, NJ 07981  
rls@neptune.att.com

Mr. Paul T. Cummings  
Digital Equipment Corporation  
24 Porter Road - LJO-1  
Littleton, MA 01460  
cummings@imokay.enet.dec.com

Mr. George B. Mitchell  
National Computer Security Center  
9800 Savage Road  
Ft. George G. Meade, MD 20755-6000  
GBMitchell@dockmaster.ncsc.mil

Mr. Charlie Watt  
SecureWare, Inc.  
2957 Clairmont Rd. Suite 200  
Atlanta, GA 30329  
watt@sware.com

### Panel Summary

A heterogeneous, multilevel secure configuration presents a number of interoperability problems, including:

- Different representations (both binary and ASCII) for security attributes
- Different variations of a system security policy (e.g., least privilege model)
- Different domains of administration and therefore disparate security policies (e.g., CMW trusted administration vs. regular B1 administration)

A major issue in a heterogeneous configuration becomes how the destination system's Trusted Computing Base (TCB) knows the user's current security attributes. On a trusted host, there are many security attributes associated with an active user that govern the services and capabilities the TCB grants to the user. In a networking environment, a user on one host, the source, requests a service from another host, the destination. In order to communicate security attributes, the end systems in a communication session must agree on a protocol and its options. While in some cases the destination system may have these in its local files, other attributes are dynamic on the source system and must be transmitted by the source TCB along with the request as shown in Figure 1.

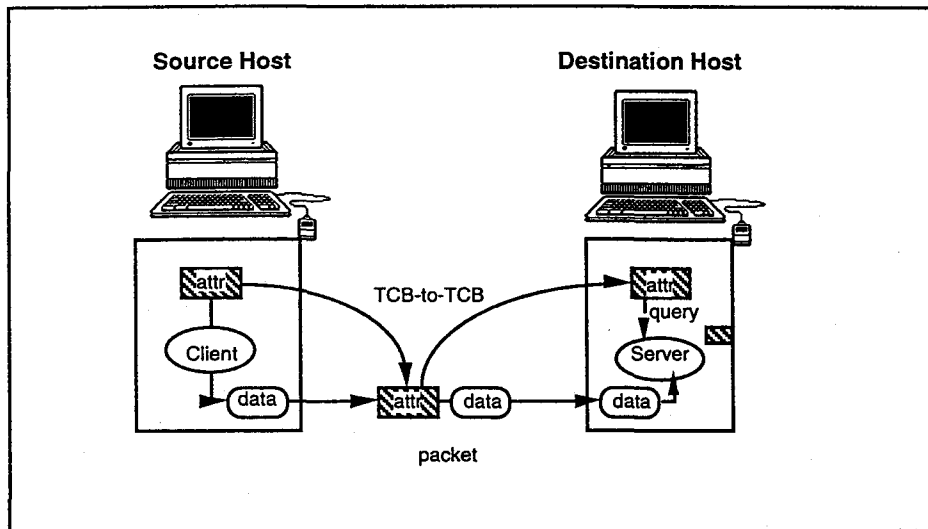


Figure 1 - Security Attribute Passing

Trusted product vendors and customers are interested in achieving interoperability among trusted systems as quickly as possible. The Trusted Systems Interoperability Group (TSIG) was established as an open forum for developers of secure networking systems with emphasis on UNIX™ and TCP/IP and a shared vision of making trusted open secure systems a reality. In order to achieve trusted product interoperability, agreements must be reached regarding syntax and semantics of data exchanged between the two systems.

No single protocol is used to provide interoperability among computer systems; in general, several protocols, used in combination, are required to transfer data from one system to another. For this reason, interoperability specifications are necessary in many different protocols. TSIG has developed specifications for security attribute passing for Internet Protocol called the *Common Internet Protocol Security Option (CIPSO)*. TSIG has developed a specification that provides B1 level security to NFS. TSIG has developed a general TCP/IP security attribute passing mechanism, called *Trusted Security Information Exchange for Restricted Environments*, TSIX(RE) for use by layered products such as DBMS's. TSIG is currently working on agreements for FTP, SMTP, telnet, tape archiving, rlogin, rcp, and various other remote services.

TSIG participants include hardware and software manufacturers, systems integrators, end users, and governmental agencies. Participants at recent meetings include representatives of: 3COM, Arca Systems, Inc., AT&T Bell Labs, Cray Research, Defense Intelligence Agency, DISA, Grumman, Hewlett-Packard, HFSI, IBM, Informix, Intergraph, Loral WDL, MITRE, National Security Agency, Network Systems Corporation, Oracle, Planning Research Corporation, SecureWare, SRA, Sterling Software, Sun Microsystems Federal, and Wollongong.

Panelists represent various perspectives on the TSIG efforts and will discuss the group's history, implementation agreements, and importance to the government.

**Historical Perspective:** Mr. Cummings will comment on the charter of TSIG, reviewing the goals of the group, and relate the ability of TSIG to "live up to" its charter. Mr. Cummings manages the Security Group within Digital's Unix Systems Group. Mr. Cummings was instrumental in the formation of TSIG, helped develop the TSIG charter, and has participated in nearly every TSIG meeting over the past 5 years.

**CIPSO:** Mr. Sharp will talk about the CIPSO security label, what motivated its creation, its goals, current status of implementations and the results from several interoperability tests. Mr. Sharp is a Member of Technical Staff at AT&T Bell Laboratories. Mr. Sharp led a team that produced a Multi-level Secure TCP/IP which employs CIPSO and RIPSO labeling. Mr. Sharp is a charter member of TSIG. He is the chairperson of the CIPSO working group for both TSIG and the Internet Engineering Task Force (IETF).

**TSIX(RE):** Mr. Watt will provide the history and overview of the TSIX(RE) specification, a description of the security features and architectures it provides, and the environmental limitations. Mr. Watt is the Director of Research SecureWare, Inc. Mr. Watt has served as chief architect and designer for SecureWare's MaxSix trusted networking products. MaxSix, along with DNSIX 2.1, served as the foundation for TSIG's TSIX(RE) specifications. Mr. Watt has been a key contributor for many of the TSIG working groups.

**Trusted Administration:** Mr. Edelheit will describe how the Trusted Administration working group is developing interoperability specifications and approaches that will hopefully ease the Administrator's burden. Mr. Edelheit is a Department Assistant for the MITRE Information Security Center. Mr. Edelheit has been an active TSIG participant for four years, particularly with the Trusted Administration working group. He recently facilitated the TSIG AFCEA demonstration in June.

**Trusted Applications:** Mr. Wisseman will describe how the group is working to provide extensions to common network applications such as telnet, ftp, rsh, rlogin, rcp and mail such that they will operate as interoperable, trusted, multilevel applications. Mr. Wisseman is the Trusted Products Business Area Manager at Arca Systems. He currently chairs the Trusted Applications working group and has facilitated the TSIG AFCEA demonstrations.

**Government Perspective:** Through its emphasis on developing solutions for secure interoperability among UNIX and TCP/IP systems, the TSIG open forum offers a substantial contribution to government's greater understanding of interoperability requirements in multilevel secure (MLS) systems. Mr. Mitchell is the Director of INFOSEC Integration for the National Computer Security Center. Mr. Mitchell has been a strong proponent of TSIG for several years.

## Historical Perspective

**Paul Cummings**  
**Digital Equipment Corporation**

### *1. Trusted Systems Interoperability Group Beginnings*

The Trusted Systems Interoperability Group (TSIG) was initiated by the Compartmented Mode Workstation (CMW) vendor community and other trusted UNIX vendors in 1989. Other non-CMW vendors quickly joined TSIG. The Defense Intelligence Agency and National Computer Security Center began an industry movement when they awarded 5 "cost-sharing" contracts for the development and evaluation of B1/CMW systems. The initial awards were to: Digital Equipment Corporation, Harris (contract work now being conducted by Argus Systems Group), IBM, SecureWare, and Sun Microsystems Federal.

Unlike most other DoD security products, each B1/CMW vendor funded nearly the entire development of his product. For this reason, each vendor had compelling reasons to ensure his product would be a success in the market - the market was the only place to recover the investment. The CMW program remains a unique example within the security arena of industry rallying around a common requirements document funded by industry investment. By most estimates, industry has provided over \$100 million in funding for B1/CMW development.

Even though trusted networking was not a part of the B1/CMW contracts, each vendor knew that heterogeneous networking was essential to success in the B1/CMW market. In other words, **necessity drove the creation of TSIG**. A group of vendors began meeting in 1989 to discuss what solutions existed to ensure interoperability in a trusted environment. Initial meetings of the TSIG were hosted by SecureWare in Atlanta, Digital Equipment Corporation in Merrimack, NH, Hewlett Packard in Palo Alto, CA and Sun Microsystems in Mountain View, CA.

For the reasons stated above, it is in the interests of each vendor to develop solutions to the interoperability problem in time to meet market demands. Therefore, the TSIG is driven by product time tables and today's market pressures. We feel that this allows the TSIG to develop timely solutions to interoperability problems. This is evidenced by the results in the Common Internet Protocol Security Option area, wherein vendor consensus was reached on a proposal to the Internet Advisory Board. With this consensus, vendors were able to begin implementation of interoperable products. This is a particularly appropriate example as the consensus was proposed to the appropriate standards group by a TSIG participant and is now under consideration by that group.



## *2. Necessary Ingredients*

Multi-vendor interoperability demonstrations at recent AFCEA meetings showed interoperability among systems from ten (10) different vendor's products using TSIG protocols. We believe this also demonstrated the success of TSIG. The question is what ingredients make TSIG successful. They are:

- A common well-defined goal,
- Efforts driven by developers working on products,
- A willingness to compromise,
- Recognition that unanimity is not necessary, and
- A willingness to accept workable near-term solutions in order to make progress while longer-term efforts are pursued.

### *2.1 A Common Well-Defined Goal*

TSIG clearly identified and agreed to the level of interoperability that was sought. In 5 years this has not changed substantially. The protocols of interest are listed in the TSIG charter and include such things as: mail, rsh, rcp, X windows, Network File System, tape archiving, File Transfer Protocol, and Telnet.

Focusing on this small set of protocols has allowed TSIG to develop solutions in a time frame that would be impossible if a grand and glorious all-encompassing trusted network solution were sought.

### *2.2 Efforts Driven by Developer Working on Products*

The predominance of TSIG participants are either developers currently working on products or users waiting for their release. With this mix of participants, there is a strong pressure on producing something vs. producing an endless debate. The developers are people with schedule and functionality pressure that come from product development. They also have the experience that comes with developing products that must exist, be supported, and compete in an open market. The resulting TSIG environment discourages longwinded academic exercises into areas not likely to occur in practice.

### *2.3 A Willingness to Compromise*

While each individual and each vendor may have a vested interest in seeing a given protocol implemented a certain way, every individual and vendor has a larger interest in ensuring that some common protocol is created. This has driven a willingness to compromise that has characterized TSIG and permitted progress to continue. Individuals and vendors commonly relegate their interests to second priority in order to allow the group to proceed.

#### *2.4 Recognition That Unanimity IS Not Necessary*

The purpose of TSIG is to provide a forum for vendors to create protocols for multi-vendor use. With this goal, it is an acceptable outcome for even a pair of vendors to come to agreement on a protocol. Not all vendors need necessarily agree - each vendor is free to implement what he chooses. While this point may be essential for progress, since it allows a small number of vendors to establish an agreement, in practice, nearly all TSIG participants seem to agree on the final outcome.

#### *2.5 Willingness To Accept Workable Near-term Solutions*

It has been said that: "Better is the enemy of Good Enough". By specifying a relatively small set of protocols, TSIG was able to bound the massive trusted network interoperability problem. Focusing on just this set of protocols, as opposed to an all encompassing network security standard, has allowed TSIG to make incremental progress.

#### *3. Conclusion*

With these ingredients, TSIG has been able to make steady progress over the past 5 years. The reasons for the success of TSIG are based on the original motivation and makeup of the participants. The motivation is market pressure. The participants are developers from industry-funded vendors working to satisfy market pressures.

# Common Internet Protocol Security Option

**Ron Sharp  
AT&T Bell Laboratories**

## **DESCRIPTION**

CIPSO is designed to provide labeling for the commercial, US civilian and non-US communities. CIPSO provides a means to label and protect data as it passes through communications systems and enables end systems to maintain security labels on stored and displayed data. The format of the option makes it possible to include the sensitivity label in the IP Security Options field of the IP protocol. The attachment of specific security attributes at the IP layer allows end and intermediate systems to parse the option and interpret the security attributes. CIPSO can support a large set of security domains and policies with differing interpretations of security attributes. An extendible format allows for multiple sets of security attributes as well as addition of new attributes in the future.

CIPSO specifies four tags, three tags which define different ways to format a sensitivity label and one tag to specify release markings. The sensitivity level tags are Tag Type 1 - Bit-Mapped Tag Type, Tag Type 2 - Enumerated Tag Type, and Tag Type 5 - Range Tag Type. Each sensitivity tag type stores a sensitivity hierarchical level in a one octet field. The release marking tag is Tag Type 6 - Release Marking Tag Type.

## **SPONSORING ORGANIZATION**

The original CIPSO specification was developed by TSIG. Computer vendors within the Internet community are supporting an effort to make CIPSO an Internet standard. The TSIG CIPSO Release 2.3 has been used as a foundation for developing an IETF CIPSO specification. The IETF CIPSO Working Group is chartered to define an IP security option that can be used to pass security information within and between security domains. The CIPSO protocol will support a large number of security domains. New security domains will be registered with the Internet Assigned Numbers Authority (IANA) and will be available with minimal difficulty to all parties. The specification has reached the stage of an Internet draft RFC. The DoD has made a military standard out of CIPSO. Called Mil-Std-2045-18501, or the Common Security Label, the draft mil-spec is the same as CIPSO from an operational viewpoint.

## **EVOLUTION**

CIPSO has been implemented on trusted operating systems from AT&T, Cray Research, Data General Corp., Digital, Harris, HP, Loral Federal, Sun Federal, SCO, SecureWare, and Silicon Graphics. Argus Systems Group, Verdix, Network Systems Corporation (a router company), and Boeing also have CIPSO implementations under development. To interoperate, vendors must support the same tag types, which is not always the case.

# Trusted Security Information Exchange for Restricted Environments

**Charlie Watt  
SecureWare**

## **Description**

Vendors recognized the need to transport a variable set of security attributes with network messages. CIPSO (and RIPS0) specifies a method for labeling IP datagrams with CIPSO-format sensitivity labels. This mechanism could be expanded to transport all the required security attributes within the IP header. However, this approach was discouraged since 1) the intent was to extend DNSIX 2.1 with additional capabilities, not rewrite existing specifications; and 2) the sensitivity label is rightfully contained within the IP header because it is used for network-level operations like enforcing network MAC and trusted routing. Other attributes have more to do with session management activities and should therefore be transmitted according to a session management layer protocol.

Given the need to communicate a full set of subject-related attributes within the network, TSIX(RE) defines a new set of communication protocols that address the attribute transport requirements of the hosts using the network. Although the RIPS0/CIPSO label formats are still used at the IP level to allow routing based on sensitivity level, a session management layer is introduced. This session management layer is responsible for exchanging the full set of security attributes, including privilege sets and information labels. Furthermore, the session management protocols use the token-mapping services to map security attributes between two systems that have different internal representations. This is essential to mapping between two distinct security architectures from different vendors. In addition, since network applications must use the same API to be portable among trusted systems, TSIX(RE) defines an OS and IPC mechanism-independent API that allows network programmers to create portable, trusted network programs.

TSIX(RE) assumes the protect environment of a DNSIX 2.1 network. The DoDIIS Reference Model (DRM) implies the following:

- Physically protected network (within domain)
- Physically protected, trusted hosts ("trusted" means that we have assurance that the hosts have not been tampered with and will operate as advertised)
- Global knowledge of domain security attributes
- Trusted users (each system on the network will correctly identify and authenticate its users, and will propagate that identity in network transactions)
- Local control vs. central control
- Type of host (DNSIX 2.1, RIPS0, CIPSO or System High)
- Encrypted network data between domains

## Sponsoring Organization

To formalize the MaxSix extensions to DNSIX 2.1, vendors proposed that the DIA adopt the MaxSix 2.1 specifications as "DNSIX 3.0". SecureWare initially published the MaxSix 2.1 protocols and the accompanying interfaces, making them available to industry for review and comment. Working with industry, these specifications were modified from their original MaxSix 2.1 base to incorporate various industry comments, including one significant modification: a change from *receiver-based* tokens to *sender-based* tokens. Without going into detail, this change from receiver to sender tokens was largely made to better support multi-cast and broadcast protocols.

Despite the headway made by industry, the specs were never officially adopted by the DIA as DNSIX 3.0. Nonetheless, the term "DNSIX 3.0" was used quite a bit by industry and government alike in anticipation of the DIA adopting it. Thus, the vendors turned to TSIG as a neutral body to adopt the specifications. At the request of TSIG, SecureWare re-published the specifications under the name TSIX(RE) -- *Trusted Security Information Exchange for Restricted Environments*, where they are currently available through the TSIG mail archive and ftp server. Thus, people are still using the term DNSIX 3.0, although what they are really looking for is correctly known as TSIX(RE) 1.0.

While TSIX(RE) is endorsed by TSIG, it is not a government standard. However, vendors are implementing the protocol since TSIX(RE) (and related TSIG documents) is the only open, published specification for multi-vendor MLS interoperability.

## Evolution

MaxSix 3.0 is SecureWare's implementation of the TSIX(RE) specification, and will support both sender and receiver tokens, so that all MaxSix-based systems can migrate to full TSIX compliance while maintaining backward compatibility with the installed base of MaxSix 2.1 systems. Project Max members such as HP, Loral Federal, SCO, and Sun Federal may have MaxSix 3.0 available soon.

The latest release of MultiSix™, from Digital Equipment Corporation, complies with TSIX(RE). MultiSix was originally derived from MaxSix 1.0; DEC has since evolved it independently. Argus Systems Group and Sequent are also offering TSIX(RE) implementations.

Given that TSIX(RE) is still based on the DRM assumptions, vendors have found difficulty selling the protocol in commercial markets. The next step is to remove some of the DoD environmental assumptions and develop a more robust protocol.

## Trusted Administration Working Group

**Jeff Edelheit  
The MITRE Corporation**

System administrators have long recognized that managing a distributed heterogeneous network of single level workstations and servers is not an easy task. Over the years, several tools have been developed that ease the administrator's efforts. These tools include the Network Information System (NIS), Kerberos, and Bind/Hesiod. While some of these tools work quite well, there are other cases where the underlying operating system differences require the administrator to subdivide the network into smaller segments; one segment for each operating system or vendor.

Several years ago, the Trusted Administration Working Group was formed to examine the problems related to administering a distributed heterogeneous network of multilevel secure (MLS) workstations and servers. This paper briefly discusses the working group's efforts and open issues.

### **WHAT ARE WE TRYING TO ADMINISTER?**

The Trusted Administration Working Group's charter identified three areas of concern: operating system, user, and audit administration.

#### **Operating System Administration**

Configuring and maintaining a MLS Unix-based operating systems is rather complex. System resources (e.g., disks, network interfaces) must be correctly labeled. Default system configuration files must be correctly defined or the system may not operate in a secure or correct manner. Environmental concerns may require that the MLS servers support clients that do not support the full range of information the server processes. Lastly, the MLS components must be configured to securely interoperate with legacy single level systems.

#### **User Administration**

Defining user's attributes like the account name, password, authorized privileges and sensitivity of information that they may process on a single MLS host is a relatively easy process. However, providing this information consistently and securely to a heterogeneous set of MLS workstations and servers is very difficult. For example, the identification and authentication mechanisms may differ or authorized privileges on one vendor's system may not map to another vendor's system. Even if these problems didn't exist, trusted or untrusted methods of easily distributing this information doesn't exist.

## **Audit Administration**

Defining a consistent audit policy is quite difficult since each vendor implements system and user auditing differently. Audit events are defined differently, system and user audit configuration files are not consistent, and audit trail formats and locations vary.

### **WHAT HAVE WE DONE TO EASE THE ADMINISTRATION BURDEN?**

Having identified a problem set, the working group had several false starts. The first effort led the working group to examine a set of protocols and approaches developed for the United States Air Force's Strategic Air Command. While this approach seemed to meet the user's needs, it became apparent that there was a general reluctance to recommend an approach that was not accepted by any standards organizations or was a de facto standard. Extending NIS to support extended security attributes seemed reasonable, except that each vendor seemed to define and store the attributes differently and some concerns were voiced about the trustworthiness of the underlying protocol.

A major advance occurred when one of the working group members suggested that Version II of the Simple Network Management Protocol (SNMP II) provided a trustworthy protocol base. Furthermore, a draft Unix systems administration Management Information Base (MIB) was being circulated within the Internet Engineering Task Force (IETF). The working group examined the draft Unix MIB and suggested that the MIB be extended to address most MLS attributes.

## Trusted Applications Working Group

**Stan Wisseman  
Arca Systems, Inc.**

With the network and session management issues resolved by CIPSO and TSIX(RE), TSIG was positioned to address application issues. The Trusted Applications Working Group was formed to meet the following objectives:

- 1) To provide extensions to the common network applications such as telnet, ftp, rsh, rlogin, rcp, and mail so that they will operate as interoperable, trusted, multilevel applications; and,
- 2) To specify an Application Programming Interface (API) suitable for supporting trusted, multilevel distributed applications within the operating environment assumed by the TSIG protocols providing the underlying trusted network.

As with other TSIG protocols, the scope of the problems were limited by using the DoDIIS Reference Model (DRM) assumptions (enumerated in the TSIX(RE) description). It was assumed that interoperability existed between heterogeneous hosts from different vendors, offering different levels of trust (e.g., CMWs, class C2 or B1), and running different security policies. The functionality of the TSIX(RE) API was used as a starting point and as a minimum functionality reference.

The working group assumes that interoperability problems of a heterogeneous, MLS configuration are made transparent to an application by an underlying attribute translation mechanism (e.g., a TSIX(RE)). This enables an application on one system to use the functionality provided by the API to package any arbitrary set of attributes such that they will appear to the recipient correctly translated (both in format and policy) into a form understood by the recipient.

The Trusted Applications Working Group is currently approaching the goal of interoperability specifications for MLS versions of TCP/IP based applications (e.g., rlogin, rcp, rsh, telnet, and ftp). The group has also studied issues related to UNIX mail, MIME, NIS, DNS, and MLS file archive.

Trusted RDBMS vendors participating in the group have described their API requirements. The Trusted Applications Working Group wants to have a better understanding of the POSIX 1003.22 efforts prior to defining a TSIG API.



## Government Perspective

**George B. Mitchell**  
**National Computer Security Center, NSA**

In the early 1980s DoD recognized that the computer and telecommunications revolution was going to generate extraordinary challenges in terms of both securing the information being processed, stored, and transmitted and protecting the information system resources. With the vast investments of the commercial world clearly driving the technology and the market it was very apparent that DoD could not achieve its goals for high performance, secure, and cost-effective information systems based solely on DoD requirements and funding. This reality led to the development of a program known as the Trusted Product Evaluation Program (TPEP), where Government provided security design criteria and evaluation resources, and industry funded and performed the product development. The objective was to create products with wide applicability, market driven performance and cost, and a range of protection levels.

The Compartmented Mode Workstation (CMW) program is one of the TPEP initiatives. It was the first TPEP effort to create a B-level trusted workstation with windowing capability. Unfortunately, initial requirements did not include networking and hence interoperability. However, as the other panel presentations have discussed, the TSIG was formed to meet this challenge.

As has been pointed out, the approach was not one of a "grand design", top down kind of activity, but rather an iterative or evolutionary process. Because of the rapid changes in technology and user requirements, it is not clear that the more intellectually satisfying top down approach would have led to better results.

There have clearly been disappointments on all sides. The developments and evaluations have taken longer than planned. The overall mission capability of the workstations has lagged customer expectations. Nevertheless, this has to be put in perspective relative to the absolutely daunting task of creating in an open, multi-vendor environment a family of highly capable and interoperable MLS workstations with B-level trust and reasonable life cycle cost. The goal has yet to be achieved, but tremendous progress has been made. The willingness of so many companies to jump in and work together has been truly amazing.

Through TSIG and associated TPEP activities a significant cadre (perhaps 150-250) of talented engineers and computer scientists have become intimately involved in the technical challenges and opportunities associated with creating trusted UNIX based networks. This work has resulted in the delivery of hundreds of trusted workstations using CMW technology - thousands more are on IDIQ contracts.

Many years were required to develop the products and raise customer awareness to the need for automatic access control (C2). This has now become an industry minimum requirement. Going the next step to labeled data and mandatory access control (B1 plus) is a big one. However, the demands and risks associated with networking will surely expand this market - both in Government and the commercial world.

# **NSA Concurrent Systems Security Engineering Support To The MLS TECNET Program**

<b>CHAIR:</b>	CSSE Manager	Bradley Hildreth, National Security Agency
<b>PANELISTS:</b>	TECNET MLS Consultant	Mary Mayonado, Eagan, McAllister Assoc.
	CSSE Consultant	Teresa Acevedo, Pulse Engineering, Inc.
	Policy and Doctrine Analyst	Jenny Himes, National Security Agency
	INFOSEC Evaluator	Gregory Wessel, National Security Agency
	Risk Assessment Analyst	Randy Blair, National Security Agency
	Air Force Certifier	Richard White, Air Intelligence Agency, Air Force Information Warfare Center
	TECNET Exec. Secretariat	George Hurlburt, Naval Air Warfare Center - Aircraft Division

This session will discuss the Concurrent Systems Security Engineering (CSSE) initiative that NSA is applying to aid the Test & Evaluation Community Network (TECNET) Multilevel Secure (MLS) system development. TECNET exists to support the Department of Defense in the conduct of both developmental and operational Test and Evaluation. This support extends to the United States armed services, defense agencies, the Office of the Secretary of Defense and qualified defense contractors who provide Test and Evaluation support to the Department of Defense. TECNET offers full featured electronic mail, an extensive bulletin board service, flexible file repository systems for text and binary file exchange, integrated facsimile capabilities, extensive data base support, Internet access and specialized information services. TECNET currently serves over 5,500 registered users supporting defense acquisition from the test and evaluation perspective.

NSA applied an approach to performing CSSE that identifies and integrates the security relevant tasks that must be performed within the overall Systems Engineering process. This approach brings diverse expertise from NSA, the certifying organization, and the customer organization together within a new CSSE framework. NSA has considerable expertise in all of the disciplines related to INFOSEC that can be applied to CSSE such as:

- Policy & Doctrine
- INFOSEC Evaluations
- Security Risk Assessment
- Security Profiling
- Certification & Accreditation

To support the TECNET program, NSA has assembled a team representing these INFOSEC disciplines and integrated their particular talents with the technical and operational expertise of the TECNET program office in a concurrent engineering process. NSA is "test driving" this CSSE process with TECNET.

TECNET operates an accredited C2 level system for unclassified support from the Naval Air Warfare Center - Aircraft Division, Patuxent River, Maryland. This system is accessible via direct dial-up modem lines, the Defense Data Network (DDN), the Defense Research and Engineering Network (DREN) and the Federal Telephone System for the year 2000 (FTS-2000). Another accredited C2 level System High SECRET TECNET capability also operates from the Aberdeen Proving Ground, Aberdeen, Maryland. This system is accessible via the Defense Secure Network One (DSNET1) and via direct dial up lines utilizing STU-III devices. It has been a TECNET goal since 1989 to integrate its classified and unclassified operations. Such integration was felt necessary to eliminate the costly redundancy of systems and data brought about by the distinctly separate systems serving the same community. Moreover, user acceptance of the classified capability would be better served if all appropriate data were more accessible in context. For these reasons, TECNET launched a focused applied research and development effort in 1991. This initiative was aimed at better understanding the dynamics and economics of operating a Multilevel Secure (MLS) TECNET capability in the not too distant future.

This initial TECNET research, funded through the Defense Acquisition Security Protection (ASP) program, brought TECNET to the National Security Agency (NSA). A natural union formed as TECNET and NSA learned that many key objectives were mutual and intertwined. As a result of their MLS oriented research program, the TECNET staff became increasingly aware that multiple disciplines would be necessary to field an MLS capability. At the same time, NSA was developing the engineering, management, and documentation concepts underlying an up-front concurrent systems engineering approach. By 1993 the affinity between TECNET's MLS needs and the rapidly maturing NSA CSSE approach was a natural fit. TECNET clearly needed a multi-disciplinary accelerated approach to MLS development at the same time that NSA was constructing a sound concurrent engineering framework. The linkage was evident and a concurrent systems engineering team was formed and working by the end of 1993.

Members of the concurrent engineering team will:

- describe their role within the team
- define what is new about this role in light of past experience
- discuss the value they see in this process
- identify the challenges they see in applying this process both to TECNET and to other systems.

**CHAIR:** Bradley Hildreth, National Security Agency

**ROLE:** I am the System Security Engineer committed to TECNET's MLS development effort through certification and accreditation. The role of a INFOSEC System Security Engineer (SSE) is to assist the customer with knowledge, talent, skills, tools, process methods, etc., so that they can build and maintain the best system for their needs. In this case I worked with the CSSE team to ensure the following:

- Commitment to TECNET's MLS development effort as first priority
- Emphasis on meeting needs as the primary goal
- Recruitment of NSA experts to participate
- Refinement of the CSSE process based on participant input
- Coordination and monitoring of the CSSE focused on TECNET
- Capturing customer's needs from both system developers and end users
- Translation of customer's needs into requirements including end user interface, performance, integrity, confidentiality, and access control
- Researching reusable information from other programs
- Development of alternative designs at each phase of CSSE for TECNET
- Modelling of relevant portions of system design
- Capturing feedback, trade-off decisions, system design, and risk
- Capturing information into reusable form at each phase
- Capturing CSSE lessons learned and communicated them to management and workforce
- Managing budget, schedule, and politics.

**SIGNIFICANT DIFFERENCES:**

The customer gets face-to-face involvement from all area experts from day one. This means a richer, faster, two way information flow in the specialities of Information Security Design, Evaluations, Policy and Doctrine, Threat, Risk, etc.

Instead of security and operational constraints placed on the user and system environment after system design, CSSE addresses security from the beginning as another system trade-off. This can help provide the system with user-friendliness, light administrative burden, effective and cost efficient security features, and other attributes which are usually subconsciously traded-off.

CSSE uses a phased design approach, with a place for every concern, arranged by level of detail. This means meetings stay on track and efficient, in spite of their large size.

CSSE stresses information and design reuse. This means that more customers can be supported and can receive results faster.

## **VALUE ADDED:**

The real value added should be judged by the customer. Please see the Value Added sections from George Hurlburt, Mary Mayonado, and Richard White, representing the customer, support contractor, and certifiers, respectively.

For future customers, CSSE's emphasis on face-to-face participating experts, phased design, and information reuse enables NSA to assist system developers efficiently. Previously, large, billion dollar programs have enjoyed excellent support from NSA. CSSE is a method for extending the same quality of support to the numerous small and medium-sized system development efforts occurring throughout DOD.

## **CHALLENGES:**

There are three main challenges to meeting future customer needs through CSSE:

- Providing an environment on future CSSE teams that supports the best integration and growth of all the team members - a working environment set up for success.
- Training the necessary SSEs in Concurrent Systems Security Engineering principles and practice.
- Growing CSSE teams in both number and experience

The good news is that NSA has some real lessons learned that support meeting these challenges, and world-class talented individuals to apply toward meeting customer needs.

**PANELIST:** Mary Mayonado, Eagan, McAllister Associates, Inc.

**ROLE:** I am currently on contract to the Naval Air Warfare Center, Aircraft Division, Patuxent River, Maryland to provide security support to TECNET. My role has changed from being the primary analyst for the initial, small scale TECNET MLS initiatives to being a member of a team of technical experts. As a member of the CSSE team, I perform the following responsibilities:

- Validation of TECNET user requirements
- Analysis & comment on proposed architectures, products, policies, etc.
- Development of the Certification and Accreditation (C&A) Plan; coordination of the C&A effort.
- Coordination with members of the CSSE team and the TECNET administrative staff (where their inputs are necessary) as well as members of the team previously dedicated to performing MLS research for TECNET.

**SIGNIFICANT DIFFERENCES:**

In general, the CSSE approach has the following significant characteristics:

- The CSSE approach provides a more thorough analysis because of the variety of expertise that is brought to the table. The meetings provide the opportunity to discuss/debate/analyze a variety of proposed scenarios.
- Participation of NSA, Program Managers, system users, system administrators, support contractors and certification officials on the CSSE team provides a necessary level of reality when making design decisions.
- Documentation of decisions and the rationale behind the decisions should make the certification and accreditation effort more valuable.
- Requirements traceability should provide the basis for future system upgrades.

**VALUE ADDED:**

My perception of the value added by the CSSE approach is described above. In addition, I feel that utilizing the CSSE approach with a team of technical experts from NSA and the services has a lot of potential cost savings to the customer/program manager. I believe this would be true even if NSA started charging some sort of fee for the service.

The level of expertise and variety of experience brought to the table by the different members of the CSSE team would be very difficult to find within a single company or organization.

**CHALLENGES:**

- Working with customers to change the perception many have of NSA; helping them to look at NSA as a resource to be used and not as an organization to be feared.
- Working with the current contracting environment to set up contracts that allow us (as contractors) to interface directly with NSA.
- Developing a C&A approach in a tri-service environment; taking the NSA C&A process and working through a real-world problem.

**PANELIST:** Teresa Acevedo, Pulse Engineering, Inc.

**ROLE:** I am currently under contract to the National Security Agency to provide system engineering and design support to the TECNET concurrent engineering team on the MLS development effort. My responsibilities include working with the concurrent engineering team to translate customer needs to design requirements for MLS TECNET, identifying and analyzing design alternatives, and supporting the execution and documentation of the CSSE Process.

**SIGNIFICANT DIFFERENCES:**

The MLS TECNET effort is applying concurrent engineering in a structured top down design approach. Some of the additional attributes of the CSSE process include:

- Progressive and structured, informal design reviews
- Risk assessment at each level of design detail
- Requirements tracking and design compliance analysis for each level of detail
- Detailed, structured design documentation that can be reused by other similar systems.

**VALUE ADDED:**

The MLS TECNET effort has realized the following benefits from the CSSE approach:

- Richer design solution set(s) based on diversity and resulting synergy of concurrent engineering team participants
- Timely customer validation of requirements and design(s) through structured concurrent engineering team meetings
- Increased design efficiency and reduced design time through real-time security assessment feedback
- Verification of design completeness at each level of detail.

The MLS TECNET experience will likely lead to potential savings on similar programs through the reuse of design analysis and documentation.

**CHALLENGES:**

The MLS TECNET CSSE team has successfully met several challenges in reaching its current point.



The primary challenges that CSSE teams are likely to meet in subsequent efforts include:

- Specification of security requirements that are hierarchical and verifiable and that support a layered design approach
- Keeping the design team at a consistent level of detail through the design process to maintain a focus that allows for progress
- Limited releasability of product analysis information due to classification and/or proprietary nature (both contractor and government)

These concerns must be overcome to enable design reuse.

**PANELIST:** Jenny Himes, National Security Agency

**ROLE:** My role on the CSSE team is to help identify policies that are applicable in governing the use of classified and sensitive information within MLS TECNET's environment.

**SIGNIFICANT DIFFERENCES:**

In support of TECNET, I have taken a very different approach by outlining applicable national policies and doctrine for TECNET's information early in the design process, rather than for a specific system with a completed design. To aid with this process a new document search and retrieval database comprised of national policy, DoD directives and doctrine was created and utilized. In the TECNET Requirements Analysis review, I presented national policies and doctrine applicable to TECNET in a layered approach, concerning information, automated informations systems (AIS), and Communications Security (COMSEC).

**VALUE ADDED:**

This new approach to policy and doctrine was well received by the TECNET customer. It seems when you talk with the customer first about "information" rather than "security" - it creates a stronger understanding and commitment for protecting that information. The policy and doctrine information and its interpretation was used to develop the TECNET security requirements.

As part of the CSSE team, I have continued to provide policy and doctrine as a part of each design phase.

**CHALLENGES:**

Providing assistance to a large number of diversified customers in quantifying and managing risk, recommending INFOSEC countermeasures for residual system risk, while continuing to provide policy and doctrine support.

**PANELIST:** Gregory Wessel, National Security Agency

**ROLE:** My responsibilities on TECNET are to provide system security guidance during the Concurrent Systems Security Engineering (CSSE) Process, provide COMPUSEC and system security evaluation support throughout the CSSE Process, participate in the Risk Assessment process of TECNET and participate in the System Security Profiling effort for TECNET.

**SIGNIFICANT DIFFERENCES:**

The most significant difference in following the CSSE Process is that the systems evaluator is involved in the process from the start. The evaluator will be able to identify weaknesses and vulnerabilities during the CSSE Process which enables them to influence the structuring of the security posture of the design and help in choosing the products that provide the best possible security solution.

**VALUE ADDED:**

I believe that there is value in an evaluator being a TECNET team member in the CSSE Process because I believe he can spot many of the system vulnerabilities in the early design phases. The process allows team members from the customer's organizations, the certifiers, the accreditors, doctrine, Risk Assessment, and the systems evaluations community to meet and develop the most secure system possible for TECNET. Each member is involved in all phases of the CSSE Process and provides input relevant to the security design of the system. The process also enables the team to address security issues early on enabling the customer to make a more intelligent decision on choosing security solutions real-time which is more cost effective.

**CHALLENGES:**

There are challenges that the team will incur during the CSSE Process:

- Working as a team of 20 people striving to provide a secure system solution is sometimes tough. Everyone must remember what their role is and provide the pertinent information when needed.
- Keeping the team focused on the particular phase of the CSSE Process is a problem because the team is always looking to the future instead of concentrating on the present. This was a very challenging part of the process while in the design phase because the team was looking ahead to equipment solutions to meet the design instead of choosing a secure design and then looking for the right set of security equipment solutions for the system.
- During the CSSE Process, juggling security -vs- cost with the customer is always a challenge that can be overcome, since the entire team is involved at each phase of the process making real-time decisions that are more cost effective.

**PANELIST:** Randy Blair, National Security Agency

**ROLE:** My role on TECNET is to provide Security Risk Assessment to support to the CSSE Process. My responsibilities include helping the CSSE team develop an understanding of the security vulnerabilities, weaknesses, and risks associated with proposed TECNET system designs. This information is then quantified and used to support design trade-offs at each stage of the CSSE process.

**SIGNIFICANT DIFFERENCES:**

The most significant difference in following the CSSE process is the use of security risk assessment techniques at each stage of the CSSE process. The other significant difference was that the security risk information was developed by the entire CSSE team. The results of these security risk assessments were used with other system risk information (e.g., performance, cost, and schedule) to drive the TECNET system design.

**VALUE ADDED:**

By providing security risk assessments at each stage of the CSSE process, the CSSE team developed a profound understanding of the security implications of its design decisions. Each team member better understood the value and impact of security features to their specialty area. As alternative system designs were developed, the entire team (not just the security specialists) would evaluate the merit of the design from both an operation and security perspective. This leads to more effective designs.

Another significant value from the use of risk assessments at each CSSE stage is the introduction of security requirements and constraints early in the system design process rather than trying to fit security in at the end of the design effort. This early introduction of security allowed the team to develop creative and cost effective security design alternatives.

**CHALLENGES:**

Vulnerability information is typically highly classified to protect fielded systems that may be exploited if vulnerability information is broadly disseminated. This was a significant problem for the TECNET CSSE team since many team members could not access this data and participate in the security risk assessment. Once the information was filtered and downgraded so that the entire team had access to it, the security risk assessment became a very important part of the design process. The most significant challenge will be to find a balance between the needs of new systems for this vulnerability information and the need to prevent its dissemination in a manner that would be harmful to fielded systems.

Most vulnerability information has been generated against specific products and is very detailed. Providing system vulnerability information at each stage in the CSSE process requires the development of more conceptual vulnerability characterizations. This challenge is significant now; however, these vulnerability characterizations should become common as NSA becomes more involved in supporting systems developments.

**PANELIST:** Richard White, Air Intelligence Agency,  
Air Force Information Warfare Center Engineering Analysis Directorate.

**ROLE:** I have been tasked to perform the role of Certification official for the Air Force on TECNET. As a certifier it is my responsibility to identify to the Designated Approving Authority (DAA) all known risks to operate the TECNET system in a secure environment (both physical and electronic). This role requires that I remain completely independent of the final design decisions.

**SIGNIFICANT DIFFERENCES:**

The concurrent systems security engineering process changes the entire up front approach to security engineering. The most significant difference is the empowerment of the certification official to directly affect the design during the system engineering process. The certification official is delegated down to a working level to allow a proactive identification of risk to the system beginning from the conceptual design through the actual product selection and integration. By allowing proactive interaction the certifier can enlighten the design team of the risks incurred based on the design decisions being made. The certifier can present options which will help mitigate the risks but maintain the operational requirements. The second significant difference for the certifier is the requirement that the certifier must have a knowledge of the certification process, trusted products and experience in design and systems engineering. This is a change for certifying officials who typically have the role of a project or program managers.

**VALUE ADDED:**

The CSSE Process adds the value of up front and concurrent risk identification in a very proactive manner. This allows product and system designers to modify the design early, while it is still cost effective to do so. Additionally, with the certifier directly involved in the decision process there is no "hear say" information going forward to the DAA; the security decisions and their rationale are reported directly to the DAA from a person on the system engineering team.

**CHALLENGES:**

There are several challenges to be overcome using the CSSE Process:

- The need for the certification officials to have a high degree of technical expertise and diversity. This knowledge base is very uncommon in the DOD environment today.
- The need for the CSSE Process to work with other DOD processes such as the source selection process and the acquisition process defined by DODD 5000.1. TECNET does not have a contractor responsible for the entire system integration effort. Programs with this type of systems integration contractor will be bound by contractual requirement. Current acquisition regulations were not developed with concurrent engineering teams in mind. This could create conflicts as contractor personnel try to adhere to these rules and regulations.

- **The need for the DAA to delegate the certification official to a working level. The current management structure within DOD does not allow the responsible official to be at the required grade or rank level.**

**PANELIST:** George Hurlburt, Naval Air Warfare Center, Aircraft Division

**ROLE:** I serve as the Executive Secretariat for the Test and Evaluation Community Network (TECNET). In this capacity, I report to a tri-service Steering Committee commissioned to oversee TECNET. This committee holds me responsible for the daily operations and future development of this growing automated system

**SIGNIFICANT DIFFERENCES:**

These meetings of the joint TECNET/NSA Concurrent Engineering Team have grown in intensity and significance since their inception. The TECNET team brings several necessary perspectives to the table:

- The system administration function, system security management role, system engineering activities, network security and planning responsibilities and the program management functions are fully represented within the TECNET team.
- By extension, TECNET has recruited and funded a tri-service certification team drawn from the three services to carry out this important independent task. These individuals have also been integrated into the CSSE team.
- In this and other cases, functional sub-groups are identified for separate deliberations in specialty areas as required.
- TECNET is also seeking full accreditation through its management structure via the two star Board of Operating Directors (BoOD) for Test and Evaluation. This group oversees the TECNET Steering Committee.

Likewise, NSA brings great and complementary expertise to the table. The natural dynamic between the actual operational perspective of the TECNET members and the security perspective of the NSA members has produced a meaningful outcome at each stage of the CSSE process. It is this process, which all parties have pledged to follow, that focuses the activities of all concerned. At each stage of this well defined CSSE process the level of specificity grows as the options clearly narrow through strong consensus. While discussion is frequently animated and vivid, the process places clear focus on the ultimate team dynamic. To date, the process has served as the glue that makes the otherwise highly diversified team cohesive.

**VALUE ADDED:**

The benefits of this experience to TECNET have been invaluable. Left to its own devices, TECNET may have reached similar conclusions, but it is doubtful that many of the desirable attributes of the CSSE process would have ever been fulfilled.

The CSSE process has benefitted TECNET by providing:

- Successive and topical documentation demonstrating the distinct steps in the highly deductive process.
- Process oriented discipline that places meetings above day to day operations, so action items are consistently addressed.
- An accelerated integration schedule
- Mutual teaming between agencies that has made the acquisition of support funding and skill such as the certification team far more credible and easily accomplished.
- Mutual respect among the team members that has fostered a professional atmosphere that is highly charged with enthusiasm. Such respect could not have emerged without the natural association of TECNET and NSA players.

Without this teaming, the chemistry of day to day operations in the same TECNET environment would have diminished the impact of the CSSE process, no matter how well conceived. Moreover, all parties brought skills not easily replicated or even available on the complementary side. Finally, joint recognition of the soundness of the CSSE process has helped forge the vital links between the various team players.

#### **CHALLENGES:**

The role of the TECNET Secretariat in this process has been important, but not vital. The primary challenge for a program manager is to maintain an objective viewpoint tempered by programmatic realities. The program manager must be receptive to new ideas while always balancing them against necessary programmatic trade-offs. If a line of reasoning goes beyond program means, than a discussion of alternatives, removal of potential roadblocks through creative management, or a tactful redirection is indicated. When appropriate, the program manager can serve as a catalyst for new ideas, opportunities and approaches, but the challenge is to avoid the temptation to dominate the sessions. If the program manager becomes too heavy handed, the process becomes stifled. Otherwise, it is the task of the system program manager to foster harmony and enthusiasm among the group.



## **Panel: Provisions to Improve Security on the Internet**

Dr. Harold Joseph Highland, F.I.C.S. **Chair**  
*Computers & Security*  
562 Croydon Road  
Elmont, NY 11003-2814  
highland@dockmaster.ncsc.mil

Frederick M. Avolio  
Trusted Information Systems, Inc.  
3060 Washington Road  
Glenwood, MD 21738  
avolio@tis.com

Dr. Stephen M. Bellovin  
AT&T Bell Laboratories  
600 Mountain Ave  
Murray Hill, NJ 07974  
smb@research.att.com

Assistant Professor Matt Bishop  
Department of Computer Science  
University of California, Davis  
Davis, CA 95616-8562  
bishop@cs.ucdavis.edu

William R. Cheswick  
AT&T Bell Laboratories  
600 Mountain Ave [Room 2C-416]  
Murray Hill, NJ 07974  
ches@research.att.com

Dr. Jon R. David  
The Fortress  
P. O. Box 731  
New City, NY 10956  
david@dockmaster.ncsc.mil

Colonel Frederick A. Kolbrener  
11998 Mojave Lane  
Lake Ridge, VA 22192  
kolbrener@dockmaster.ncsc.mil

A. Padgett Peterson, P.E.  
Martin-Marietta Information Group  
12506 Lake Underhill Road [MZ342]  
Orlando, Florida.  
padgett@tccslr.dnet.mmc.com

### **About This Session**

Networks operating under TCP/IP have inherent weaknesses. Try a word association test: Internet security? → *firewall*. If designed properly, they work; but they have their weaknesses. Are firewalls really the ultimate answer?

This panel is an olio of network communications, computer security and personnel specialists. They will discuss the critical *holes* in Internet security. Can these holes be plugged? What can be done quickly and easily to increase security and assure privacy? What is really needed?

Quick fixes can reduce security threats. Sniffers can test firewalls. It is obvious that we cannot redesign the Internet. Therefore we all agree that firewalls and modification of protocols are not the full solution to the network security problem. Where do we go from here?

**Note:** The opinions expressed in the following position papers and in the statements made during the session by any of the participants of the panel or the chair, do *not* necessarily express that of their employers or any professional organizations to which they belong nor those of the sponsoring agencies of this conference.

# Security on the Internet •••• A Viewpoint

by Harold Joseph Highland

As a dinosaur any discussion to improve network security is *déjà vu*. My first computer security problem, and that was about 35 years ago, was to determine which door lock to install to keep intruders out of our computer *laboratory*. The second came a year or so later when I saw the first punched card file cabinet with a *lock*. Why spend the extra \$10 for a simple lock? As the salesman explained, it would provide added security for our computer laboratory.

We found a real need for security in the late 60s when we attached a terminal to the mainframe and placed that terminal outside the computer room. But it was an easy solution. The user entered his/her name and a table lookup granted the access; we didn't bother with passwords then.

The Internet<sup>1</sup> in the United States was created for a free exchange of information among scholars and researchers. Most of us had a common goal and we freely exchanged data and even programs. Computer security was based on trust, not passwords or gadgets -- biometrics, tokens, retina scanners. We did not read each others mail nor did anyone consider breaking into another system -- it was always wide open to us. The question of security became important to us when our own cyberspace was invaded by *bandits*<sup>2</sup>.

Of course we have a different situation today. We have really advanced. Consider the following:

- Internet, Inc. does not exist!

No one collects fees from the individual internets. Everyone pays for his own way, more or less. NSFNET in the U.S. is paid for by the National Science Foundation. EASInet in France is funded by IBM and 18 European institutions in nine countries. CREN, the Corporation for Research and Educational Networking is a membership organization with fees.

- Internet is a loose confederation of internets.

Each has its own opinions about how things should work. There is no single authority for standards and controls. Each network has the right to do its own thing; believe me many do.

- Internet is now international; there is no universal Bill of Rights to protect human rights.

World laws and practices vary greatly when examining individual rights and privacy. I am not even considering third world dictatorships; they have their own rules. I am talking about the

---

<sup>1</sup> Note I use *internet* [lower case *i*] to refer to any collection of networks interconnected by a set of routers which allow them to function as a single, large virtual network. *Internet* [capital *I*] is the largest internet in the world.

<sup>2</sup> Note I use *bandits*, not *hackers*. *Bandits* were students from a neighboring university who illegally used our system because of a port shortage on theirs. We use *hackers* to describe many of our former top students.

United Kingdom, France and the Netherlands. The Defence of the Realm Act in the U.K. gives the Queen the right to read anyone's mail. In France you register your encryption programs and keys with the government. In the Netherlands the government may have by now a law that permits the use of only government approved encryption algorithms.

- There are no international laws governing Internet.

The neo-Nazi network in Germany sends you their hate literature via e-mail. They ignore your repeated requests to delete your name from the list. What can you do legally? Or consider the Norwegian programmer, who this past June, was enraged by seeing a Phoenix law firm's advertisement [which he considered offensive] on Usenet. "He launched the electronic equivalent of a Patriot missile; each time the law firm sent out an electronic advertisement, his computer automatically sent out a message that caused the network system to intercept and destroy the firm's transmissions."<sup>3</sup> And he was hailed by many overseas and in the States as a hero.

- There are many users on the Internet who do not want controls.

As of April 1994 there were some 32,000 internets in 76 countries with e-mail gateways to reach 146 countries and territories. There were well over 2.2 million computers on the Internet. And there is an estimated 35 million users. Military and commercial users are a minority!

The Internet is a classic example of a computer system that is being retrofitted for computer security. Because there are no standards or laws that can be enforced the world over, we should address four basic problems:

- [1] how to stop uninvited guests and messages from entering our systems,
- [2] how to protect our messages from being read by unauthorized eyes as they pass over the internets,
- [3] how to verify the source of messages we have received, and
- [4] how to verify that messages sent were actually received.

This may sound like a medieval fortress/moat mentality but it is as good a starting place as any. We have the technology to do the job. Having worked on the international level for more almost two decades, I see little chance of implementing any meaningful network security for many years to come. Possibly local internet fortresses might work on a national basis for those who elect to go that route. Others in the world may follow; I hope so. But it is up to them; we cannot dictate the rules.

But remember we cannot do this job with technology alone. We must involve our users, the people on our internets. People play a more vital role than hardware. Our attempts at information

---

<sup>3</sup> Peter H. Lewis "No More *Anything Goes*: Cyberspace Gets Censors," The New York Times, June 29, 1994, page A1.

security education thus far has often been pitiful. Maybe we should turn to personnel managers and psychologists, specialists knowledgeable in man-computer interface, to see if we can complete the security job beyond building firewalls and using encryption.

**Harold Joseph Highland** received his B.S. in 1938; as honor graduate was commissioned in the U.S. Army. Four years later he received his Ph.D., some 15 years before he entered computing in 1957. His formal education in computer science was a one-week course in machine language at IBM in 1959. He quit the program after that week and studied on his own, using his university's IBM 650 and an IBM 1620 as his learning tools.

In support of his wife's contention that he could never hold any job for a long time, note that Dr. Highland has worked as a research statistician, tv producer, newspaper columnist, consumer magazine editor, AP stringer, economist, book editor, educator and handyman. Being a workaholic he periodically held two jobs at once.

He turned to academia in 1957 and became Dean of a graduate school at a university in New York City. From there it was all down hill. He served as Associate Dean of a liberal arts college for a few years. He then left to become a Department Chairman and Director of the Computer Center at the State technical college, filling in with teaching at the State medical school. In 1978 he was promoted to the rank of Distinguished Professor by the Trustees of the State University of New York. Three years later he retired when his wife retired from the City University of New York.

To keep busy after retirement he created **Computers & Security** and acted as Editor-in-Chief. Two years later this refereed publication became the official journal of IFIP's Technical Committee 11 on computer security. Together with his wife, who served as Managing Editor, they ran the journal until their second retirement in 1991. As Editor-in-Chief Emeritus he still writes his column, "*Random Bits & Bytes*," regularly for each issue. Besides he serves on the editorial board of six professional publications in the U.S. and overseas.

A prolific author he has written several hundred technical articles and papers as well as some 27 books. Several of the books have been translated into Japanese, German, French, Italian, Russian, Dutch, Swedish and Finnish. In addition to his writings, speeches and workshops, Dr. Highland serves as Counsel to the Technical Committee on Computer Security of the Chinese Computer Federation [a government group] of Beijing, PRC and other government agencies here and overseas.

He was the first recipient of the *IFIP Kristian Beckman Award* in 1993, which was made in recognition of his significant contributions to the development of information security, especially achievements with an international perspective. He also received the *IFIP Outstanding Service Award* for his role in international information security education. This year he received the *Thomas Fitzgerald Award* in recognition of his contributions in infosec from the ISSA. He has awards for his work in modeling and simulation, random number generator research, newspaper and magazine writing, etc -- but they are too numerous to include here.

Dr. Highland is the only American Fellow of the Irish Computer Society [ICS]. He is also a member of the New York Academy of Science [NYAS] and the American Association for the Advancement of Science [AAAS]. He's been a member of the Association for Computing Machinery [ACM] for 30 years. He is a member of The Internet Society [ISOC], the IEEE's Computer Society [IEEE/CS], Computer Professionals for Social Responsibility [CPSR], Information Systems Security Association [ISSA] and the Society for Irreproducible Results [SIR].

For those who want more: additional biographic data can be found in *Who's Who in the World*, *Who's Who in America*, *Who's Who in science and Technology*, *Who's Who in the East*, and *Who's Who in Education*.

© Complit, Inc. 1994. All rights reserved.

## Security on the Internet •••• A Viewpoint

by Frederick M. Avolio

*Firewalls Are Not Enough:* You have just bought a house. It is red. Is a dead-bolt lock on the front door enough to secure it? The color of the house is extraneous information; you haven't been given any other information. You have no idea if a dead-bolt locked front door is sufficient. You wouldn't dream of making a security related decision on such limited information, and yet daily organizations are trying to establish security perimeters for their networks with little more data than we have on the above-mentioned house, thinking that firewalls are enough. I've nothing against firewalls. In fact, I am all for them. The problem with today's attention to firewalls is that focusing on an Internet firewall focuses on only part of the broader area of network security.

To secure a private network, we establish what we call a network security perimeter. A security perimeter is established by a security policy and security policy enforcement mechanisms and methods. An internetwork firewall may be one of the mechanisms. There are usually others as well, but they come after the security policy, not before. A security policy must be joined to an implementation (the mechanisms and methods), but not directly. The things that join a security policy and an implementation together -- and help them to mirror reality -- are a risk analysis and a business needs analysis.

These steps are well practiced in the DoD arena -- although, unlike in the private sector, the security policy often comes first -- but much less so in industry, especially in relation to connecting to the Internet.

Not only is each of these four steps -- a security policy, a risks analysis, a business needs analysis, and identifying security mechanisms and methods -- required, but order is important, too. While among purists, a security policy is viewed as primary and something that should be established before anything else is done, I suggest that a security policy useful for an organization cannot be drawn up unless a clear understanding to the answer "What are the threats" exists. To put it another way, an organization needs to know what it needs to protect and what it is afraid of.

Often a security survey is required to gather this information. Two people in an organization might both agree that they want to protect their network against unlawful electronic entry. Ask one person why, and she might say that she would be afraid of the information on the network getting out (to competitors, perhaps). The other person might say that he wants to keep the company from the "bad press" of a network break-in. A security survey gathers everyones list of what needs to be protected, from what, and why.

This information, of course, is drawn out into a formal risk analysis, wherein threats are postulated, vulnerabilities identified, probabilities of the exploitation of those vulnerabilities assessed, and countermeasures identified and priced out for cost effectiveness. (Again, while the purist would say that a cost benefit analysis has no place in a risk analysis, I say that it has to go somewhere, and since it must be done in conjunction -- hand in hand with -- with a risk analysis, I call it out as part of the risk analysis.) Without such a risk analysis, an organization will have no way of knowing if their security policy matches reality and has no way of measuring if the methods they put in place are adequate.

A business needs requirement document is also needed. This does not have to be elaborate, but should include what the service requirements are and a statement of what happens to the business if the services are interrupted.

After these two steps, a security policy may be developed. Every organization thinking of connecting their private network to another, such as the Internet, has a network security policy. The policy may not be written down or well formulated, but the organization has one, if they are lucky, and they have several in conflict, if they are like most organizations.

A security policy must match reality, which is why a risk analysis and a business needs analysis should precede it. Readers may remember the television program "WKRP in Cincinnati." The news announcer of that radio station, Les Nessman, didn't have a private office and couldn't get one, so, Les established his office perimeter with masking tape applied to the carpet. He got annoyed when someone walked through the "wall" instead of waiting at the "door" until invited in. To Les, his policy was sufficient. There are organizations today that likewise have policies that do not match reality and, so prescribe methods that are insufficient, while like Les Nessman, thinking -- or pretending -- that they are sufficient.

After a risk analysis and a business needs analysis, the security policy can then suggest security mechanisms and methods. Mechanisms and methods are based on the security policy, help meet business needs, and counter perceived threats. In a network security perimeter, we may use security mechanisms and methods such as encryption of files, data transmission encryption, user authentication servers and tokens, and internetwork firewalls.

Firewalls are not enough. A risk analysis and a business analysis is almost always required, leading into the development of a security policy and the prescription of security mechanisms and methods for implementation. Doing this once is not enough. Threats change, vulnerabilities change, business requirements change, and the available countermeasure change. All of these must be periodically and routinely re-evaluated.

Security methods, such as Internet firewalls, are very popular now, but many organizations may believe, or be led to believe, that an Internet firewall alone is sufficient for securing their network. It's like getting the most secure front door money can buy for your house but leaving the garage door unlocked, or the same, weak sliding door entrance from your back deck. It's like making a stand in a fortified city, with gates and walls, but forgetting about the water shaft that runs below and outside the walls, allowing an army to make a secret entrance. (It's been done: 2 *Samuel* 5:6--8.) And it is like Les Nesmen's office. Only if everyone plays by the same rules is it effective.

**Frederick M. Avolio** is a principal analyst with Trusted Information Systems, Incorporated, and is responsible for commercial network security consulting and product development. He is product manager for *Gauntlet*, TIS' Internet Firewall Product. Since the early 70s, he has lectured on the subject of Internet gateways and Firewalls and electronic mail configuration and has performed consulting services in these areas, both for government and in the private sector.

He has written on the topic of Internet firewalls and network security and is co-author of a book on Sendmail coming out at the end of the Summer. He has one wife, five children, and another on the way, so obviously his activities are not limited to network security.

© Trusted Information Systems, Inc. 1994. All rights reserved.

## Security on the Internet •••• A Viewpoint

by Stephen M. Bellovin

The Internet is often a dangerous place, and it is becoming more so every day. To further strain an already tired metaphor, the *Information Superhighway* runs through a bad neighborhood.

There are three main reasons for the problems we are currently experiencing: lack of standardized cryptographic authentication, buggy host software, and the difficulty of systems administration.

Unlike the other two problems, we know how to do strong authentication. No new science is needed, simply some engineering decisions and the will to develop and deploy the necessary techniques. To be sure, there are obstacles, both economic and legal, to widespread use of cryptography; with luck, they can be overcome.

However, the best cryptography in the world will not protect you if the endpoint of an incoming call is a piece of buggy software. The message may be both authentic and secret --- but it may be coming from an authentic enemy who is using bugs in your host software to penetrate your machine.

Here, we have a problem that may be insoluble. Empirically, the industry as a whole cannot produce reliable software. To put it bluntly, most programs are buggy. And by Murphy's Law, if a program is both buggy and security-sensitive, some of the bugs will be security-related as well. Of course, this applies to network programs, too.

A related issue is the difficulty of system administration. Modern computer systems have lots of knobs that need adjusting. Erroneous settings can make a system either vulnerable or difficult to use; vendors often react to the latter problem by shipping systems with minimal protections, since that eases the administrator's basic task. To run a secure system, one must then find and tighten all of these myriad widgets; too often, administrators don't know how to find all of them.

Our solution is a firewall, an electronic barrier between our internal networks and the outside world. With a firewall, only one machine is exposed (and hence must be very tightly administered), rather than many. It runs much less software than a general purpose machine; accordingly, there are many fewer security bugs to worry about. There is one central point for the deployment of a strong but non-standard authentication system. In short, to dredge up our metaphor yet one more time, we have created a customs stop in Cyberspace.

It is important to realize that firewalls are not a solution to a network security problem. Rather, they are a network response to a host security problem.

Firewalls are not a panacea. Ours guards a single entry point; it does not address other threats, such as insider attacks, wide-open modem pools, physical security issues, TEMPEST, etc. These threats need to be dealt with, too; defenses here include trying to harden all internal hosts.

Even in their chosen domain, firewalls have their weaknesses. Attacks at a higher level---crafty mail headers, Trojan horses in imported software, etc. --- can still get through. If your system or

your users are vulnerable to such attacks, you still face dangers. Trying to eliminate such residual risks is an open research topic.

Nevertheless, firewalls are an important contributor to overall site security.

**Steve Bellovin** received a B.A. degree from Columbia University, and an M.S. and Ph.D. in Computer Science from the University of North Carolina at Chapel Hill. While a graduate student, he wrote the original version of pathalias and helped create netnews. However, the former is not an indictable offense, and the statute of limitations on the latter has expired. Nevertheless, he is still atoning for both actions. He has been at AT&T Bell Laboratories since 1982, where he does research in networks, security, and why the two don't get along. He is the author, with Bill Cheswick, of the recent book *Firewalls and Internet Security: Repelling the Wily Hacker*<sup>1</sup>.

---

<sup>1</sup> *Firewalls and Internet Security: Repelling the Wily Hacker* by William R. Cheswick and Steven M. Bellovin was published in 1994 by Addison-Wesley Publishing Company, One Jacob Way, Reading, MA 01867 USA. Price: US\$26.95 [ISBN 0-201-63357-4]. The book is available from local bookstores or by calling (800) 822-6339 in U.S. and Canada. A detailed review of this book is included in Dr. Highland's regular column, "Random Bits & Bytes," in Computers & Security, Volume 13, Number 3, May 1994.



## Security on the Internet •••• A Viewpoint

by Matt Bishop

Security consists of three attributes: confidentiality, integrity, and availability. The degree to which the absence of any of these features implies a lack of security depends entirely on the specific definition of security being used. For example, on a public bulletin board system, security consists entirely of the last two attributes, since the function of a bulletin board is to pass information to all its users, which implies a lack of confidentiality.

The diversity of the sites connected to the Internet renders the question "how secure is the Internet" meaningless. Evaluating remote hosts, and those hosts making up the network infrastructure, to see if they conform to the local host's requirements for each of the three attributes shows the assumptions the local host may make when evaluating the security of the data being sent or received over the Internet.

Each protocol provides a set of security services so that it may function correctly in the face of an adversary. With some protocols (such as tftp or ident), the data is simply placed on the network, so the set of security services is null. With other protocols, such as privacy enhanced electronic mail, the data is transformed to ensure correctness and privacy in transit to the destination, so the set of security services is not empty.

The protocol designer identifies a set or sets of security services appropriate for that protocol; the users of the protocol determine if those support services enhance the security of the protocol, given their specific environment, or if they must add other security enhancements, or if they should simply use a different protocol. For example, the security mechanisms of telnet are minimal, in that they allow the interception of cleartext passwords; some sites have added encryption to their versions of the telnet protocol, thereby enhancing its security by concealing the passwords using encryption.

The Internet Security Architecture (ISA) is a collection of generic types of threats to network-based services, and a description of mechanisms to counter them. Protocol designers can analyze their protocol within the framework of this model, and choose countermeasures for those threats that pose an unacceptable risk.

If the user of a protocol does not understand the type of threats that the protocol protects against, that user acquires a false belief in the security of the protocol and the correctness of the data and commands upon which security-related decisions (such as access) are based. For example, the ident protocol identifies the port and user at the remote end of a connection. It does not guarantee correctness, because the remote system could lie or the data could be changed in transit. Hence any mechanism that trusts the remote identity as given by the ident protocol is basing a decision on untrustworthy data.

The sending host's security mechanisms protect the data and commands that the protocol transmits after they are generated but before they are placed into a packet. Similarly, once received, the data and instructions are removed from the packet and then given to the waiting process. If an attacker is able to read, alter, or delete the data and commands, the attacker has breached the security of

the network communications. So, the vulnerability of a host on the Internet affects the security of other hosts that assume the vulnerable host is not compromised.

The network infrastructure is itself supported by hosts -- computers with vulnerabilities. That these hosts function correctly is a fundamental assumption of all computers connected to the Internet. When this assumption is incorrect, many hosts can be subverted.

Thus, Internet security has four cornerstones:

- [1] the definition of security of each host on the Internet;
- [2] the knowledge of the security of those hosts with which it communicates;
- [3] a knowledge of the definition of security for the protocols used; and
- [4] a knowledge of how well these definitions are realized.

**Matt Bishop** received his Ph.D. in Computer Science from Purdue University, where he specialized in computer security. He was a research scientist at the Research Institute of Advanced Computer Science and was on the faculty at Dartmouth College before joining the Department of Computer Science at the University of California at Davis.

His research areas include computer and network security, and he teaches both, along with operating systems and software engineering. He chaired the first two UNIX Security Workshops. His column on computer security appears regularly in the *Best Practices* newsletter.

© Compulit, Inc. 1994. All rights reserved.

## Security on the Internet •••• A Viewpoint

by William R. Cheswick

The traditional TCP/IP network application has been written with limited concerns about security. We've been so pleased that the dog danced that we failed to notice that it is rabid.

- Telnet and FTP passwords have always been targets of easily-tapped Ethernets.
- Rsh and rlogin have allowed users to make site security policy (via .rhosts) and are subject to DNS-based attacks.
- The basic premise of the X window system is to give away control of the screen, keyboard, and mouse.

In general, many services are implemented with large, incomprehensible programs. These are often woven with 'ifdef's, spreading machine dependencies throughout the code. They often run as user 'root' without needing the privilege, or without relinquishing it when it is no longer needed.

The vendors' responses to these problems vary, leaving the ultimate decisions to the individual system administrators. Since administrators' skills vary, and we have tens of thousands of hosts to protect, a perimeter defense in the form of a gateway provides a lot of protection from external intruders who would exploit security holes if they could.

But it is getting harder to protect a large company. We get requests of the form: "we want a secure gateway, and we want to let X, NFS, the MBone and, of course, WWW access through it." Sometimes the security is not available, and the most appropriate gateway is a simple wire.

It would be nice to be able to let more services a gateway in a safe manner.

- a TCP-based network file system. NFS's UDP port in the kernel is a pain. I can authenticate and encrypt a TCP connection.
- One-time password support in a login mechanism that is used by telnet, rlogin, ftp, and others.
- Simple proxy protocols for gating services. The little bag attached to the large Mosaic server is the wrong answer. If it is more than two pages of code, it is probably wrong.
- Smaller, simpler client programs can be audited, controlled, and trusted more easily.

**Bill Cheswick** is a Member of the Technical Staff at AT&T Bell Laboratories in Murray Hill, NJ. He works in the Computer Science Research Group: the same swell folks who brought you Unix, C, and the Belle chess computer.

He is currently installing the third version of an Internet gateway, fiddling with Plan 9, and occasionally acting as postmaster. He frequently consults on security issues and is a reluctant PC expert.

He broke into his first computer at Lehigh University, and was graduated anyway in 1975 with a BS in something-that-looks-like Computer Science. Since then he has picked up a patent at the American Newspaper Publishers' Association/Research Institute, provided system programming to a variety of universities, and pursued errant students at same. He signed on at Bell Labs in 1987.

His favorite polypeptide is oxytocin. His least favorite neurotransmitter is serotonin.

## Security on the Internet •••• A Viewpoint

by Jon David

Security professionals know that any security can be breached with enough effort. With the Internet, though, it requires only minimal efforts to effect various types of security breaches.

The RFCs (Requests for Comments) on which the Internet is based clearly detail the operations of Internet components, and those details show not only what to [mis]do, but how to get away with it. Further, devices which are legitimately and properly used for *good* things, such as the verification of the propriety of traffic on and through a given host, are also readily misused to do such things as capture passwords. (These are the *sniffers* which have gotten so much bad press.)

The standards set forth in the RFCs are treated as a floor (minimum), but not also as a ceiling (maximum), so that individual hosts may deviate significantly from one another. There are no firm *laws* governing host operation on the Internet, and each host is, within certain broad constraints, free to do almost anything. We are left with a situation where, for example, a message sent to one host may be rejected in whole or in part (because it at least minimally deviates from the "specs"), yet is fully accepted by a second host )because that host has made its software more tolerant).

Most of us know hosts serving large numbers of users: thousands, tens of thousands, even hundreds of thousands of users. Logic would indicate that these users would be better served if the specifications coordinating these hosts were tighter and more formal, and closer adherence to these specifications was required for participation on the Internet. We now have upwards of 20 million Internet users, and that number is reported as growing at the rate of 15% per month. The hosts servicing these users have a frequently large dollar investment in their present software, and for most of them the priorities are to maintain their level of service and to add more users. While the logic might have applied when the Internet was being designed, it now conflicts with present priorities.

Possibly most insidious is the ability of even individuals, with little more than a single personal computer, to become Internet hosts. This means that certain hacker/cracker or otherwise disruptive/abusive practices which require host control (i.e. sys admin status), and which are not normally within the province of mere users, now can readily be done (as permitted by the RFCs); anyone can become a rogue host, and as such can capture passwords, spoof messages and the like.

*The Internet cannot be properly secured!* True, many changes and new methodologies can be introduced to improve existing security, but even the improved security will be able to be readily bypassed. This does not mean that we should not make the improvements that we can, but rather that we must be aware of our vulnerabilities and treat Internet transmissions as if they have been or will be compromised.

Individual users must assume everything they send can be [improperly] read by others. Since it is sometimes necessary to send information of a sensitive nature, such information should be

encrypted. Further, since it is trivial to *spoof* a message, i.e. send it under somebody else's name and e-mail address, messages should be viewed as suspect, and should be verified/authenticated if of importance. These functions can all be concurrently accommodated via use of a public key encryption scheme such as PGP (which is available on the Internet at many sites by anonymous FTP).

Other mechanisms can also be used to detect spoofed messages. Message sequence numbers can both indicate an incoming message is not expected, and further point to lost mail. Since most spoofed messages contain information within the header areas that can be used to point to the originating party, the entire message envelope, or at least certain predefined fields, should be captured, and archived for a reasonable period. These capabilities are in the control and audit areas of security, rather than the secrecy or access control areas usually getting the lion's share of attention, but are none the less important because of this. (To be effective in backtracking forged postings, capturing and archiving must be done across the entire Internet because of the frequent occurrence and large number of intermediate *hops* often involved in getting mail from its source to its destination.)

One-time passwords can be used to enhance the security of individual hosts (i.e. in regard to use by local users), and thereby make it less likely that restricted capabilities of these hosts will be used by unauthorized or improperly authorized personnel. This concept can be extended (in a software implementation, of course) to the communications between hosts. (This would reduce the likelihood of success of a rogue host.)

Many organizations (and of course individuals) receive mail primarily from a fixed number of locations. Since these locations can readily be converted to IP addresses, mail from other than those locations can be given more scrutiny than mail from *normal* locations. (This can be an *eyeball check* by individual recipients, or an automatic alert from an appropriately programmed server.)

Larger organizations tend to have many hosts. These hosts are frequently interconnected, and individually provide varying levels of security. Since the weakest one can be breached to allow access to all of the others, and since it is often in the difficult to impossible range to bring all hosts up to the proper level of security, *firewalls* (systems with the highest level of security; used as interfaces between the systems within an organization and the rest of the e-world) are a ready means of elevating the security of the weaker hosts.

Local user files are at risk due to breach of their host. Even with a firewall in place, user systems are vulnerable should the firewall be breached. (They are of course always vulnerable to inside attack, but that has nothing to do with the Internet.) Any and all critical or even sensitive or important files would ideally be maintained on a physically separate processor. Since that is most often not feasible, they should at least be kept in a separate partition.

If secrecy/privacy is important, the partition can be kept encrypted, or at least encrypted prior to establishing an Internet connection (and decrypted upon disconnected; this can obviously be time consuming, the amount of time depending on both the power of your processor and the volume of data to be protected, but some security products provide transparent encryption/decryption to

mitigate against the load placed by specific requests); if integrity and availability are the concerns, the partition can be quickly [software] write protected as part of establishing an Internet connection.

Implementation of all (or even any) of the above would increase security of various types and to varying degrees. They are all relatively quick (at least relative to the implementation of authentication servers with token passing), and will all improve the security posture. Some require cooperation of hosts on the Internet, and such cooperation cannot be enforced and may well not be voluntarily provided. Encryption would seem to offer the most effective "quick fix," but there may be some legal considerations that can deter some from this option. For the foreseeable future users are advised to explicitly verify any and all significant incoming e-mail. Unless you work with the concept that you can readily be fooled with a false message, you can easily fall victim to such easy abuse.

(Note: Certain normal service disruptions, such as those that might be caused by the iterative exchange of "I'm away" notices (person A sets his/her system to send an automatic response to all incoming messages while he/she is away on vacation, and person B does the same; A additionally sends a broadcast message to a select group, including B, advising of the vacation, and an automatic A-B-A-B-... exchange commences), should be treated by administrative host controls, not specific security measures.)

**Jon David** has been involved with system and network security for over 30 years, and has been a security consultant since 1967. He has been an Internet user for many years, and has personally experienced some of the breaches he will discuss.

As an expert in testing and with extensive experience in tiger team efforts, he naturally looks for ways to "break" systems and networks, and later helps his customers protect themselves against the problems he discovers.

He is a frequent author and lecturer on various aspects of security, holds leadership and advisory positions with many professional groups, and services a client list consisting of many of the largest organizations in the world from his home in New City, New York.

© Compulit, Inc. 1994. All rights reserved.

## Security on the Internet •••• A Viewpoint

by Frederick A. Kolbrener

Security of the Internet is a tough nut to crack and I do not refer to the difficulty in breaking in, but of the general solution of the security problem. There are several dimensions of the issue that have to be considered and a key consideration is **people**. If one reviews the internet's evolution, it is readily apparent that it sort of "just grew" like the character 'Topsy' in Harriet Beecher Stowe's book, "*Uncle Tom's Cabin*." The Internet started out in a period when there were few individuals with access to the net because there just was not a lot of equipment out there with which to access it. It was originally set up to foster the exchange of ideas between researchers. This factor alone discouraged the development of very tight controls.

Therefore, the security issue was never really a planned factor because few had access to programming code or security routines and for the most part, computer professionals with access respected the rights of others. They were probably too busy to be concerned with breaking into other's machines.

Additionally, the computer sites were pretty isolated at that time and few had the equipment to communicate from remote sites with mainframes. All this has changed with the proliferation of cheap computers into more and more homes and resultant growth of computer equipment access for the common person.

As mentioned earlier, the problem is people. People break into systems and people are the ones who don't assist in protecting the system by not following established guidelines. The question then becomes how to motivate people to assist in network security, and how to discourage intruders from trying to gain access.

We already have a system of access controls into the Internet. Each site with a gateway has a system of passwords and authentications to try to control access to the primary computer that is connected to the Internet. One has only to read a book such as *The Cookoo's Egg* to begin to appreciate the problem. In that book the persistence of hackers is outlined and their use of the same algorithm used to form encrypted system passwords on a dictionary in order to "backwards crack" user's passwords.

Using this system, they were highly successful in obtaining access to the system. If users had been more aware of the problem faced with hackers at that time, perhaps they might have been more careful in choosing passwords that were more difficult to guess. Another problem is that users have to be reminded from time to time not to write their password down. A chief reason that they do is that some passwords forced on them are just about unrememberable.

Thus the temptation for the access code to be written down somewhere. Clearly, there has to be a balance struck between the need for system security and making access for legitimate users more difficult. It must be remembered that users often feel they have a divine right to be on the system. We as managers and supervisors need for our personnel to have access to do their jobs. They must also be taught and appreciate the reasons for system security measures early in their careers. While that may be a simplistic approach, education will go far toward making systems more secure, but



will still not solve the problem as users are people and there will always be some who will not cooperate.

As we move into the future and more and more of the population becomes computer literate, the security problem will be both easier to control, and will present new challenges -- technical and otherwise.

Restriction is an approach, but is not the only answer to the problem. As long as there is a control system, there will always be someone who wants to see if they can break not it. It is human nature no matter how disciplined an individual is. The challenge is there and if the initial attempt to break in is successful, it likely that other's can too.

People will make our systems work, and people will find ways to break into them. It is our job to try to secure the willing cooperation of our personnel in order to make our systems and the Internet more secure. This basically equates to leadership. Without the willing cooperation of workers, few of our systems security actions can succeed.

**Frederick A. Kolbrener** is an Army officer commissioned in the Chemical Corps. He holds a Bachelors degree from Alfred University in Chemistry and a Master of Arts degree from Central Michigan University in Management and Supervision.

He entered service in 1966 and has held a succession of positions involved with training, research and development, and several years dealing with personnel management. He is a graduate of the US Army Command and General Staff College and both the Chemical Officer Basic and Advanced Courses. Currently he is assigned to a special task force in the Office of the Under Secretary of Defense (Personnel and Readiness) in the Information Resource Management Office.

Col Kolbrener is the immediate past chairman of the Pentagon PC User Group, which he headed for two years. He has an deep interest in security and has been associated with user groups helping others learn more about computers for over eight years.

© Compulit, Inc. 1994. All rights reserved.

## Security on the Internet •••• A Viewpoint

by A. Padgett Peterson

*Internet Security - A Deliberate Oxymoron:* In the late '60s and early 1970's when the Internet was designed, the avowed purpose was to provide a survivable network, one that could survive a nuclear war. In terms of the traditional Confidentiality-Integrity-Availability triangle this placed the design goal solidly in the "Availability" corner - no consideration was given to Confidentiality or Integrity, rather all effort was directed to making sure that *the mail would go through*.

In fact, the ability to have mail reply to a different location or person was a feature despite the fact that the same feature would make forgery of e-mail simple and difficult (at least from the application layer) to detect. And it is a feature since the ability allows a person to designate a single reply address no matter where in the world the message might be sent from (as this message is being created at a hotel room in San Francisco but replies will be sent from Orlando).

Similarly, while the use of the name instead of an IP address for the reply site raises the specter of subverted domain name servers and would seem to aid and abet the spoofing of e-mail also makes possible the concept of a diskless workstation with the IP address assigned for this session being drawn from a bank of available numbers and changing with each session.

Of course when the relevant RFCs were written, domain name servers were typically well maintained mainframes and not desktop SUN or PC platforms in a wiring closet somewhere (often on a box to keep it out of the water when the roof leaks).

In short, the Internet is totally lacking in the familiar *Orange Book* notions of security *deliberately*; it is just not in its charter. As a result, while a site can be assured that barring an unusual situation, a packet for a particular site on the net, anywhere in the world, will probably get there even though it may take several days to do so. Further, if by some unusual circumstance such as a node failure that removes it from the net, should the packet be undeliverable, notice will be sent to the identified reply node/ID.

All of this is very clearly spelled out in the relevant RFCs (requests for comment). In the case of SMTP (simple mail transfer protocol) this is RFC822 which governs the transport mechanism (RFC821 is for the mail itself). Of course RFC822 was last altered in 1981 and reflects a different time but is very effective in providing a mechanism for mail delivery.

To the user, this means that if *confidentiality and integrity* are required, it is necessary to accomplish this at the user's site and before the packet is ever sent. And it must be verified by the recipient at his/her site after the packet is received, typically with cryptography. As a consequence, the state of security in the Internet is just what it was designed to be: **none**.

Now this does not mean that use of the Internet cannot be done in a secure manner, just that it is the responsibility of the users to do so. Obviously firewalls are the first point of contact with the outside world and like the guard at the gate of a medieval walled town can provide an effective filter. However this technology at present is being used in a passive mode: firewalls today check

incoming packets for three things: source, destination, and type and on this basis decide whether to pass, refuse, log, or alarm (assuming that this has been implemented).

Recently, we have been seeing this ability taken to extremes with multiple machines acting as filters and gaps in the transmission lines, but still acting passively.

In the future, I expect to see firewalls begin to exploit the Internet actively, with a level 3 interrogation taking place back along the path of the packet to determine the actual source and not just trusting the information in the packet itself. For the very, very nervous further confirmation could take place with route tracing and verification made to expose spoofs.

Confidentiality and integrity could be accomplished through cryptography and could be done at two levels: encrypting all packets beneath the headers could be accomplished at the network level (3), while complete messages could be encrypted at the application level (7). Such an operation at the packet level could take place at or immediately behind the firewall, while application level encryption would take place at the workstation.

There is no reason why encryption at both levels could not take place. The first would be transparent to the users while the second might be transparent (if only communications with similar sites were permitted) or discretionary.

Note that if universal, this would also provide an additional level of distribution limitation by allowing communication only with trusted and prepared sites.

Now there are some functions and commercial providers that cannot be handled this way and may justify different methods. *Usenet* obviously cannot be encrypted unless a dedicated server is used since the provider has no capability. Of course NNTP (network news transfer protocol) is subject to the same limitations as SMTP (and the capacity for forged and spoofed addresses has grown so common that reply sites and signing are always viewed with suspicion).

Similarly, any common mechanism (gopher, mosaic) must use clear systems and as such must be treated as *untrusted* unless application layer mechanism are used.

In short, the Internet is operating exactly as it was designed with all of the emphasis being on the availability and reliability of the network itself. Any consideration for confidentiality or integrity is strictly the responsibility of the user.

**A. Padgett Peterson**, P.E is the System Integrity Manager for Martin-Marietta Information Group in Orlando, Florida.

Playing Tic-tac-toe on a Univac in 1957 was the start that led to learning FORTRAN II before the IEEE was the IEEE, installing and maintaining digital cryptographic devices in 1967, designing automated manufacturing facilities using digital computers, fiber optics, and infrared sensing in the early seventies, design of full-authority redundant digital flight controls for the F-16, communications topologies for the FAA, before returning to security and now cryptography to complete a career circle.

He was the recognized architect of the award-winning Martin-Marietta Computer Security Plan.

© Complit, Inc. 1994. All rights reserved.

## MODEL INFORMATION SECURITY PROGRAMS

**Chair** Richard W. Owen, Jr.  
Information Security Administrator  
Office of the Attorney General  
P.O. Box 12548  
Austin, Texas 78711-2548  
Phone: (512) 441-0717 x231      FAX (512) 444-1599  
E-Mail: Rich\_W.\_Owen@alias.austin.tx.us

Information Security Programs will be presented from the state, federal, private, and academic sectors. Highlighted will be their common and differing: sources of requirements; security organizational structure; security management process; and methods of security awareness.

**Academia** Stephen J. Green  
Associate Vice Chancellor for Information Services  
University of Houston  
Room 358D, McElhinney Bldg.  
Houston, Texas 77204-5883  
Phone: (713) 743-1461      FAX: (713) 743-1424  
E-Mail: SGreen@UH.EDU

Security has only recently been a topic of growing interest within the University of Houston campuses. This growing interest has not occurred because of security incidents. Instead, this emphasis is caused as a result of trying to comply with state mandates and because of my direct involvement keeping the issues active and the search for solutions, a management focus. Universities operate in a considerably different environment from other public institutions or commercial institutions and view their missions apart from these institutions. Management by consensus and freedom of access to information are two key differences that directly influence the establishment of security policies, perception of risk, and application of security procedures and techniques.

The University of Houston, like most other universities, address their security needs by dividing the problem into separate administrative or academic environments. Administrative environments are handled by traditional approaches with rigorous regard to the protection and integrity of information. Academic environments however, have no consistent approach. We are now beginning to address the issues that account for this variability in approaches to satisfy academic concerns.

**Commercial** Genevieve M. Burns, President, ISSA  
Manager, Data Security  
Monsanto Company  
800 N. Lindbergh, G2EE  
St. Louis, MO 63167  
Phone: (314) 694-7661

FAX: (314) 694-7625

Monsanto Company has received recognition for its proactive security programs for several years. Developed under the leadership of Genevieve Burns, the concepts of these programs have been shared with, and incorporated within, both the private and public sectors. At the request of many organizations, Mrs. Burns contracted with a distributor of quality video programs to allow further dissemination of Monsanto's formal security programs. Most of the branches of the armed services have purchased these videos to supplement their own programs. Mrs. Burns' first endeavor in the use of video resulted in three Emmy nominations and two 1989 Emmy awards from the St. Louis Chapter of the National Academy of Television Arts & Sciences (Training & Writing), the 1989 U.S. Industrial Film Festival's Creative Excellence Award - Training and the 1990 Annual Telly Awards' Finalist. Since that first effort, Monsanto has received other prestigious awards for its subsequent security awareness videos. In addition to the formal programs undertaken by Mrs. Burns, an ongoing informal awareness and education program continues to provide an up-to-date foundation. Success of the total program efforts are measured by Mrs. Burns in several ways. Internal Audit reports identify the areas of concern and the need for focused education. Comparison of audit reports over time identifies improvement or the need for refocused attention to a security issue. Increased requests, for clarification of policy and consulting early in the development cycle, are also measurement opportunities for the value of the program and its reach. Monsanto, a Fortune 100 company with locations worldwide, endeavors to attain a consistent level of security awareness and proactive participation by its more than 30,000 employees plus contractors. The programs designed by Mrs. Burns have provided a mechanism to move the company in that direction.

**Federal** Philip L. Sibert  
Senior Computer Specialist  
Information Technology Security Division  
U.S. Department of Energy, HR-421  
Washington, D.C. 20585  
Phone: (301) 903-4880

FAX: (301) 903-4101

The specific aspects of the DOE security program will be discussed at the conference.

**State**            Jan W. Wright  
Information Resources Management Consultant  
Information Resources Commission  
725 South Calhoun Street  
112 Bloxham Bldg.  
Tallahassee, FL. 32399-0950  
Phone: (904) 488-8036                      FAX: (904) 922-5929  
E-Mail: WRIGHTJA@FREENET.TLH.FL.US

The State of Florida, through statute and rules, has established a model of decentralized implementation and centralized oversight and compliance monitoring of information resource security. Department heads are responsible for assuring the security of the information resources within their departments. Minimum requirements for state department managers include: the appointment of an Information Security Manager to administer the department's security program; comprehensive risk analysis; written internal policies; cost effective risk management; internal EDP audits and evaluations; addressing security issues when developing procurement documents; and annual information resource security certification. The responsibility for the oversight and monitoring is assigned to the Information Resources Commission (IRC) composed of the Governor and elected members of the Cabinet. Security related functions performed by the IRC include: facilitating the work groups for rule amendment of security policies and guidelines; coordinating security training for multiple agencies; acquisition of a statewide contract for risk analysis and other tools; development and maintenance of security guidelines; statewide security incident and breach trend analysis; evaluation of security requirements in solicitations for information resources; and development and administration of the certification of compliance to statewide security standards.

**Summary:** In general the driving force behind security remains the need to comply with rules or mandates whether from internal or external sources. The idea of the real threat only arises briefly as a major incident hits the papers (Columbus Day Virus, Internet Worm, World Trade Center Bombing, etc.). The Security Manager is typically a staff function that defines and monitors the program, whereas the responsibility of security remains with the line management. The concept of risk management is catching on, but in general the typical line manager is looking for the specific requirements that must be met. Once confronted with the requirements the line managers begin to warm up to the concept of risk management. More and more the concepts and requirements of security are beginning to spread across the entire life cycle of a system. This involves the training of not only programmers and systems managers but also procurement personnel. General user awareness is still seen as the single most cost effective measure that can be taken in the state, federal, commercial and academic sectors to reduce the risk to our information assets.

# 17th National Computer Security Conference

## *Interdisciplinary Perspectives on InfoSec*

# Bringing the Humanities into Cyberspace

**Michel E. Kabay**

**Director of Education, National Computer Security Association, Carlisle, PA  
President, JINBU Corporation, Montreal, QC**

*InfoSec depends on much more than technology. Perspectives from the humanities enrich our capacity to reach our colleagues, our clients, our students--and perhaps even our enemies--to increase the security of information systems.*

This panel on *Interdisciplinary Perspectives on InfoSec* resulted from discussions at the 16th National Computer Security Conference in September 1993. A group of interested security specialists met with the encouragement of Dennis Gilbert of the National Institute of Standards and Technology to consider how non-technological views of InfoSec issues could stimulate thought and discussion (in that order) among participants of the next, 17th, NCSC in October 1994.

Our panelists will begin with a brief presentation of the most important points in their papers, which are in the *Proceedings*. For this monumental task they have each been allotted ten minutes.

The first paper is an anthropological perspective on the culture of cyberspace. The main argument is that criminal and psychopathic elements must not be the ones to determine the norms of human interaction in cyberspace.

The second paper presents a legal philosopher's views on how to answer the question, "Who's to say what's right or wrong?"

The third paper discusses a psychologist's recommendations on how to improve compliance with information security rules in an organization.

The fourth paper shows that military science has much to offer to information security specialists.

Following the presentations, the panelists will entertain questions from the audience and, in true academic style, from each other.

# 17th National Computer Security Conference

## *Interdisciplinary Perspectives on InfoSec*

# **An Anthropological View: Totem and Taboo in Cyberspace**

**Michel E. Kabay  
Director of Education  
National Computer Security Association**

*Cyberspace, the realm of computer networks, voice mail and long-distance telephone calls, is increasingly important in our lives. Unfortunately, morally immature phreaks, cyberpunks and criminal hackers are spoiling it for everyone. Security professionals must speak out in the wider community and change the moral universe to include cyberspace.*

We are seeing today a period of exploration and development in a new realm reminiscent of the colonization of North America by Europeans. As in the American experience of the frontier, there are colonists and Amerinds, soldiers and outlaws, priests and thieves. The frontier is cyberspace: that immaterial world where we have phone conversations; where credit card information travels while we wait for approval of a purchase; where our medical records and sometimes our credit records paint a picture of our pains.

For an increasing number of us, cyberspace is also the place we meet new friends and keep in touch with old ones, learn more about our hobbies and our professions, and work for social and environmental change. Electronic bulletin board systems have mushroomed throughout the world, ranging from country-clubs like CompuServe and Prodigy through the grungy cafés of the hacker underground and on into the pullulating bazaar of the great Internet, where philosophers rub shoulders with dropouts and where age, gender and race are only as visible as you want them to be.

Unfortunately, the spectacular growth of cyberspace has not been accompanied by rules for civilized behavior. Cyberspace at the end of the twentieth century resembles the frontier at the beginning of the eighteenth: bullies and criminals swagger electronically through the commons, stealing what they want, breaking what they don't, and interfering with decent people's activities. Far from helping to set standards of mutual respect, some government agencies have been acting like totalitarians rather than democrats. For all these reasons, we citizens of cyberspace must evolve guidelines for civilizing our new frontier.



## THE GRANDDADDY OF ALL NETWORKS

The Internet is possibly the most complex and rapidly-growing construct humanity has ever created. The cathedrals of medieval Europe pale in comparison with the electronic edifice that is the Internet. The Internet grew out of ARPANET, funded in the late 1960s by the Defense Advanced Research Projects Agency (DARPA). This experimental network linked a few universities and research laboratories electronically. ARPANET begat the Internet when the National Science Foundation (NSF) decided to make internetworking possible for many more universities than the first-tier institutions that had been in from the beginning. ARPANET itself disappeared as a formal entity in 1990.

From the very beginning, the group inventing ARPANET had a refreshingly non-bureaucratic attitude towards their work. For example, meetings of the network coordinators at Bolt Beranek and Newman in 1968 had two ground rules: Anyone could say anything; and nothing was official. The current management style of the Internet reflects the belief in unhindered engineering excellence as the best way to find solid solutions for technical problems. This tradition of frank criticism and unfettered creativity has been misinterpreted by some newcomers to the Internet as an excuse for frank rudeness and unfettered criminality.

The Internet today functions like a combined mail route, supermarket bulletin board, and library. Electronic mail (email) is much faster than paper mail ('snail mail' as it's derisively termed on the Net). Electronic Bulletin Board Systems (BBSs), Special Interest Groups (SIGs) or Forums allow us to post electronic notes asking for advice, help, friendship, and all the other dimensions of social interactions. There are electronic equivalents of newspapers ('newsgroups') and magazines ('moderated newsgroup digests') dealing with interests from the sublime to the prurient. Scientists from distant institutions collaborate fruitfully on research without concern for geographical barriers. Textbooks and novels are posted on 'the Net' (the affectionate term for the entire Internet and all the networks connected to it in any way) for enjoyment and comment, sometimes coming out better for the free flow of criticism and advice. So many repositories of information are on the Net that doing research without using its resources is unthinkable for a growing number of enthusiasts.

Because the Net has grown by cooperation and consensus rather than legislation and government regulation, there is no way to know exactly how many people use how many computers on this fishnet of the mind. Generally-accepted estimates are that there are about 13 million regular users linked via roughly 1.3 million computers ('hosts'). Registration of hosts has exploded since the Internet community agreed to allow commercial firms to join.

According to a document, (named, in typical style, '/infosource/internet\_info\_for\_everybody/how-big-is-the-internet/domain-survey-jan93') from the Network Information Systems Center at SRI International in Palo Alto, California, there was an 80.6% increase in the number of hosts in 1992. Of the 1,313,000 hosts, 410,940 or about a third were in the educational (.edu) domain. Some 347,486, or about a quarter, were in the commercial (.com) domain. The annual growth rate in 1992 for .edu was 69%, but the growth in .com was 92%. The advent of users from .com has elicited howls of protest from some quarters on the Internet; however, commercial users may bring new standards of behaviour to the Net.

The total rate of information transfer in the Internet is unknown; however, it appears to be Terabytes (Tb) per day. This number, 1,125,899,906,842,624 bytes, cannot reasonably be apprehended. A byte corresponds approximately to a character of text. This article has about 50 thousand bytes. A 1,000 page textbook might have a few million bytes (Mb) of text; that there are a million Mb in a Tb. Even more astounding, the total traffic is growing by about 25% every month a 14-fold increase in a year.

## **A MORAL VACUUM**

Cyberspace is growing fast, and the values which inform our lives in physical communities have not yet found their way into cyberspace. Just as in the physical world, unethical, immoral, and illegal behavior threatens the agreements that allow people to live and work together in peace.

Many users of cyberspace are well-behaved. They are sensitive to nuance, capable of expressive and articulate prose, careful not to hurt feelings, and responsible in spreading verified information and not rumor.

However, we also find the cyberspace equivalents of slum lords, drug pushers, boors and bully-boys. There are people running private BBSs that cater to thieves, drug users, Nazis, and paedophiles. People who might never think of insulting a stranger to her face write nasty and juvenile notes.

Different service providers adopt different stances about the content of communications on their network. For example, the commercial value-added networks (VANs) Prodigy and CompuServe are among the most custodial in their attitude towards the message base. These services employ system operators (Sysops), volunteers who manage specific sections by monitoring traffic, responding to questions and cooling tempers. Some Sysops on commercial services and private BBSs explicitly censor unacceptable or irrelevant contributions, usually to howls of protest and hyperbolic invective from the censored authors. These howls are then themselves removed from view, prompting yet more appeals to First Amendment rights. As a Sysop myself, I have had to explain that the Forum or SIG is not public and that the Sysop has a responsibility to maintain a professional tone and to prevent abuses such as posting text files or software without permission of the copyright holders. Some moderated newsgroups on the Internet also have strict enforcement. For example, the RISKS Forum Digest is tightly controlled by its moderator, who personally determines whether any given message reaches the members.

At the other extreme, there are networks, Forums, SIGs and BBSs where anarchy reigns. Contributions are unfiltered, unfettered, frequently ungrammatical, and sometimes illegal. Some boards and groups pander to unusual sexual orientations, with hundreds of pornographic text and picture files available online. Others specialize in stolen or malicious software, and instructions on picking locks, stealing services and building bombs.

Such rude, unethical, immoral and illegal behavior puts the entire Net at risk from self-appointed as well as legally-delegated guardians of public morality and corporate interests. I fear that politicians looking for an easy target may impose restrictions on the content of electronic communications. Legislative interference would likely include requirements for paperwork and would render the volunteer job of Sysop impossibly demanding. The ultra-religious forces of intolerance could also seize the opportunity to attack a new den of iniquity, whipping up their doctrinaire supporters to acts of harassment, sabotage and even physical violence.

## **CRIMES IN CYBERSPACE**

What kinds of problems are there? The issues boil down to theft of services and software, invasion of privacy, outright damage, and the threat of terrorism.

In a landmark study, John Haugh and his colleagues at Telecommunications Advisors Inc. in Seattle, WA, have recently built up a staggering picture of the extent of toll fraud (using someone else's telephone services illegally) and telabuse (using one's employer's phone service without authorization). Haugh et al. consider that the total losses to the economy from toll fraud and abuse of corporate telephone systems are in the \$2-8 billion range per year. Toll fraud rings using stolen telephone credit card numbers have been operating virtually unchecked in all major urban centres. The cycle often begins with 'shoulder surfing,' in which someone watches as a victim punches their access codes into a public telephone in a public place. Organized gangs of youths have been caught in New York's Grand Central Station and La Guardia Airport. Within days, the credit card can be used for hundreds of long-distance phone calls generating thousands of dollars of expense for the victim. Although the phone companies generally do not insist on repayment, these calls do cost the U.S. economy something: inter-carrier charges must be paid to the national telephone services of the countries of destination. Most of the stolen calls go to South American drug havens, certain Caribbean islands, and to the Indian subcontinent.

Some criminals use control codes or special tone generators ('Blue Boxes' and others) to steal telephone services; others dial into corporate phone switches using public 800 numbers, then use outbound lines for long-distance calls. Some victims have had more than a quarter million dollars of calls placed in a single weekend. The invoices from the phone companies sometimes fill several crates with thousands of call details all fraudulent.

Voice mail subversion is another tactic used by 'phone phreaks.' Voice mail systems allow callers to leave messages for specific employees. Unless supervisors pay close attention to usage statistics, a voice-mail system can become host to dozens of unauthorized accounts for strangers, thus putting an unexpected load on phone lines and consuming storage space on the voice-mail computers.

By far the greatest problem caused by criminal hackers is the loss of confidence in system integrity. Take for example a computer system used for production of mission-critical information. There can be no tolerance for error. Programs written for such a system are subjected to strict quality-assurance procedures; every program must pass extensive testing. When the operating system (the software that coordinates communication among programs and regulates access to

different kinds of computer resources) has to be changed ('updated'), many system managers run acceptance tests over an entire weekend to ensure that there will be no glitches once production starts up again. It is considered normal to forbid programmers to modify production databases; and careful audit trails are usually kept to track exactly which specific user altered what specific records at any give time in the files.

Discovering unauthorized use causes chaos in the production shop. A hospital pharmacy discovers the transposition of two digits in its pharmacy database, leading to potentially fatal errors in drug administration for patients. A faulty program in a telephone switching center disrupts phone service over an entire geographical region. Since there is no way of knowing what intruders have done (criminal hackers do not leave neat system alteration notices), the only reasonable response to intrusion is to audit the entire production system. That means time-consuming, mind-numbing labor to run verification programs on all the data, careful comparison of every program with a known-good copy to see if it has been altered illegally, and hours of overtime for quality-assurance and system management personnel.

Credit records are relatively easy for criminal hackers to find, although it's much harder to modify them. Patient files are supposed to be protected yet many hospitals have rudimentary safeguards that do not deter determined hackers. On another front, government employees have disclosed confidential information such as tax files and criminal records. In some cases the theft of data was for money (a few dollars for reports to unethical private investigators) and in others merely for fun (printing tax files of the rich and famous to impress one's friends). These are the electronic equivalent of breaking and entry in the physical world.

Another area of concern is eavesdropping. Industrial espionage is growing as competition heats up, especially across international borders. In the U.S., Symantec and Borland have been at loggerheads over the alleged theft of confidential information by an executive who defected from one company to the other. In Europe, General Motors and Volkswagen have been denouncing each other over allegations of a similar theft by a high-placed official.

The last decade has witnessed a troubling proliferation of malicious software such as viruses, worms, Trojan Horses, and logic bombs. A computer virus is a program which adds itself to executable code (programs and boot sectors on diskettes and disks). When the infected code is loaded into main memory (usually on a microcomputer such as an IBM-compatible PC or an Apple Macintosh), the virus can both reproduce by infecting other programs and also deliver its payload. Virus payloads range from the merely annoying (e.g., the STONED viruses usually put a plea for the legalization of marijuana on the screen) through the irritating (the Autumn viruses make the letters on one's screen drop to the bottom like so many leaves) to the destructive (viruses written by Bulgaria's Dark Avenger tend to cause random changes in data and programs anywhere on disk, leading to unpredictable and pernicious damage).

Depending on how one judges variations to be different, there are from two to four thousand recognizable viruses circulating in cyberspace. About 30 virus types account for almost all the virus infections that ordinary users are likely to encounter. STONED and JERUSALEM alone

account for about five sixths of all infections. Unfortunately, criminals have put virus-writing kits into the underground networks, so now even incompetent programmers can create mutating ('polymorphic') viruses that employ sophisticated techniques ('stealth') to avoid detection.

Recent industry surveys suggest that the risk of virus infection of microcomputers (PCs and Macintosh) is a few percent per year per computer. There are currently no viruses found on user systems which infect large (mainframe) computers. There are only a few which affect UNIX operating systems or local area network operating systems.

The most widespread computer crime is software theft. Estimated rates of theft range from about 35-40% in the USA to 99% stolen in Thailand. Robert Holleyman, president of the Business Software Alliance, reports that more than 80% of the computer programmes in China are pirated, making it one of the worst stealers of software in Asia and costing the worldwide industry US\$500 million a year. Sometimes stolen programs are available in Asia before they are released legally.

Apparently China is now concerned about copyright violations in part because its own software industry is being harmed. Yang Tianxin, chief of the computer division of the ministry of electronic industry, claims that China is just beginning to attack this problem using criminal penalties and education.

Western nations also need to integrate respect for intellectual property into normal morality. Too many managers, teachers, technicians and just plain users are stealing software by making unauthorized copies of copyrighted programs. It's no wonder children trade pirated copies of computer games with no awareness of doing wrong.

Most computer crimes are not perpetrated by criminal hackers. Recent surveys suggest that about 85% of all computer-related crimes are committed by personnel authorized to use the computers they abused. The probability of being attacked by outsiders is only about 1 or 2% per system per year.

Within organizations, programmers occasionally write malicious software. 'Trojan Horses' are programs which have secret functions (e.g., keeping a record of passwords) along with their ostensible purposes. The AIDS Information Diskette which circulated worldwide a few years ago was a Trojan which pretended to offer information about the dread disease, but then scrambled the user's disk directory and tried to extort payment for a recovery utility. Trap Doors involve programming secret entry points for later unauthorized use; the password 'Joshua' was part of a trap door left by the creator of a top-secret government system in the movie 'War Games.'

Logic bombs are sections of program which check for particular conditions and then wreak havoc in the system. In the film, 'Single White Female,' a programmer leaves a logic bomb in her code to wipe out her creepy client's entire fashion database because he hasn't paid her full fee. In November 1993, a Manhattan programmer and his technician were accused of planting a logic bomb in a client's software when he refused to pay the full cost of the package. Some programmers insert logic bombs in their code as a matter of course.

The cyberspace equivalent of vandalism occurs when intruders or disgruntled employees deliberately damage or destroy information. The 414 Gang (so named from the area code of their Milwaukee homes) damaged clinical research data in their forays through the networks in the early 1980s. Two teenagers from Staten Island caused \$2.1 million of damage to the voice-mail system of a publisher by erasing orders for advertising and leaving obscene messages which offended clients. When they were finally tracked down and arrested, the 14- and 17-year olds admitted that their depredations were revenge for having failed to receive a promised poster from the publisher.

In a report at the 16th National Computer Security Conference in Baltimore, MD in September 1993, an investigator whose team tracks the underground BBSs revealed that detailed instructions for weapons of terrorism are freely available in cyberspace. The published recipes for home-made bombs were evaluated by professionals from military special forces and were pronounced to be workable, albeit dangerous for amateurs.

Some administrators at universities with Internet connections have been put under opposing pressures because of the availability of graphic pornography graphics. There have been threats of lawsuits for allowing such materials to enter the campus systems and threats of lawsuits for forbidding such materials to enter the campus systems. Some paedophile BBS operators have been found to use their systems to entice youngsters into meetings by offering illicit files and cheap stolen hardware and software.

It is easy to create false identities through electronic mail. Some denizens of cyberspace use one or more pseudonyms ('handles'). A major hacker conference was announced on the Internet by 'drunkfux@cypher.com' with no other identification made available. Some 'cypherpunks' insist that there should be no interference with this practise, arguing that any attempt to enforce identification would be a gross infringement of their privacy.

Advocates of anonymous and pseudonymous postings defend their preference by pointing to the long-standing acceptance of pseudonyms in print. I wonder if they would defend wearing face masks during face-to-face conversations?

## WHO ARE THE TECHNOPATHS?

Because of the shadowy nature of the computer underground, where real names are few and role-playing is the norm, it is hard to find reliable statistics about the demographics of what famed Bulgarian anti-virus researcher Vesselin Bontchev (now at the University of Hamburg) has called 'technopaths.' The consensus in the computer underground is that they are predominantly teenaged boys and young men. These maladapted, undersocialized, emotionally-underdeveloped individuals adopt noms-de-guerre ('handles') like Phiber Optik, Acid Phreak, Dark Avenger, The Leftist, The Prophet, The Urvile, and Necron 99. They form electronic gangs with ludicrous names like Masters of Deception and Legion of Doom. Much of this is adolescent posturing; as one member of the latter group commented, 'We couldn't very well call ourselves the Legion of Flower-Pickers.'

Several popular books have provided insights into the psychology of criminal hackers. One of the best is by Katie Hafner and John Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. (Touchstone Books, Simon & Schuster (New York, 1991). ISBN 0-671-77879-X. 368 pp. Index).

## ARE HACKERS CRAZY?

The standard reference work on psychiatric disorders (DSM III; APA, 1980) defines the Narcissistic Personality Disorder in these terms:

'The essential feature is a Personality Disorder... in which there are a grandiose sense of self-importance or uniqueness; preoccupation with fantasies of unlimited success; exhibitionistic need for constant attention and admiration; characteristic responses to threats to self-esteem; and characteristic disturbances in interpersonal relationships, such as feelings of entitlement, interpersonal exploitativeness, relationships that alternate between the extremes of overidealization and devaluation, and lack of empathy....

...In response to criticism, defeat or disappointment, there is either a cool indifference or marked feelings of rage, inferiority, shame, humiliation, or emptiness.... Entitlement, the expectation of special favors without assuming reciprocal responsibilities, is usually present. For example, surprise and anger are felt because others will not do what is wanted; more is expected from people than is reasonable.

Sound like criminal hackers?

During the 1990 December holiday season, some 25 hackers gathered for their 'Christmas Con' in a hotel near Houston airport. After consuming too many beers and pulling fire alarms, the group was evicted from the hotel. This sort of behavior is associated with the Antisocial Personality Disorder, whose '...essential feature is... a history of continuous and chronic antisocial behavior in which the rights of others are violated....' (DSM III; APA, 1980). In 1993, some of the 200 attendees at HoHoCon in Austin pulled fire alarms after a night of drunken carousing and viewing pornographic movies.

In the Austin HoHoCon in December 1993, criminal hackers discussed cracking cellular phones, shared information on new techniques for stealing long-distance services, and boasted of posting anarchist files on BBSs. When I challenged "Deth Vegetable" for having posted instructions on how to make bombs out of household cleaning supplies, his friends glared angrily at me and hissed, "It wasn't illegal. He had a right to post whatever he wanted." Deth Vegetable rejected responsibility for the consequences of his actions; although he regretted that two children had recently destroyed their hands in an explosion while following the details of his file, he sneered that perhaps it was evolution in action. He admitted that maybe it seemed wrong, but he didn't know why. "And anyway," he shrugged, "who's to say if it's right or wrong?" At that point, I seized him by the shirt and gently drew him to nose distance. "Who's to say??" I asked. "You are. I am. We are."

The culture of criminal hackers seems to glorify behavior which would be classified as sociopathic or frankly psychotic. These behaviors must not become normative.

## **TECHNICAL SOLUTIONS**

Technical approaches to behavioral problems have a limited scope. Some attempts to protect cyberspace concentrate on making it harder to do harm. For example, system managers are supposed to pay strict attention to how people can enter their systems and networks; this area of concern is known as access control. Some of the more successful methods currently in use include one-time password generators. Such hand-held units, about the size of a credit card, generate random-looking codes which can be used for logging into computer systems and networks, but which are valid for only one minute.

Modems which garble transmissions make it impossible to crack systems using brute-force methods. Instead of trying hundreds of passwords without hindrance, criminal hackers would be forced to turn to the much slower techniques of lying and spying (social engineering). Even if criminal hackers were to enter a secure system, encrypted data would severely interfere with their ability to cause trouble. Unfortunately, encryption is still not in general use in the business community.

Finally, if more victims of computer crime were to report what happened, the computer security industry could develop the same kind of shared expertise as the insurance industry's actuaries. It would help immeasurably to have a library of documented case studies of computer crime available for study by computer science students, sociologists, criminologists and security experts. All organizations hit by computer criminals are encouraged to report what happened to the Computer Emergency Response Team Coordination Center (CERT-CC) at Carnegie Mellon University in Pittsburgh, PA.

## **HUMAN SOLUTIONS**

Technical solutions appeal to the rational propensities of security specialists. But since people are at the core of computer crime, psychosocial factors must be at the core of efforts to contain it.

Security is the tooth-flossing of the computer world: it's boring and repetitive, slightly distasteful, and has no obvious, immediate benefits. Even worse, the better the implementation, the less frequently problems arise. Security cannot be achieved by superficial changes of style. Just as the Total Quality Management movement emphasizes that the concern for quality must pervade all aspects of working culture, information security must become part of the corporate culture.



Security professionals have to deal with the psychological difficulties of trying to change long-rooted patterns of social behavior. For example, a typical security policy states that no one may allow another employee to 'piggyback' into a secure area; that is, each person entering through a secured door must use their own access-control device. However, politeness dictates the opposite: we hold a door open and invite our friends and colleagues to enter before we do. To learn new habits, it is useful to address the conflict directly: acknowledging that the policy will be uncomfortable at first is a good step to making it less uncomfortable. For example, employees should participate in role-playing exercises. First, they can practice refusing access to colleagues who accept the policies graciously, then move on to arguments with less-friendly colleagues. Finally they can learn to deal with confrontations with colleagues who pretend to be higher-rank and hostile. Managers should practise being refused access to secured areas.

In grade schools, high schools, colleges and universities, students are introduced early to computer systems and expected to master and use computers in their studies. All too often, however, ethical issues about computer usage are neglected. Some instructors blatantly steal copyrighted software or tell their young charges to do so ('Here, copy this diskette and return the original'). Other children entrain their younger contemporaries into the glitzy world of computer virus exchanges and virus writing. There's always the allure of computerized pornography on local bulletin boards an allure enhanced by the lack of knowledge of parents and teachers about the very existence of such sources.

Lonnie Moore is computer security manager at the Lawrence Livermore National Laboratory. With the help of Gale Warshawsky, an employee who happens to be an experienced puppeteer, Moore has created an appealing and entertaining security awareness video for children in elementary schools. The heroes are Chip, the friendly computer, and Gooseberry, the hapless untrained user. The villain is Dirty Dan, the nasty hacker. Dan drops crumbs into Chip's keyboard, destroys files and makes Chip cry, then makes Chip dizzy by feeding him a virus from another computer. Moore explains, 'What we're trying to do is learn from the mistakes that have been made. They understand good guys and bad guys. We also teach them to try to have some feeling for the others involved.'

A major telephone company in the U.S. has created a video for middle-school children which addresses telephone fraud in an entertaining and informative way.

The **Computer Ethics Institute** in Washington, DC, has published the *Ten Commandments of Computer Ethics*:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not use other people's intellectual output [without due acknowledgement].

9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that demonstrate consideration and respect for your fellow humans.

Efforts such as these are the beginning of a response to lawlessness in cyberspace. Operating at the human level, they are ultimately as important as technical solutions to computer crime.

## **THE MORAL UNIVERSE OF COMPUTER USERS**

It takes time to integrate morality into our technological universe. Twenty years ago, many drivers felt that driving under the influence of alcohol was adventurous. Today most people feel that it's stupid and irresponsible. Smoking in public is becoming rare. Many of us in northern cities have witnessed exiled smokers huddled together in the cold outside buildings where they once lit up with impunity.

Similarly, we need a consensus on good behavior in cyberspace.

Criminal hackers who break into computer systems and roam through users' private files should be viewed as Peeping Toms. Criminals using computers to extort money or steal services should be recognized as thieves. Those who destroy records, leave logic bombs, and write viruses should be viewed as vandals. Hackers who smear obscenities in source code should be seen as twisted personalities in need of punishment and therapy. Government agencies proposing to interfere in electronic communications should be subject to scrutiny and intense lobbying.

Beyond such prohibitions and inhibitions of taboos, cyberspace needs the electronic equivalent of Emily Post. We need to discuss the immorality of virus writing, the ethical implications of logic bombs, and the criminality of electronic trespassing. We should teach children how to be good citizens of cyberspace and not just in schools. We should sit down with computer-using youngsters and follow them through their adventures in cyberspace. Parents should ask their teenaged whiz-kids about hacking, viruses, software theft and telephone fraud. We must bring the perspective and guidance of adult generations to bear on a world that is evolving faster than most of us can imagine.

Participants in the **National Computer Security Conferences** should be at the forefront of efforts to reach out into the wider community. If experts in security cannot express their values, who will?

The adolescent confraternity of criminal hackers and virus writers have already begun developing totems: the personae of Dark Avenger and Acid Phreak loom over youngsters much as Robin Hood once did for another generation.

What we need now are taboos to match the totems.

# 17th National Computer Security Conference

## *Interdisciplinary Perspectives on InfoSec*

# Philosophy of Law and InfoSec: Justifying Morality in Cyberspace

Prof. Virginia Black

Department of Philosophy, Pace University, Pleasantville, New York, NY

*How shall we justify prohibiting breaches of computer security? Why are such breaches morally wrong, and what can we justify doing about them?*

My remarks are divided into six parts:

- I. Why is this a moral question in the first place?
- II. What kinds of reasons are appropriately given for questions that are relevant to the problem of computer security breaches?
- III. Some meta-ethical factors to consider before continuing our enquiry
- IV. Why should I be moral?
- V. What can we justify doing about security breaches?
- VI. Probable motives for security breachers.

### **I. Why is this a moral question in the first place?**

We can answer on at least four levels.

- A. We can answer by defining the term "moral" and what the term generally involves.
- B. We can answer by indicating the kinds of reasons that are appropriately given for certain questions. (We will return to this response in II, below.)
- C. We can answer by reminding ourselves that morality is a social, rational, and practical discipline, and the issue of breaching security has elements of all three of these.
- D. We can answer by indicating that it is a moral question because it is not another kind of question, nevertheless it is one whose features may overlap with legal and other questions (e.g., prudential, aesthetic).

But it is not a legal question because--

- \* Moral reasons are logically anterior to legal reasons;
- \* In order to be legal, an action or rule has to be shown to be either not immoral or not imprudent (un-reasonable, impractical); hence morality "comes first." We use moral arguments to inform the law.
- \* The illegality of this issue has already been settled; and we already know in general what to do about legal wrongs (we apply sanctions, etc.). Legal wrongs are less problematic because their authority status is more certain and often their definitions and limits are made clear.

Let us return to the most interesting and useful of the above levels on which we can examine the question, namely--

## **II. What kinds of reasons are appropriately given for arguing against breaches of computer security?**

The substance and content of these reasons are what make the problem a moral one. I shall suggest six types of morally relevant reasons, all of them not only appropriate for our enquiry about InfoSec but also very fundamental to many moral questions in general. Stating these moral reasons as imperatives, they are--

1. Do not needlessly commit serious harm to individuals and institutions (harm implies that human sentience is very relevant to the moral life);
2. Conform to your contracts and other kinds of reciprocal understandings and agreements;
3. Do not infringe people's rights (e.g., property rights);
4. Do not diminish people's personal freedom (i.e., the capacity to reason that is tied in with the discovery of opportunities and self-realization);
5. Do not be unfair or unjust;
6. Do not act so as to diminish the common good: the good of society at large.

Each of these moral considerations can be illustrated by concrete cases of InfoSec breaches which the audience can cite. We take up briefly at the end (sec. VI) some typical motives that can cause, say, hackers to breach security or to spin viruses into programs. When these motives are uncovered, it is easier to propose methods for their remediation.

## **III. Some meta-ethical factors to consider before continuing our enquiry**

- \* The syllogistic nature of justification: moral and prudential (to be illustrated below);
- \* The "incompleteness" of moral justification: it is not an exact science because life situations, unlike controlled lab research, have multiple variables, often hidden, at play;
- \* Taking the moral point of view: conceptual clarity, impartiality, universalizability, being rational and informed.

We can attack breaches of InfoSec on many levels at once. From a philosophical perspective, we apply the substantive content of the basic moral principles selected as relevant to our problem. We then apply these principles to the problem at hand. We can also include in our arguments facts drawn from the particular situation we are analyzing.

As an example of this syllogistic, deductive method of moral justification, and taking the first substantive principle we stated above:

1. (first premise) Do not needlessly commit serious harm to individuals and institutions. (This is our pertinent general rule standing as the first premise in the justification syllogism)
2. (2nd premise) Breaching the security of this computer or releasing a virus into this system seriously harms this institution. (This is our factual premise in the justification syllogism)
3. Conclusion: I ought not to breach the security of this institution or release a virus into this system (etc.).

Showing that certain crucial or basic moral reasons (moral rules or principles applied to a situation) override the desires of the security hacker by avoiding a grave moral wrong to some party, defines what it means to provide a moral justification.

As we can see, the moral reason (principle) given in the syllogism above easily overrides the hacker's self-interested reasons. *For the moral point of view, embracing a fundamental consideration always overrides the self-interested, prudential point of view where the two conflict.*

Moral reasons less easily but nonetheless do also override what I will call the hacker's negative reasons; e.g.,

- \* Why should I care about the common good?
- \* I didn't make a contract.
- \* I have a good defense (excuse) for what I'm doing.
- \* I have a right to know--I'm entitled to know--what I can find out.
- \* Information is public anyway: Information Wants to be Free!

That the moral case can be confirmed, however, does not mean that the moral case will always be accepted. We draw here the distinction between proof and acceptance of a proof.

Here it is relevant to mention "role morality," the moral rules that generally hold between persons in some sort of understood relationship: parent/child; student/teacher; employer/employee, etc. Where security breaches are committed by well-meaning and otherwise loyal and trustworthy persons within an organization, role morality may be the best approach: that is, getting breachers to renew their understanding of what it means to be loyal to the organization, what their contract as an employee entails, and how the organization (their organization, and hence part of themselves) is seriously hurt, undermined, or crippled by such breaches.

But there is something else, something that, in the end, the wrongdoer may feel justified in asking:

#### IV. Why Should I Be Moral?

Some of the answers:

- \* Being moral is being rational.
- \* Being moral is prudent (self-interested).
- \* Being moral is deciding what kind of life I want to live.
- \* Being moral defines what kind of person I want to be.

If none of these works to convince a wrongdoer to desist, then he has declared himself outside the moral community, with all that this isolation entails. He may not care--or say that he doesn't care. Then he is also irrational: for he is saying, in effect, that inconsistencies don't bother him. There is nothing more to do. Moral justification, persuasion, logic--have come to an end.

It is in consideration of this general question that people sometimes ask: "Who says?" or "Who's to say?" This implies that they think being moral is like conforming to an authority (e.g., the police, or even, for a Catholic, the Church), and they wonder why they should. The indiscriminate and mindless rebellion against authority that characterizes some people in every age furnishes a plausible context for this now too-prevalent attitude.

Our first response must be: "No one says--ever." And if they do say, this, for a mature adult, is never a reason for being moral. Being moral is not, in any respect, conforming to someone else's will. It is, above all, conforming to the impersonal ("fair") rules or principles that are relevant to the situation, applying them sensitively to the situation--and voluntarily taking the moral point of view.

At this juncture, individual autonomy and responsibility for one's choices become pertinent. It is the individual's responsibility to determine how he ought to act. *But in no way does this mean that any way at all that he, or others, decide, is necessarily right.* Being right is applying the

considerations discussed above, just as doing good science is applying the criteria and rules of reliable research.

#### V. What can we justify doing about security breaches?

- \* First: Even to posit the question of justification is to posit the wrongness of security breaches.
- \* Second: Consideration of our *obligation* (not only our *right*) morally to censure computer security breaches.
- \* Third: Consideration of moral sanctions (blame, shame, holding responsible, punishment).

#### VI. Probable motives for security breachers

Breachers--

1. Are narcissistic, egotistic, hedonistic; want the kind of attention that results from being clever, intelligent, crafty, winning the challenge (one-upmanship); gratifying ego-gains;
2. Regard computer instruments, programs, techniques, networks, etc., as impersonal, remote, abstract; so personal injury is not seen to be involved;
3. Regard the ownership of the same as indecisive, unsettled; "ideas" are "out there," nebulous, intangible--hence not "private property" in any concrete sense;
4. Do not see that the idea of reciprocity or of a reciprocal contract is involved, that is, that morality requires reciprocity of consideration, the golden rule, two-way empathy and sensitivity;
5. Have likely breathed in the cultural norms of "entitlements" and are also keenly aware of conflicts between rights, so they emphasize their "right to know" (a right, by the way, that is hard to justify as a general right) as against someone else's right to his property or to his privacy: to the hacker, the latter do not seem so important. Under this rubric, conflicts of loyalty may also arise. This is a genuine problem. Whose interests shall I satisfy if they conflict with others' interests, including my own?
6. Perhaps make an implicit, almost unconscious analogy with the publicness of the media: radio, TV, print--and hence pattern computers and their products, as media, on this attribute of publicness. If it's public, it doesn't belong to anyone--hence no one is harmed by hacking and no one is responsible for doing it either.
7. Have breathed in the social decay of excuses, non-agency, non-responsibility, non-work--all exacerbated today by our legal system.

8. Can sometimes gain attractive remuneration for hacking.

Insider breachers who may not be driven by antisocial motives like those above may be driven by sheer mindlessness, authority insecurities, ill-defined job boundaries, ignorance, or even by positive motives of loyalty to others or the desire to be nice to someone. "Social engineering" relies on these motives.

If some of the above constitute the motivational field of hackers and other computer criminals, then we have to ask how moral reasons and moral justifications can override these motives. Knowing what motivates someone to do something often furnishes important background knowledge for knowing which approach to use.

But if justifying reasons (moral considerations) prove ineffective in overcoming InfoSec breaches, then one tries to cause the breacher to change (as one causes a marine recruit to change his orientation to life and death by manipulating his surrounding conditions and motivations). At this point, we have left morality and entered the domain of social psychology.

We have not touched on virtue ethics. Without individual virtue and character, no moral rules or principles can take hold; they are nothing more than personal conveniences--shams. Unless individuals want to be virtuous, want to strive toward improvement in their character, no rational syllogism will persuade them that the moral life is, on balance, better than a life of self-interest.

But this is another story.



# 17th National Computer Security Conference

## *Interdisciplinary Perspectives on InfoSec*

# Psychology and InfoSec: Improving Compliance with InfoSec Policies

Prof. Percy Black

Department of Psychology, Pace University, Pleasantville, New York, NY

*Why is it that people know what is good but do bad?*

Socrates, 2500 years ago, claimed that this question pressed him more than any other. After years of reflection, he concluded that although people feel they benefit themselves when they knowingly do wrong, they actually harm themselves. Why? Because they alienate themselves from their society, from which they have derived everything of importance to themselves--their name, their mother tongue, their cultural heritage. Therefore, if they could but realize that they are actually harming, not benefitting themselves, they could not possibly do wrong.

There is some truth to Socrates' view. But today we know from child psychology and from sociobiology that individuals differ markedly in the degree to which they internalize their culture's beliefs, especially its moral expectations. Each of us, in short, is wired somewhat differently from the start. Therefore a set of conditions designed, for example, to make people act responsibly do not fall on the same soil.

Nonetheless, in line with Socrates's assumptions, human beings in the main share certain common attributes, thus making it possible for most aspects in a given culture to rub off in approximately the same way. For example, most individuals in a given culture learn to speak the same language, to share common religious beliefs, and be guided by the same social norms, such as rules of reciprocity and civility.

As specialists in information security, you must encourage people to exert constant vigilance and responsibility in protecting information. You must convince them that such care constitutes a high moral principle and duty. And you must bring this about without creating a work climate that is unduly suspicious or pathologically paranoid, thus without diminishing the North American spirit of good-natured informality and jocularly. Within the general parameters and limitations I've just outlined, I offer here several general suggestions that you may wish to consider in your efforts.

## **On Motivating Employees To Maintain Responsible Behavior in Protecting Information**

### *Key Concept: Convey Rules in a Matrix of Human Warmth*

Rules for moral compliance are generally not alone sufficient to engage human beings to behave responsibly or sensitively. Before rules can become dynamic properties of human action, people must first want to behave responsibly. Want must come first; then the rules. People must first feel connected emotionally to those whose cold, logical rules they are expected to internalize, to be guided by as if by nature. How can this matrix be achieved and maintained on an ongoing basis?

### **To Build a Receptive Matrix for Information Security**

#### *1. Create Identification With Organization and Supervisors*

People internalize those rules best which are expected of them by those whom they respect, whom they can identify with, and model after. Toward this end, I venture this principle: People become receptive to expected rule-following behavior to the degree that they feel their employer, their school, their country, or even their parents care about them.

The norm of reciprocity is deeply implanted in the human psyche. If you feel that I am earnestly concerned about your well-being, you are in turn the more likely to follow my expectations for self-aware and responsible actions. Not only one's supervisors must demonstrate that they care, but the total climate of the organization from the top down--should exude caring and concern for everyone in the organization.

Human beings are rule-following creatures. We love to follow rules. And we follow those rules best when we feel that those who expect us to do so are people whose characters and personalities we respect and who we feel care for us. How can an administrator or supervisor exhibit caring and interest in the person at the bench or "little me" at the secretary's desk or in the mail room?

*Connect with the person beyond the job.* The answer lies in relating to the individual under your jurisdiction not solely as a work object, as someone who performs a particular function, but as a person with concerns, interests, and capacities that stretch beyond the work station. Nothing can be more endearing to each of us than to feel that those in positions of authority remember from time to time to inquire about an ailing parent, or that we collect toys for poor children, or that we are considering taking a course in ancient music, or that we still haven't made up our mind about what career to follow. Within a climate of human concern, we human beings feel motivated to learn, to work, to do our best for those who show the warm face of humanity to us. Rule one therefore is: Connect with the person beyond the job.

## *II. Be Not Overly Perfect*

Research has shown that people identify best with those authority figures who are undoubtedly expert and proficient but who are not so perfect that they are error-free in all respects. An experiment showed that an expert lecturer was much better liked by one group of students though he had accidentally spilled a cup of coffee on his suit during the lecture than when he gave the same flawless lecture to another group of students but this time his coffee drinking was without mishap. The moral of the story is that when authorities are too perfect, they may be admired but they are less likely to be identified with because they appear out of reach of most of us. John F. Kennedy's ratings went up after the Bay of Pigs disaster when he admitted to making a wrong decision. He was seen as all the more trustworthy because he was not so perfect as he appeared in speech and manner. He was human.

This lesson is especially relevant to those who prescribe rules to others for self-vigilance and responsibility for the success of the total operation in safeguarding information. Rule-prescribers, self-appointed moral gurus, can readily appear to be perfectionistic "goody two shoes," out of reach for the rest of us imperfect mortals.

*Implication: Fear not to disclose your imperfections.* Tell about instances where you too have flipped, and therefore had to redouble your efforts at self-monitoring. With such honest self-disclosures, you as an authority will garner respect for your honesty, and therefore increase the likelihood for others to identify with and to model after you.

## *III. Inoculate Against Counter-Persuasion*

Research in social psychology has shown that people can be fortified against weakening in their beliefs and attitudes if they are provided scenarios in advance indicating how others may seek to "outrason" the rationale for their beliefs, attitudes, or actions. Similarly, in providing rules of conduct for safeguarding information, it makes good sense to provide examples about how, in the easy-going, non-suspicious atmosphere of North American life, the individual may unknowingly compromise important information. To counteract such possibilities, say, in effect, "This is what you will encounter when such and such...." Another approach to enhancing responsible behavior is to enter into discussions of values--why, for example, they feel it is important to maintain vigilance, and to act responsibly at all times.

I feel fairly confident that all or most of you already provide such antidotes in prescribing your rules of conduct, so I will not belabor this point. But I cannot leave the topic without mentioning a useful tool for fortifying people against loosening their informal yet cautious vigilance: Role reversals.

*Psychodrama and role reversals.* In this approach which is a form of theater first used by the ancient Greeks and elaborated in our own day into principles for the harmonization of human relationships by the late renowned psychiatrist, Alfred Moreno--individuals switch roles and imagine themselves acting in different roles and different situations. In one scenario, your immediate supervisor might act as a fellow employee who happens to be your buddy, while you remain in your own role, and then you switch roles. By asking people to imagine confronting a variety of scenarios and responding spontaneously to the respective exigencies within the guidelines of the rules, the importance of self- vigilance and responsibility for safeguarding the confidentiality of the total operation may be the better stamped in.

#### *IV. Once Is Not Enough*

As in advertising, presenting a message only now and then, however convincing, is not likely to stamp in the expected rule-following behavior. As is done also in medical and nursing colleges, it is necessary to convey the message on a regular basis, and in a variety of circumstances. For the tendency toward laxity or memory interference especially when we are tired or under time pressure--has been repeatedly shown in psychological research. The antidote: Repetition, repetition. The manner of presenting the ideas, however, should not be allowed to become stale. Variation of approach is imperative, lest you dull your audience's senses.

#### *V. Relieve the Tedium of Rule Recitation With Humor*

For three reasons it seems advisable to suggest that humor is a fitting vehicle for communicating the do's and don'ts for safeguarding the confidentiality of information. First, because rules are cognitive structures involving a mixture of situational variations matched with practical reasons and moral oughts for acting in particular ways, to recite them in sequence can become tedious to the communicator and boring to the listener. Well-designed humor, be it in cartoons, catchy phrases, or film, may relieve the tedium.

Second, because the acquiring of new rules because it is expected of us can be perceived as imposing on oneself restrictions of one's autonomy and spontaneity, humor may lighten the felt burden and thus may facilitate the individual's rule-learning and rule-following.

Third, humor can convey the notion that one need not throw off one's culture of easy-going informality and good- humor simply because one has to be extra-careful in one's relationships with others where confidential information is involved. Indeed, via humor all staff can learn how to challenge even senior officials who may demand certain information to which ordinarily they are not privy to.

## *VI. Enhance Awareness of Moral Rectitude*

Research by social psychologists since 1972 has repeatedly demonstrated that when people are tempted to violate their moral rules in order to benefit themselves in a some way, they become inhibited from doing so when their self-awareness is increased. In this condition, people become more attentive to their moral rules, and this increased salience buffers them against the current temptation, e.g., to steal, cheat, or lie.

One technique that has proved effective in eliciting self-awareness is the availability of mirrors so that people can see themselves. Accordingly, by strategically placing attractive mirrors in relevant work locations, people might appreciate seeing themselves while at the same time keeping their sense of responsibility awake.

### **Conclusion**

Multiple psychological routes are available to enhance information security. Although the routes suggested above issue from solid concepts, it is possible some or all have not been specifically applied to specific requirements of maintaining security of computer information. Accordingly, these ideas if applied, should be tested for their efficacy in "outcome research." I predict that in those facilities where the application of these concepts were applied over a substantial period, significantly fewer cases would result in compromise of confidential information by negligent, irresponsible, or deliberately unlawful actions.

However, given the complexity of shifting human wants, changes in mood, resentments, information overload, and so on, will require of administrators in information security constant vigilance and constant upgrading of approaches. There is no easy way to prevent memory lapses and irresponsible actions. There is no magic wand that can be wafted in front of people's faces to hold them without wavering to expectations of high standards in moral and legal responsibility.

Sorry, Socrates, we have learned some answers to your question about why people do wrong even when they know what is right, but the work of those who guard the integrity of information must remain a task of constant vigilance.

## **Summary of Psychological Guidelines for Enhancing Implementation of Information Security**

- I. Elicit spontaneous identification by employees with their organization and its supervisors:
  1. Foster a climate within your organization that regards all employees as respected parts of it;
  2. Convey rules in a climate of informality and warmth.
- II. Be not overly perfect.
- III. Inoculate against counter-persuasion by self-protective phrases and by role-reversal experiences.
- IV. Vary the formats of repeated do's and don'ts.
- V. Clothe the heaviness of rules in humor.
- VI. Enhance the power of conscience through self-awareness: Use mirrors.

# 17th National Computer Security Conference

## *Interdisciplinary Perspectives on InfoSec*

# Military Science and Information Security

**James P. Craft**  
**Manager, Security Engineering**  
**Systems Research and Applications Corporation, Arlington, VA**

*Pan Ta Re - War is the Father of All Things --Ancient Greek Saying*

The growth and integration of information systems in the United States has opened all of our technical and economic data to exploitation. This exploitation when carried out by other nations may take the form of information warfare. If we are engaged in information warfare, then military science offers useful insights for information security (InfoSec).

Military Science includes, at the least, military history, strategy, tactics, operational planning, leadership, and the study of specialized technologies. A related military discipline, counter-intelligence (counter-espionage), has been a major contributor to InfoSec. However, military science, as a whole, serves as both a model for how InfoSec should be structured and offers insights that translate into useful principles for InfoSec. Today, nations are actively competing to collect, or have access to, the best global technical and economic information. This drive to excel on economic and technological levels leads to Information warfare. Nations that deny this reality may find themselves impoverished as they produce inferior goods and lose in global, information-driven economic competition.

The major arena for this Information warfare has become the national and international databases and their connecting information networks, such as the Internet and the planned National Information Infrastructure (NII). Additionally, the vast amount of information used to propel technology advances and support economic activity requires advanced storage, retrieval, search, and analysis mechanisms being developed in the information technology (IT) field. IT may become the primary military technology of the 21st Century. Warfare, the conflict between nations, has been a history of technology advance and the ability of nations to exploit it. Technologies that dominated 19th and 20th century military attentions (e.g., metallurgy, chemistry) now fall in line behind IT as forces for change. Unfortunately, many military thinkers only think of Information warfare in terms of using computers during the execution of a traditional war, not as the conflict for the global sum of human knowledge. The confusion over the nature of Information warfare has created some confusion over who is in charge and what national actions to take.

One may be prompted to ask, "Is there really Information warfare? and, if so, is it significant enough to warrant imposing the combative mind-set found in Military Science?" IT has largely

grown out of academia where the value of the open exchange of knowledge has been a basic tenet. In the United States, our society has translated this belief into an open society that prizes individual privacy, but distrusts governmental or organizational secrets. In this view, information systems are the public libraries of our age. We cherish the open access to knowledge that has fostered our technological growth. The concept of information warfare is a double edged sword. Measures that protect our information may also restrict the free flow of information that provided the information initially. To get we must give. Open systems dominate the IT world, and we must use them, but we marginalize the threats to our interests. We admit that there are bandits on the information superhighway but we are not watching for invading armies.

Be it warfare or merely banditry, the effect is devastating even if it is not obvious. Traditionally, warfare is the organized effort of a nation to use force to seize assets, disrupt the normal life of another people, or actions to defend from such efforts. Warfare can be described as banditry on a grand scale; it is the taking of property by nations. Information warfare is different because it is largely unseen. If we have difficulty accepting the reality of Information warfare, it is because we have not fully accepted the notion of intellectual property, i.e., that knowledge has value and can be owned, sold, and traded. As some of our national information dependent industries (steel, chemical, electronics, etc.) are weakened or taken over by foreign interests, it is reasonable to view the organized collection of key data by competitors as a form of warfare.

In the United States, many professionals would not be upset if they came to work and found someone working on their desk computer, using it to access corporate information. However these same professionals would be furious if they went to the office parking lot and saw a stranger eating lunch in the front seat of their car. There is no widespread feeling of group ownership of information. This parallel is reflected in our national policy. Our country would react violently if a few thousand citizens of another country arrived on our shores, uninvited, and started carrying away anything in sight; yet we seem to have little concern that our technology and economic data are routinely carried away by thousands of foreign interests with no control and no exchange of value. Examples of information warfare include:

- \* The former Soviet Union (and now Russia) used several international organizations (such as IAE, IASA, etc.) to gain effectively unrestricted access to the Internet and other western networks (e.g., VENUS, TYMNET, Radio Swiss, ESA). The Soviet Union and its allies used these avenues to collect technical data to be funneled into their military industrial complex. This information was worth trillions of dollars during the cold war. These former adversaries are now using the cold war intelligence services to gain economic and technical advantages.
- \* Germany's industrial giants, which see themselves as partners of the national government, routinely delay the release of technical and scientific papers for years to allow their industry to take advantage of these advances before other nations can.
- \* France uses the full weight of their intelligence services to support French industry. In the 1970s and 1980s, France used United States government-provided software, U.S. super-computers, and current United States economic data bases to conduct economic modeling and wargaming. France's restrictions on outgoing scientific, technical, and economic data are even tighter than those observed in Germany.



- \* Japan uses subtle techniques, like the security features of a Zen garden, to restrict data going out and maximize technical and economic data coming in to Japan. Japanese databases can be searched jointly with English-based databases by means of English titles and keywords, but the abstracts and full text of on-line resources are in Kanji, which poses an innocent looking barrier to outside researchers.

Issues associated with information warfare include national policies on trans-border data flow. Foreign ownership of database holders and vendors operating in the United States, have been addressed by others. The use of public networks to collect this information has even reached the popular culture in books, such as *The Cuckoo's Egg*. Yet the InfoSec community has not translated this realization into a discipline geared to respond effectively to the perceived national threats. As an open society, we have accepted the military as a necessity even when its existence conflicts with cherished beliefs, so it will be with the InfoSec warrior. To remain an open society, the capacity to survive and win Information warfare must be fostered as a national policy and individual choice.

To respond to the reality of Information warfare, I propose that we examine military science, in total, to decide what may be applicable in the InfoSec area. From Sun Tzu's *The Art of War*, Mushashi's *The Book of Five Rings*, and B.H. Liddle Hart's *On Strategy* to military leadership philosophy and the structure and execution of military alliances, we would benefit from deciding what we can adapt and what we need to discard. The Japanese have so adapted *The Book of Five Rings* to business and are likely to refer to it in the area of information warfare. Western writings also offer rich sources for review. For example, B. H. Liddle Hart's works on strategy can be summarized into eight principles, six positive and two negative. Shown below, Hart's principles of dislocation, attack, and exploitation, are as applicable to information warfare as to traditional conflicts of arms:

#### Positive principles:

1. Adjust your ends (objectives) to your means.
2. Keep your objective always in mind.
3. Choose the line (or course) of least expectation.
4. Exploit the line of least resistance (towards the objective).
5. Take a line of operation which offers alternative objectives.
6. Ensure that both the plan and the dispositions are flexible--adaptable to circumstances.

#### Negative principles:

7. Don't throw your weight into a stroke whilst your opponent is on guard.
8. Don't renew an attack along the same line (or in the same form) after it has once failed.

Our dependance on IT is reaching the point where an InfoSec "Pearl Harbor" in the global economic arena is not out of the question. Currently, we are dealing with the unrestricted collection of our valuable intellectual property by other nations. In the future, we may be dealing with the corruption of technical data or the denial of critical, national IT assets. The next Internet worm may be an Internet dragon! Military science, adapted to information warfare, offers insights on how we may attempt to slay the beast and deal with those who unleash it.

## **Panel: Ethical Issues in the National Information Infrastructure**

Jim Williams, Chair  
The MITRE Corporation  
San Diego, CA 92152  
jgw@mitre.org

Dorothy Denning  
Computer Science Department,  
Georgetown University,  
Washington, DC 20057  
Denning@cs.georgetown.edu

Grace Hammonds  
Vice President, AGCS, Inc.  
Stoneham, MA 02180  
Hammonds@dockmaster.ncsc.mil

Hilary Hosmer  
President, Data Security, Inc.  
Bedford, MA 01730  
Hosmer@dockmaster.ncsc.mil

Eric Leighninger  
Andover-Newton Theological School  
Newton Center, MA 02159

Marc Rotenberg  
Director, EPIC  
Washington, DC 20003  
info@epic.org

The NII is to be an advanced information infrastructure that will enable U.S. firms to compete and win in the global economy, generating good jobs for the American people and economic growth for the nation. As importantly, the NII is to transform the lives of the American people - ameliorating the constraints of geography, disability, and economic status — giving all Americans opportunity to participate more fully in the political process and promoting equity of professional opportunity.

As with any major new undertaking, the NII will involve ethical tradeoffs and potential conflicts of interest. Moreover, the social, legal, and ethical values reflected in the design, implementation, and management of the NII will be highly visible in the security policies supported by the NII (or lack thereof). Already, the question of balance between privacy and the government's need to investigate criminal behavior has been reflected in heated controversy over the Clipper Chip. This panel will address broad issues that might easily devolve into similar controversies. This panel overview presents sample issues that may be discussed and introduces the panelists.

### **Sample Issues**

1. *Provision of Security Services.* Who should provide security services such as back-up, encryption, filtering, and virus protection — telecommunications service vendors, end host vendors, add-on software product vendors, or individual users? Current Internet users are relatively well-educated, from middle class backgrounds, and accustomed to working within voluntary guidelines. Opening NII to a more diverse population may require significantly more attention to security.

2. *Information Overload.* The Internet is already burdened by junk mail, unwanted pornography, and excessive quantities of legitimate mail, despite the fact that commercial use has been greatly restricted. Our telephone systems provide only partial protection against telephone harassment, obscene calls, and computerized cold-call telemarketing. The wide-open NII will apparently be much freer and more powerful than existing communications infrastructures, so that the information-overload problem will intensify and must be dealt with. Additional legal and technical support for recipient control over the transmission of information may be needed.
3. *Privacy Versus Accountability.* Computer Professionals for Social Responsibility (CPSR) advocate anonymous network connection, so that one has privacy in navigating throughout the network. Reconciling this goal with traditional billing and accountability goals poses both ethical and technical challenges, and may require new approaches to Identification and Authentication. For example, the Swiss telephone companies do not log phone calls and expect customers to accept billing information on faith, as a result of lessons learned during World War II.
4. *Privacy Versus Surveillance.* Who owns employees' electronic mail? Under what circumstances may it be monitored by an employer? Who owns the personal information in the customer databases of large corporations? To what extent may it be sold to the public?
5. *Equity of Access.* The Clinton administration advocates universal access to the NII and would provide public terminals and subsidies to libraries, hospitals, and public schools so that all Americans can participate. Universal access implies much more competition for currently scarce resources. Equitable ways must be found to share and pay for NII services. It may also be prudent to restrict access to criminals who are likely to misuse the NII - universal access need not be completely universal.
6. *International Ramifications.* Wide access to foreign exploitation by people and governments that traditionally have not respected our way of life may make some issues far more acute. Will availability of information cause us to lose our competitive advantage? Can the NII be used to evade domestic laws by migrating illegal activities to foreign countries?
7. *Adequacy of Historical Precedents.* As can be seen from the above issues, the greater technical capabilities of the NII amplify partially solved problems in existing communications systems. The NII can not only profit from judicious extension of existing policies for these systems; but can also sharpen our understanding of existing issues with these systems.

## About the Panelists

Dorothy Denning chairs the Forum on Rights and Responsibilities of Participants in Networked Communities, under the sponsorship of the National Research Council and the Computer Science and Telecommunications Board of the National Academy of Sciences. Dorothy is author of *Cryptography and Data Security* and is a frequent speaker at National Computer Security Conferences.

Grace Hammonds is a member of the National Council of Negro Women. As a Black woman, she is constantly reminded of the racism that exists in this country. She envisions the NII as potentially a "great leveler," because of the anonymity possible when one uses a computer as the method of interaction with others. Grace foresees a future where everyone will be able to benefit from NII developments, with negative stereotypical characterizations not an issue. For this to happen, the NII must be accessible to all at an affordable cost, and potential conflicts between privacy and accountability must be carefully resolved. Grace has been involved in information security work for 18 years and authored an early draft of what became the TCSEC.

Hilary H. Hosmer sees the emerging NII "I-way" as multicultural, pluralistic, and resilient. Supported by Small Business Innovative Research (SBIR) grants from the Hanscom, Kelley, and Rome Air Force Bases, she is currently focusing on the problem of multiple conflicting security policies in a potentially infinite network. After graduating from Bryn Mawr College, Hilary spent two years in the Ivory coast as a Peace Corps volunteer, then trained American teachers to deal with problems of desegregation before starting to work with computers in 1972.

According to Eric Leighninger, the fact that the NII must operate in a multicultural, technically pluralistic context will require particular attention to what constitutes right, good, and fitting ethical responses to questions of accessibility, accountability, and privacy in the face of often conflicting private, corporate, and government interests. Eric holds a masters degree in mathematics from Arizona State University and has worked in the defense community as a software engineer specializing in computer security and trusted system development. He is a divinity student whose professional interests include social ethics of computing, the uses and abuses of cryptography for trust and privacy, and security policy modeling.

As director of the Electronic Privacy Information Center (EPIC), Marc Rotenberg wishes to focus public attention on emerging privacy issues relating to the NII, for example, the Clipper Chip, the Digital Telephony proposal, medical records privacy, and the sale of consumer data. EPIC was established in 1994 as a public interest research center in Washington DC. EPIC pursues Freedom of Information Act litigation, conducts policy research on emerging privacy issues, and publishes the EPIC Alert and EPIC Report. Marc is a former counsel for the Senate Judiciary Committee and is currently a Fellow in International Law at Georgetown University Law Center.

Jim Williams sees the NII as an opportunity for significant advances in our understanding of information security. His current activities include contributions to new protection profiles for trusted information products, the modeling of external consistency in high-integrity systems, and the modeling of multilevel-secure database systems. Jim has been involved in security modeling and the use of formal methods for the last 18 years. He holds a Ph. D. in mathematics from UC Berkeley.

# **Medical Information Privacy Current Legislative And Standards Activities**

**Marc Schwartz, Chair  
Director of Clinical Services  
Summit Medical Systems, Inc.  
Minneapolis, Minnesota**

The appropriate application of electronic information systems to health care will be critical to the future success of any reform initiative, irrespective of which specific reform proposal, if any, is passed by Congress this year. The ability to provide efficient, appropriate and cost-effective care will only be met by the implementation of standard structured methods in information systems, electronic data interchange and privacy and confidentiality within this complex environment. Health care has seen the haphazard implementation of information systems without any central focus or system-wide strategy. Most systems have been applied to solve very specific problems within the clinical or administrative departments of hospitals, clinics, doctor's offices, employer based health services, insurance companies and other payers of health care, medical product manufacturers, research entities or local, state and federal agencies without any consideration of broad information processing and access needs. This dissonance has resulted in the creation of "isolated islands" of both paper-based and electronic-based data that provide for massive duplication of information, lack of timely access due to missing or otherwise inaccessible records resulting in repeated medical procedures and increased cost, and the great potential for inappropriate disclosure of data to third parties without the consent of the patient. Information security is typically not considered as an integral part of these systems and is viewed as an "add-on" function to these systems.

The medical information industry has been identified to have a potential market on the order of billions to tens of billions of dollars. This has attracted the "major" players in the computer hardware and software industry to this very lucrative marketplace. However, without the utilization of emerging system standards, we will find that these islands of data may only grow larger, and may not, in fact, be brought together in an efficient way. The ability to link the data between the various entities with a "need-to-know" will be critical to the efficient delivery of care. The need to incorporate the concepts of privacy and confidentiality early on in the design and development phases of these systems will be critical to their effective functioning, while insuring, to the best of our abilities, the patient's right to privacy.

Current paper based systems, in fact, offer no trusted method for access control (other than physical restriction of access to the paper records, which can be easily circumvented by anyone with a white lab coat), data integrity, audit of access and identification and authentication for entries or modifications. Electronic systems can provide these functions, but they will be held to a higher standard than the current systems. The well founded fear within the general public of breaches of these systems by crackers or legitimate "inside" users searching for information that may be of "value" to some entity, demand that we find the means to protect this information.

However, technology alone will not solve the problem. We must provide the means for behavioral modification on the part of existing system users so that they do not become, as in many environments, the prime target or source for information disclosure. We must also make sure that "the mission is not compromised due to security". We cannot ask a nurse in the intensive care unit to enter multiple passwords, user IDs or scan "smart cards" or perform biometric I&A in the middle of a critical situation. The patient

would likely be dead by the time the nurse returned. We then, must acknowledge that there are differing levels of access, different levels of "need-to-know" within these environments such that the same mechanisms for information security will not fit every situation. A simple example would be the separation of medical and financial information. The clinical personnel have no "need-to-know" vis-a-vi the financial data and vice-versa. On the other hand, coded financial transactions can infer or even explicitly define clinical information. How do we best protect this information while providing the infrastructure to enhance the effective delivery of information to support medical decision making in this complex system?

This year Congressman Gary Condit (Calif.) has introduced legislation (*The Fair Health Information Practices Act of 1994*, H.R. 4077) that will provide the legal basis for the implementation of privacy and confidentiality in the medical environment. This legislation is the reflection of the activities of many professional organizations within the health care community and the federal government, that have realized the need for preemptive national legislation to resolve the inherent conflicts amongst the current plethora of state based statutes that are in place, some of which have been interpreted to actually prohibit the implementation of computer based information systems for the medical record. This bill sets the standards by which all holders of health care information will have to abide in the implementation of any information system. The bill, out of necessity, leaves open the specific details of implementation of information security in these environments recognizing the great potential for changes in technology and functional requirements as these systems mature. Thus, there will be a great deal of discretion on the part of system designers and users during the classic risk/benefit decision making process of making sure that the legal requirements are met while insuring minimal financial investment and the least impact on the users. This balance will be critical in affording the patient an appropriate level of privacy, recognizing that absolute privacy is likely not realistic.

Our panel will consist of the following recognized leaders in this domain:

- Mr. Robert Gellman, Chief Counsel to the House Subcommittee that formulated H.R. 4077 will present this critical piece of legislation during this panel session.
- Ms. Molla Donaldson, Project Director for the Institute of Medicine's 1994 publication "*Health Data in the Information Age: Use, Disclosure and Privacy*" will present the Institute's findings and position.
- Mr. C. Peter Waegemann, Executive Director of the Medical Records Institute and a representative to the ANSI Health Care Information Standards Planning Panel (ANSI-HISPP) Privacy, Security and Confidentiality Workgroup will report on their standards activities.
- Mr. Dale Miller, Director of Consultant Services for Irongate, Inc. and the information security consultant to the Computer-Based Patient Records Institute, will present the current activities of the CPRI Confidentiality, Privacy and Legislation Workgroup.
- Mr. Gerald S. Lang of The Harrison Avenue Corporation has served on various governmental and private committees pertaining to information privacy and storage standards and will present some provocative views on the use of Smart Cards in this domain. Mr. Lang was the chairman of this panel at the 15th National Computer Security Conference in 1992.

Please refer to each individual's specific panel summaries for further details on their presentation.

**Robert Gellman**  
**Chief Counsel**  
**Subcommittee On Information, Justice, Transportation and Agriculture**  
**United States House Of Representatives**  
**Washington, D.C.**

The Fair Health Information Practices Act of 1994 (H.R. 4077) was introduced on March 17, 1994 by Representative Gary Condit (CA), Chairman of the Subcommittee on Information, Justice, Transportation and Agriculture. The bill is intended to be considered as part of the Health Security Act (H.R. 3600). Subtitle B of Title V of the Health Security Act has been referred to the Subcommittee.

The purpose of the Act is to establish a code of fair information practices for the use and disclosure of health information that originates in or becomes a part of the health treatment or payment system. The Act establishes uniform federal rules that will apply to covered health information in all states.

There are two new basic concepts in the Act. First, identifiable health information relating to the provision of or payment for health care that is created or used during the medical treatment or payment process becomes *protected health information*. In general, protected health information remains subject to statutory restriction no matter how it is used or disclosed.

The second basic concept is that of a *health information trustee*. Almost anyone who has access to protected health information becomes a health information trustee under the bill. There are three different types of trustees. Those directly involved in providing treatment and in paying for treatment are *health use trustees*. Those who use identifiable information for public health or health research purposes are *public health trustees*. Finally, others who have an occasional need for health information to accomplish a specific purpose authorized by law are *special purpose trustees*.

Each class of trustee has a set of responsibilities and authorities that have been carefully defined to balance legitimate societal needs for data against each patient's right to privacy and the need for confidentiality in the health treatment process.

Trustees are required to:

- Maintain appropriate administrative, technical and physical safeguards to protect integrity and privacy of health information.
- Maintain an accounting of the date, nature and purpose of any disclosure of protected health information.
- Use protected health information only for a purpose that is compatible with and related to the purpose for which that information was collected or obtained by the trustee.
- Limit use or disclosure of protected health information to the minimum necessary to accomplish the purpose.



- Disclose protected health information only for a purpose that is authorized by the Act. Permissible disclosures vary by trustee; health care trustees have the most authority and special purpose trustees the least.

Patient rights vary slightly depending on which type of trustee maintains protected health information. For health information used in treatment or payment, patients have rights to:

- Inspect and to have a copy of medical information about themselves.
- Seek correction of health information about themselves that is not timely, accurate, relevant or complete.
- Receive a notice of information practices describing their rights, the procedures for the exercise of those rights, and the disclosures of protected health information that are authorized.

The Fair Health Information Practices Act of 1994 includes several different enforcement mechanisms. There are criminal penalties (up to ten years in prison), civil remedies for aggrieved patients, and civil money penalties that may be imposed by the Secretary of Health and Human Services. In addition, the Act provides for alternate dispute resolution as another mechanism for resolving disputes between patient and protected health information trustees.

**Molla Donaldson**  
**Senior Staff Officer**  
**Institute Of Medicine**  
**National Academy of Sciences**  
**Washington, D.C.**

The escalating intensity of public interest in the cost, quality, and accessibility of health care services has engendered a need for better health data. The coming of the computer age to medicine and health care has opened new frontiers for data collection, management, and use, and experts envision that greatly enhanced electronic data-handling capabilities could present an unparalleled opportunity to employ computer technology in addressing these information needs. Consequently, diverse groups of researchers, business leaders, health professionals, and policymakers at state and regional levels have begun to develop comprehensive, population based databases that will reliably provide needed health information and permit far more sophisticated analyses than have been possible to date. Use of such databases, however, raises the specter of misuse and harm to patients if these data are not carefully protected. The benefits of such databases and the ways in which such harm can be prevented or mitigated are the subjects of a new report from the Institute of Medicine (IOM), *Health Data in the Information Age: Use, Disclosure and Privacy* (Donaldson MS and Lohr KL, eds., Washington, DC: National Academy Press, 1994).

The IOM Committee on Regional Health Data Networks, chaired by Roger J. Bulger, MD, President, Association of Academic Health Centers, offers recommendations about protecting the confidentiality of personal health data held by what it terms regional health database organizations (HDOs). Such organizations would have access to and possibly control of considerable person-identifiable health data outside the care settings in which they were originally generated.

Because HDOs will accumulate the most comprehensive and sensitive personal record databases yet established in the health sector, they challenge privacy principles. In health policy, privacy is best considered as informational privacy—a state or condition of controlled access to personal information. Two trends prompt concerns about informational privacy. First, the increasing complexity of health care and the involvement of larger staffs of health personnel have dramatically increased the number of people with access to a patient's health record as well as the amount of information collected and stored. Second, electronic storage and transmission of data enable interested parties to aggregate information on individuals from diverse sources, rendering computer-based health data a valuable commodity.

Various federal and state laws impose a duty to preserve the confidentiality of personal health information, but they have significant weaknesses. First, the degree to which current law requires confidentiality varies according to the holder of the information and the type of information held. Second, legal obligations of confidentiality vary widely within a single state and from state to state. Third, present laws offer little real protection against the disclosure of confidential health information to unauthorized persons. Finally, in many cases in which patients or their families ostensibly authorize disclosure or release of private personal information, that consent is neither truly voluntary nor fully informed.

**Federal Preemptive Legislation.** Given the generally scanty and inconsistent legal protections for privacy across geopolitical jurisdictions, the IOM committee believes that HDOs have both an obligation and an opportunity to fashion well-delineated privacy protection programs. The report recommends federal preemptive legislation (a federal statute that preempts or overrides state law). Such a law ideally will: establish a uniform requirement to assure confidentiality and protection of privacy rights for person-identifiable health data, specify a Code of Fair Health Information Practices, and impose enforcement

mechanisms and sanctions related to violations of the act. The law should clearly establish that the confidentiality of person-identifiable data is a property afforded to the data elements themselves regardless of who holds them.

**Access to Person-Identified Data.** The committee concludes that the sensitivity of a given piece of data is not inherent, but rather depends on the harm to which individuals are or believe themselves to be vulnerable if the information were known to others. Such assessments could differ dramatically by person, circumstance, place, or time. Therefore, the committee prefers that all data held by HDOs be afforded stringent protection.

The committee enumerates a very restricted set of individuals or entities to whom HDOs should give access to person-identified or -identifiable health information. They include: individuals for information about themselves; parents for information about a minor child except when such release is prohibited by law; legal representatives of incompetent patients for information about the patient; researchers with approval from their institutions' properly constituted Institutional Review Boards; licensed practitioners with a need to know when treating patients in life-threatening situations when patients are unable to consent at the time care is rendered; licensed practitioners when treating patients in all other (non-life-threatening) situations, but only with the patient's informed consent; and other HDOs whose missions are compatible with and whose confidentiality and security protections are at least as stringent as those of the HDO holding the requested information. Otherwise, the committee recommends that HDOs not authorize access to, or release of, information on individuals with or without informed consent. In particular, the committee holds that employers ought not to be permitted to require receipt of an individual's data from an HDO as a condition of employment or receipt of benefits.

**Person Identifiers.** The committee recognized the need for a unique, individual person identifier to facilitate the efficient operation of HDOs and data interchange among HDOs. It details the strong arguments against using the Social Security Number or its derivatives (e.g., for Medicare) as that unique identifier.

Many health care reform proposals place considerable emphasis on the development of person-level databases, and this factor heightens the importance of protecting such information. These kinds of databases hold tremendous promise for evaluating and improving health care and implementing effective new ways, in this computer age, to guard health information against unauthorized disclosure. Although the large public benefit may be easily understood, the potential for harm or lack of fairness may create concern and fear in many. To gain public and professional support for the vision advanced in this report—and to ensure the best uses of the health-related information that will be released—HDOs, government agencies, and public- and private-sector institutions must implement carefully planned strategies for privacy protection and must educate the public, health care providers, policymakers, and patients about these protections. The IOM report is intended to be an early step in that educational and public policy-making process.

**Dale Miller**  
**Director of Consultant Services**  
**Irongate, Inc.**  
**San Rafael, California**

The Computer-Based Patient Record Institute (CPRI) was formed in 1992 as the result of the recommendation of an Institute of Medicine Committee in its report, *The Computer-Based Patient Record: An Essential Technology for Health Care*. The committee recommended that the public and private sectors should join in establishing a Computer-Based Record Institute to promote and facilitate development, implementation, and dissemination of the computer-based patient record. The committee had been convened to examine the problems with existing medical records systems in order to address the needs identified by the National Institutes of Health and the Institute of Medicine to make patient records more useful for patient care, teaching, and research.

As a not-for-profit organization with a mission of initiating and coordinating urgently needed activities to facilitate and promote the routine use of computer-based patient records through-out healthcare, CPRI is unique because it is the only organization that represents all of the stake-holders in computer-based patient records.

As one of four workgroups, the CPRI Workgroup on Confidentiality, Privacy, and Legislation has several projects underway to contribute to achieving CPRI goals. Within the workgroup, the information security subgroup is addressing tasks related to three of these goals:

- Encourage creation of policies and mechanisms to protect patient and provider confidentiality and ensure data security.
- Coordinate the building of the technical and legal infrastructures for computer-based patient records.
- Serve as a clearinghouse for efforts to promote and develop activities related to computer-based patient records.

Following the publication of a white paper on *Access to Patient Data*, the workgroup established an information security subgroup to develop and publish guidelines for developing information security policies at organizations using computer-based patient records, to develop guidelines for managing information security, and to develop guidelines and materials for information security awareness training. Future tasks include developing guidelines for information security related application functions, guidelines for audit functions, and evaluation of technical methods for identification and authorization of access to CPR systems.

This presentation will describe the healthcare information security issues related to the computer-based patient record and will discuss the CPRI projects and activities designed to address those issues.

**C. Peter Waegemann**  
**Executive Director**  
**Medical Records Institute**  
**Newton, Massachusetts**

The Health Care Information Standards Planning Panel of the American National Standards Institute (ANSI HISPP) was formed to:

1. Coordinate health care standards within the United States
2. Be a focal point for communication with CEN TC 251

HISPP has a task group on Privacy, Security and Confidentiality. This presentation will give an overview of the various ongoing activities within the United States. It will also explain the efforts of the various standards organizations within the European Union which are involved in Privacy, Security and Confidentiality.

**Identifying the Needs of Future Health Care Systems**

- Special computer requirements in regard to confidentiality
  - Information security requirements for health care
  - Minimum requirements for availability
  - Minimum requirements for reliability
  - Minimum requirements for data integrity
  - Minimum requirements for permanence
  - Minimum requirements for auditability
- Authentication of health information
  - Minimum requirements for the five electronic signature categories

**Surveying Current Activities**

- Standards Development Organizations
  - ASTM, ASC X12, HL-7, ACR NEMA, IEEE MEDIX, NCPDP, ASC X3, ASC X9, Others
- Other U.S. Organizations
- Legislative Efforts
  - Federal
  - Selected States
- European Activities

**Gerald S. Lang**  
**The Harrison Avenue Corp.**  
**Silver Spring, Maryland**

There is much controversy concerning the storage, security, and portability of patient medical records. What I have to say today is intended not to quell the controversy but to make sure a fuller spectrum of factors bearing on this issue are considered. Also, I will delve into the use of selected health care data to increase health service productivity.

Consider it is mandated that every subscriber of the health care delivery system use a credit card sized storage medium capable of storing several megabytes of data, enough to record on X-ray image, an EKG or EEG strip, and medical record data. Should a patient's recent MRI image, for example, supplant a prior X-ray ordered by another physician? The security of medical information is affected by the answer.

If time is essential in the care of a patient, then the documents we store and protect for possible emergency use should convey the essential information quickly and easily. The medical record does not do this. If we do use a secure patient medical card, it should be zoned to provide unsecured access to basic administrative and emergency information, and then selectively zoned and secured for clinical access based on a legitimate need to know and with assured protection of patient rights and privacy. Remote access to patient records stored in data bases can be protected from access by unauthorized people if both the provider's and patient's health care cards are engaged simultaneously by the system. This procedure is similar to physical access to a safe deposit box at a bank which required insertion of both the subscriber's and bank's keys.

Suppose a patient card has to be replaced in order to store a new image. Who is responsible to make certain that all the other data on the card are recorded on the new card? Under what circumstances will providers and their staffs be authorized to issue new patient cards and to see sensitive data concerning drug and alcohol abuse, HIV tests, and AIDS treatment? Title 38 U.S.C. 4132 addresses this sensitive area for veterans and Title 5 U.S.C. 7361 and 7362 protects the confidentiality of substance abuse records for employees. Will we keep psychiatric information out of the system and if not, how will very personal and possibly damaging information be protected?

What happens when a patient loses or says he lost his medical record card? With a patient base of over 250 million, and with only a 3% loss factor per year, we can expect to encounter and replace approximately 15,000 lost and misplaced, and damaged cards per week. Patients may end up with two or more cards, and the medical data on each will not be identical. Further, when replacement cards are re-sourced and re-recorded, previously recorded transactions of outpatient visits and even hospital stays may vanish. Some provider treating a patient using a card with incomplete data may later on be accused of making an error and subject to possible malpractice claims. Audit trails may not contain sufficient information to cover situations such as this.

Now I will touch briefly on the use of health care data and improved productivity of health care services. Clinicians from their earliest training in the profession learn to extract data from the patients' medical records. This is the way they developed their skills. So they unwittingly spend considerable time in their daily practice performing lower skilled tasks such as those of data clerks and clericals while searching and collating patient data from the medical record. We need to

improve the way people gather and assimilate facts and synthesize this information into meaningful assessments of patient health status and health change.

If we can improve the information transfer process, much can be gained, because manpower is the most expensive resource in the health care delivery process. Except for the ritual of habit, it is unnecessary and a waste of physicians' time to wade through a medical record consisting mainly of reference and archival data to find and extract timely and pertinent information about the patient and his course of treatment. Somehow we must get physicians to realize they are not just practitioners of patient care but the main managers of the health care teams providing care to their patients. As medical care managers, physicians make decisions which mobilize the activities of the medical care team and have a direct affect up patient care, outcomes, and health care costs.

To contain costs and deliver more effective care, it appears necessary to interject more and better management into the health care delivery process. How can we do this? The answer, I believe, lies in the use of a management medical record.

A management medical record is not a patient summary, nor is it the repository of data we know as the medical record. The typical one page management medical record is designed to present three things for quick assimilation: the medical status of the patient, the current patient care plan, and the health care facility's responsiveness to doctor's orders and patient activities.

The information captured by the management medical record accumulates directly from the medical record, from staff inputs, and from ancillary service status indicators. Dr. Kenneth Dickie and I called this record a RECORDGRAM and it was published in 1978 in the book: *The Practice-Oriented Medical Record*. There are a number of features we would add to the RECORDGRAM to make it even more functional today.

There is one RECORDGRAM for each day of the patient's hospital stay and for each outpatient visit. If the physician and others on the health care team wanted to go back to the medical record to check on something, the process is simplified because there are direct linkages between items on the RECORDGRAM and documents stored in the medical record or in service archives such as in radiology.

The purpose of the RECORDGRAM is to improve the cost-effectiveness of health care delivery by giving the providers an unobtrusive management medical record they can use to quickly discern the essential facts and activities of a case. The RECORDGRAM file is not bulky—each page represents a daily snapshot of the patient during the care process. Rather than recording X-rays, scans and electro-waves with the RECORDGRAM, which would then need expert analysis and interpretation, the technique we used and still propose is to have the charge physician append to the service ordered, the essential information he extracted from the service report. That information is immediately available and the inquirer can still go back to the source to review the original clinical information, if desired. Another important feature of the RECORDGRAM is that the physician can use it while he is with the patient, whether at the bedside or in the examining room or at an outreach site.

Since a typical RECORDGRAM consists of only one page, it can be stored easily on current smart cards which would give maximal security for the data in portable applications. The RECORDGRAM format provides low storage demands and excellent security for general medical practice and for regional and national network use. It contains the necessary linkages to the

various embodiments of the patient's collective medical record that may reside at one or more hospitals, private physicians' and dentists' offices, clinics, HMO's, and special data bases.

I have no doubt that huge data repositories tied into high speed communications can be built and maintained. What troubles me is unauthorized remote access to medical information stored by such a system or consortium of systems. One of the problems is accurately identifying a person making a remote inquiry. There are three ways to verify the identity of such a remote user: by what the user knows, by what the user has, and what the user is. This last attribute requires biometric controls which do not seem necessary for our purpose. Through the process of *visual eavesdropping*, people in a work environment are usually able to pick up a fellow worker's access codes, thereby eliminating the protection of what a person knows as a line of defense. If, however, the system user also has to use a device in his possession, such as a smart card, the level of system protection increases many-fold. Further, because it is possible to change the authorized user's access codes and privileges while the user is on-line, without either the knowledge or participation of the user, the level of system protection increases even more.

I personally believe we should simplify the operation of the computer-communications system complex by keeping the system open just as the telephone companies do with their lines. Doing this should dispel the notion that centralized security can adequately protect a national medical data base. Secondly, why duplicate records that already exist at the provider facility? The medical information complex, or highway, threads all these facilities into an active network that can be protected by end-to-end controls. Access to these records would require the use of a smart card type of device for both the provider and the patient. The patient card would have the security keys needed to release the desired level of information. Lacking a patient card, a provider can contact an information officer at the facility controlling the patient's records. Based on an assessment of the situation and the remote identification of the caller and caller facility, the information officer can use his smart card device to release the desired information. Such a decentralized system permits the possible creation of medical record repository centers at a measured pace allowed by the economics of the time and also permit individual facilities to upgrade their systems from time-to-time and to benefit from the high bandwidth speeds and low costs afforded by the medical information-communication complex or highway.



# PRIVACY AND THE HANDLING OF PATIENT RELATED INFORMATION IN THE PUBLIC SWEDISH HEALTH CARE SYSTEM

Torleif Olhede, Spri, Box 70487, 107 26 Stockholm Sweden  
voice +46 8702 4600 facsimile +46 8702 4799

and

Center for Security Informatics, Dept of Computer and System Science  
Stockholm University/Royal Institute of Technology  
Electrum 230, 164 40 Kista, Sweden  
e-mail: tor@dsv.su.se

## Abstract

The goal for the Public Swedish Health Care system (PSHCS) is a *good, safe and secure care*. *Security* has at least three aspects namely *availability, integrity and confidentiality*. This paper focuses on confidentiality and especially *privacy* of patient related information handled in the PSHCS.

The Swedish ethical and legal claims on health care information systems concerning privacy is treated. The Constitutional Act about the Freedom of Information, the Act about the Freedom to Print on the one side and the Secrecy Act, the Medical File Act and the Data Act on the other, mirrors the ethical attitudes and sets the evaluation criteria for the study.

The project started in Oct. 1993 and the final results from the questionnaires and interviews were completed in April 1994. The results are based on a total investigation of four counties in Sweden. All district health care centres and laboratories, clinics and their sections at hospitals are included in the study. The medically professional parts were investigated through the questionnaire. Data, financial and archive departments were interviewed.

The questions in the questionnaire and in the interviews are coupled to the legal obligations. The purpose is to find out if decisions and if transferring routines are carried out in accordance with rules and recommendations. The outcome is compared with the norms deduced from the legal complex.

Even if the awareness of the legal framework and the knowledge of the demands deduced from it, seem to be widespread and the good intentions to fulfil the demands are expressed by the health professionals, the practical implementation to guard the patient's privacy is not carried out to the extent intended by the legislator.

### Key words:

health care, medical file, medical record, patient related information, security, confidentiality, privacy,

# **1.The Swedish health care system**

## **1.1 Basic figures**

Sweden has about 8.8 million inhabitants and her area is 449 000 square kilometres which is equivalent to 175 000 square miles. Public health care in Sweden is organised in 26 counties grouped in six regions. The most populated county is the Stockholm county with about 1.7 million inhabitants. The smallest is the island of Gotland county in the Baltic. It has about 60 000 inhabitants.

Sweden uses about 8% of her GNP for health care (HC) compared to the US approximately 13 %. The costs in Sweden are declining.

## **1.2 Political control and regulations**

The counties are led by politicians elected in general elections. They are independent and have their own right of taxation. HC is primarily financed by county taxes. The national insurance system does however also play a certain role in reimbursement of medication and of smaller parts of outpatient treatments.

During the last three years important changes have taken place at a very high pace. The main objective has been to reduce HC costs. Because of the independence of the counties various methods are being tested in different parts of Sweden. The general idea is to implement some kind of management by objectives system (MBOS). This leads to the attempt to assign responsibility for the management of services to local production units. The intention is to keep the political control of basic principles and quality.

The hospitals and outpatient clinics, including the district HC centres are still largely owned by county councils but the effectiveness and the efficiency of the individual clinics, are being compared and a competitive market of service production is establishing at least in the more populated areas. Recently it was decided that all inhabitants have to be listed at a General Practitioner (GP) at choice. The GP is going to get payment based at the number of patients listed rather than performed HC. This has lead to an increased number of private GPs with whom the publicly owned practices are competing on relatively equal terms.

The patients in Sweden pay a small fee for each visit and medicine up to a maximum of about US \$ 200 per year. This system protects patients with very high need for HC services as elderly and people suffering from chronic diseases.

The costs for sick-benefits and pensions are covered by the National Insurance System. This comprises everybody and is separated from the financing of HC.

### 1.3 Organisation

HC in Sweden is divided into three classes namely:

- **Primary care** that is performed by district HC centres, district nurses and mother and child care centres.
- **County care** that is performed by county hospitals and hospitals responsible for the population in geographically separated parts of the county.
- **Regional care** that is performed at the regional hospitals. This care is more specialised than the county care. Groups of counties have formed alliances and co-operate to perform this care. These regional hospitals also have educational and research facilities and belong to the Swedish Universities.

The GPs that recently have started their activity are regarded as a part of the primary care. The concepts county care and regional care are sometimes clustered and referred to as **secondary care**.

Care is carried out primarily in two different modes namely open care and closed care (outpatient and inpatient treatment):

- **Open care** means that the patient does not stay over night for treatment. This care is carried out at primary care receptions but also at county and regional care hospitals' laboratories, clinics and their sections.
- **Closed care** means that the patient is admitted at a clinic and is placed at some of the sections belonging to that clinic.

Some types of care is organised in specific ways:

- **Psychiatric care** is one concept and not divided into open and closed care. It belongs to the county responsibility.
- **Hospitals for long time care** belong to the county care.
- **Care Homes** - mostly for elderly - are run and paid by local governments.

### 1.4 Some concepts and terms

The goal for the PSHCS is a *good, safe and secure care*. *Security* has at least three aspects namely *availability, integrity and confidentiality*. This paper focuses on confidentiality and specifically *privacy* in the handling and communication of patient related information in the PSHCS.

In the health care theatre, patient related information is recorded in many types of documents as e.g. in referrals or in notes of admission or in "medical files". The concept "medical file" is in Swedish called "Patientjournal". It is a record that by law has to be written in plain Swedish. The "medical file" is perhaps equivalent to a combination of medical record, medical notes and "findings" concerning a specific patient. The concept "medical file" is used in order to separate it from the "medical record" that to my knowledge mostly contains managerial and coded information.

The introduction of the MBOS leads to, that patient related information will be specified at invoices. Specification of tests and treatments of a particular patient on an invoice can make it very sensitive.

## **2. Technological changes**

During the last years the Swedish health care system have been carried through a major change that has comprised the introduction of new paradigms and a change of ideology. This has consequently resulted in the implementation of new management tools.

The PSHCS have used EDP since the 60ies. In the beginning, the main interest concerned management systems. Most counties used economy systems for planning and budgeting as well as for control. Salary systems and planning systems in order to utilise the staff were also used. This is obvious as about 75% of the costs in the hospital area are personal costs. Patient booking systems etc. have been used a long time.

From the beginning of the 80ies central computers have been used for some kind of medical records, but the medical files have in general been on paper until the last years.

Management and medical records systems have grown larger and larger until recently. The introduction of the MBOS and the GP system (GPS) is a paradigmatic shift. It introduces buyers and sellers on a fictitious market. This leads to a genuine decentralisation of decisions and thus to a decentralisation of systems for the total Swedish HC.

The low costs and the potential power of the PCs of today accelerates this shift of structure.

Towards this background it is of course quite understandable that the use of PCs in the health care sector has evolved at a very rapid rate. Today, more than 70% of the primary care units use PCs for administrative work as well as for storage and information retrieval of medical files.

The use of PCs in the secondary care at hospital clinics is today not at all as abundant as the use in the primary care. Some clinics use computers for telemedicine and also certain laboratories use the computers for their specific purposes. The overall use is however not very large compared to the use of computers in other sectors of the Swedish society. It is expected that in one or two years we will have a boom in the use of computers also in the secondary care.

Till a few years ago and also today we store our medical files on paper, but looking at the description just given it is easy to understand that most of the new medical file information in the primary care sector will be stored in an electronic form. This implies that in a few years we will have a much larger extent of our medical files stored at electronically readable media even if we do not transfer old already stored information from the paper medical files to storage at electronically readable media.

The ethical ideas concerning privacy have not changed even if the technology to store information has changed. Thus the laws and regulations have not changed either.

How can privacy be upheld when we use this new storage technique and how can it be upheld in the era of networking and fast electronic communication?

### **3. Ethical and legal aspects**

The treatment of patient related information is carefully regulated in laws and directives. Some state agencies have also published interpretations of the laws and advises for the practical application. In order to guard the privacy of the individual the legislators have expressed very high demands. The following laws, directives and publications giving advises are applicable.

- Constitutional Act about the Freedom of Information e.g. Regeringsformen
- Act about the Freedom to Print e.g. Tryckfrihetsförordningen
- Secrecy Act ( Sekretesslagen; [SFS<sup>1</sup> 1980:100; re-printed 1989:713])
- Medical File Act ( Patientjournallagen; [SFS 1985:562])
- Health Care Act (Hälso- och sjukvårdslagen; [SFS 1982:763])
- Data Act (Datalagen; [SFS 1973:289])
- The Insemination Act ( Lagen om insemination; [SFS 1984:1140])
- The HIV Act Concerning Contagion and Criminal Offence ( Lagen om undersökning beträffande hiv-smitta i brottmål; [SFS 1988:1474])
- Forensic Psychiatric Care Act (Lagen om rättspsykiatrisk vård [SFS 1991:1129])
- Contagious Diseases Act (Smittskyddslagen; [SFS 1978:1472])
- Health Care Supervision Act (Tillsynslagen; [SFS 1980:11])

---

1 SFS is the Swedish Government Publication series for Swedish laws and regulations.

- Advises and Rules Concerning Medical Files from the National Board of Health and Welfare [SoS 1993:20]
- General Advises Concerning Personal Records from the Swedish Data Inspectorate [DI 1993:1]

The Freedom of Information is a constitutional right in Sweden.

The first chapter in the Swedish constitution Regeringsformen (RF) states that *the community shall protect the private and family life of the individual.*

The Freedom of Information Act is in the second chapter. In this chapter there is a reference to the special act about the Freedom to Print Tryckfrihetsförordningen (TF). In the 2nd chapter of the TF there is a specification about the general availability to so called "common documents". Also the concept "common document" is specified.

A "document" is a multimedia recording or part of a multimedia recording. A document is a "common document" if it is kept by an agency or if it in any sense is available for an agency. An agency is defined as the parliament, the church general assembly or any state, county or local government decision making body.

The main scope of this act is to provide the citizens means to control the authorities. The basic ideas in this act was introduced in the Swedish constitution in 1776.

If the public agencies have information about individuals this act can counteract the intentions in the first chapter of the RF to protect the private and family life of the individual. In order to see to which extent the state intends to protect the privacy of the individual it is important to look at the exceptions in the public rights to acquire information in the form of a "common document".

The rights for the public to get access to "common documents" may be limited only if it is necessary because of:

- 1 national security and Swedish relations to other states or international organisation
- 2 the nations finance policy, monetary policy or exchange rate policy
- 3 agencies' legal tasks and activities to inspect, control or supervise
- 4 the interest to forestall or fight crime
- 5 common economic interest
- 6 the protection of an individual's personal or economic conditions
- 7 the interest to sustain species of specific herbs or animals.

The Secrecy Act deals with all the points specified above in points 1 to 7. It deals with confidentiality, secrecy and privacy. The most interesting part concerning HC is point 6 above or chapter 7 that covers privacy for the individual.

The secrecy covers the health conditions and other personal conditions of the individual if it is not clear that the information can be revealed without causing harm to the individual or somebody with close relations to him. This is also valid in other medical activities as forensic medicine and forensic psychiatric investigations, insemination, establishment of sex, abortion, sterilisation, castration and measures against contagious diseases and in special activities concerning care about mentally retarded.

Secrecy is not accepted to cover a decision concerning violation of freedom of an individual if the decision is based on the act concerning forensic psychiatric care or the act concerning contagious diseases .

Information in a "common document" containing HC-information shall be kept secret for a maximum time of 70 years.

The Medical File Act [SFS 1985:562] specifies that a medical file shall contain information concerning

- 1 the identity of the patient
- 2 important information about the background to the care
- 3 information about diagnosis and the cause of more important measures
- 4 important information of taken and planned measures

The medical file must also contain information about who has made a certain notification in the file and when the notification was made. The person responsible for the information in the file shall sign the file if not certain and very specific conditions are valid.

The Health Care Act [SFS 1982:763] states that the patients to every possible extent shall be given information about his or her condition, care and treatment. The privacy and patient related information is strictly handled between the care provider and the patient.

The Data Act [SFS 1973:289] essentially concerns privacy. The law is interpreted for practical use in the information General Advice Concerning Personal Records from the Data Inspectorate [DI 1993:1].

The main idea is the "classification" of personal files into three security levels namely, basic level, high level and very high level. Each level is assigned specific means of protection in the technical as well as in the surrounding and management system.

The DI technical report [DI 1993:2] concerns security regarding person related information transmitted via facsimile explaining potential threats foreseen, and the countermeasures to be used.

## 4.The study

The study explores the handling, transmission and flow of patient related information between the medical file archives, clinics, HC-centres, laboratories and other medical service and treatment units in the respective county and between one county and other counties or regional care units.

It gives an approximate estimate of the flow between the county care units and non medical organisations, units, insurance organisations, regional and state agencies police authorities etc.

The patient related information handled by the county financial divisions, the data divisions and the archive departments has also been studied.

The study only deals with the collection of information, the registration and handling of information, the communication of information and the delivery of information. The information processing and the storage of information is not included.

A total investigation has been carried out in the counties Jämtland, Blekinge and Halland and also in the town Malmö.

<b>County or equivalent</b>	<b>Inhabitants</b>	<b>District HC centres</b>	<b>Clinical sections</b>	<b>Service units</b>	<b>Response rate</b>
Blekinge	150 000	13	13	9	70%
Halland	260 000	28	77	-	71%
Jämtland	135 000	28	55	-	67%
Malmö	237 000	15	91	10	55%

This table gives a view of the sizes of the actual counties.

The response rate has been rather good except in Malmö. This is because of a reorganisation that took place in January and in February 1994 when the questionnaire was sent out. In order to increase the response rate, new questionnaires were sent to those who did not answer the first time. A telephone call followed for those who did not answer the second time. The reasons for not answering was mainly referred to as work overload. If this is reality or if there are other reasons are difficult to judge. The low response rate in Malmö indicates that the results from Malmö must be treated with special care, especially if conclusions differ from the those in the other regions.

The questionnaire was intended to be answered by either a physician, a nurse or a physician's secretary. In some cases more than one person from these categories have been involved and they have answered the questionnaire together.



County or equivalent	Med. doctor	Nurse	Physician's secretary	Combination of categories
Blekinge	19%	0%	58%	23%
Halland	8%	29%	44%	19%
Jämtland	13%	25%	41%	21%
Malmö	14%	14%	39%	33%

The different categories that have answered the questionnaire is regarded not to have influenced the results in any specific direction as all these categories have a very good knowledge of the issues treated.

In Blekinge no nurses answered the questionnaire. This deviation has not been investigated especially, but the explanation can be that the study in Blekinge got much more support from the county administrators than the studies in the other counties.

## 5. The evaluation model

The evaluation model created is based upon the directives and rules deduced from the valid laws quoted. As is easily understood from the description given they are difficult to interpret in an unambiguous way. In order to grasp the problem and to get a better overview, the evaluation is structured in four domains in order to make an easier comparison with the requirements set up by the legislator.

The domains are:

- work routines at handling of medical files and referrals
- information channels used for data transfer
- ethical questions
- volumes of information. (Not reported in this paper.)

### 5.1 The work routines

The work routines are divided into the delivery of medical files, the delivery of referrals, the reception of medical files and the reception of referrals. The following rules apply.

#### 5.1.1 The delivery of medical files

- The person that asks for a medical file or part of a medical file must always be identified. The Medical File Act {MFA}<sup>2</sup>§7
- The basic rule is that the person responsible for the medical file must decide about the delivery. MFA §11.

---

<sup>2</sup> For the readers convenience acronyms are used here instead of formal references.

- There are six cases when a medical file is allowed to be delivered, left out or disclosed namely
  1. the consent of the patient (the Secrecy Act {SA} 14:4).
  2. emergency situations (SA 1:5)
  3. if it is necessary in order to make it possible for the delivering agency or care-giving organisation to perform it's obligations for instance if the care-giving organisation has got a referral and has to report back (SA 1:5)
  4. if the care-giving organisation is obliged to deliver the information according to law or directives (SA 14:1)
  5. if the medical file can be delivered without direct or indirect harm to the patient or his or her relatives (SA 7:1)
  6. if the information has been depersonalised (MFA §11)
- The content of the medical file must be scrutinised from confidentiality principles before delivery. (MFA §11).
- The receiver's access rights and need to use the information in the medical file must be controlled.(MFA §§7 and 8).

#### **5.1.2 The delivery of referrals**

- Until recently no demands have been expressed concerning equipment or methods in the delivery of referrals. The National board of Health has however recently, more to confirm practices in some areas, stated an equivalence between referrals and medical files in this respect [SoS 1993:20].

#### **5.1.3 The reception of medical files**

- From security and privacy reasons the facsimile transmissions are of special interest. If the receiving facsimile equipment is not placed in a closed and sealed area it should be of the SEAL-fax type that automatically puts the received facsimile in an envelope. (MFA §7)

#### **5.1.4 The reception of referrals**

- As specified in section 5.1.2, no demands have until recently been expressed [SoS 1993:20].

### **5.2 Information channels used for data transfer**

The general responsibility is shared between the sending and the receiving part so that the sending part is responsible for the security for the information transferred and for situations that can happen depending because of failures in the transmission. The receiving part is responsible for the security of the received information. The possibility to utilise an eventual trusted third party to take care of the transmission is not discussed.

Concerning information channels the general rule is that sensitive patient related information shall be transferred so that only the receiver is given access to the information. At internal distribution within an hospital the transmission is recommended to take place in closed envelopes and in external transmissions registered letters are recommended.

The Data Inspectorate (DI) has published directives and recommendations concerning facsimile and electronic data transmissions [DI 1993:1]. As already said the DI gives the directive that information shall be divided in three sensitivity levels with respect to confidentiality and the DI also specify that very sensitive information **must be encrypted** during transmission.

### **5.3 Ethical questions**

The ethical question are in a way treated when the DI's directives are quoted as they say that information shall be divided into sensitivity levels with respect to confidentiality. In the PSHCS, the practice have so far been that within each clinic all professionals have access to all information. This is a kind of "horizontal" division of information in different groups with no "vertical" sensitivity level division. In the questionnaire we ask the PSHCS about this "vertical" division.

## **6. Results**

The general overall analysis indicates that there are not any significant differences between the treatment of information by the with respect to security counties. Some differences can however be notified. In this paper I will only give the broad and significant results the details will be published later. In the interviews different subjects and special questions have been discussed depending on the administrative and organisational situation in each county. Some of these are taken up here.

### **6.1 The delivery of medical files and referrals.**

From the investigation it seems that the delivery of referrals and medical files are harmonised even if the regulation about this harmonisation had not been enforced before our investigation. Here I only show the delivery of medical files for delivery. Referrals and other documents will be treated elsewhere.

In section 5.1.1. five absolutes were specified to fulfil the legal obligations.

1: Identification; 2: Decision about delivery; 3: Scrutinisation; 4: Access rights; and 5: Need of information.

County or equivalent	Identification	Decision of delivery	Scrutini-sation	Access rights	Need	Over all
Blekinge	76%	83%	83%	73%	9%	3%
Halland	57%	96%	77%	83%	33%	12%
Jämtland	70%	91%	88%	52%	20%	6%
Malmö	43%	95%	84%	50%	11%	2%

This table shows the relative numbers of respondents saying that they **always** identify the person asking for information and that they **always** use the physician in charge to decide about whether to disclose information or not. They also **always** scrutinise the information so that nothing that can harm the patient or his relatives is disclosed. They also **always** make themselves fully aware about the access rights of the receiver to the information and at last they **always** clarify that the receiver has the need for the information sent.

The questionnaire also contained the alternative **often**, and if that is included the situation looks better, but of course then the stringency of the behaviour is less tight.

It is interesting to note that the figures in Malmö mostly are lower than most of the other figures. In the over all figure made as a multiplication of all the five figures show, that if the absolutes are statistically independent only 2% in Malmö; 3% in Blekinge; 6% in Jämtland and 12% in Halland carry out a complete inquiry before medical file information is delivered.

The regulations to protect the patient's privacy seem not to be implemented to the extent intended by the legislator. In spite of this there is in practice no complaints about the handling of the medical file information with respect to privacy. Does this mean that the demands from the legislators are higher than necessary or is the risk negligible? How is the development of risk, threat and vulnerability when the medical files are connected to the communication networks?

## 6.2 Information channels used for data transfer

The channels for transference of information has been investigated in many dimensions, and I will also present overhead pictures showing the complex picture, but the most frequently used media are internal mail with sealed envelopes, external mail as ordinary letters, internal mail with open envelopes, facsimile, patients that bring the information in open or sealed letters, registered mail, special systems and electronic mail. Of the respondents about 50% often use sealed internal mail, about 25% often use ordinary mail and about 10% often use facsimile transmission.

The difference in volume of information (no:s of characters) sent on paper and in electronic mail cannot be accurately estimated. However the electronic mail involving medical files is practically zero in spite of the fact that medical files is the largest category of information sent.

### 6.3 Ethical questions

The questions put are: Is it your opinion that

- 1 it is important to classify patient related information in different sensitivity classes?
- 2 access to differently classified sensitive patient related information shall be dependent of your position or task?
- 3 the laboratory data belonging to one patient shall be accessible for all clinics at an hospital?

The answers are guided to be yes or no and the respondent are requested to motivate his or her answer.

County or equivalent	Classification of info	Classification of access	Reuse of laboratory results
Blekinge	92%	100%	69%
Halland	79%	96%	63%
Jämtland	68%	70%	61%
Malmö	75%	92%	92%

This table shows the relative numbers of respondents saying yes to the questions.

There is a great majority in favour of sensitivity classification and separation of information to personnel with different tasks or positions. There is also a majority in favour of reuse of laboratory results even if the legislation is restrictive about this.

Their motives are placed in different order. One class of motivations is that it is more convenient and less pain for the patients if they can be cured with fewer tests taken. The other class is that answers can be given faster if information is shared and this is of course good for effectiveness, efficiency and thus for hospitals economy. Some say that this is acceptable for non sensitive tests, but not for tests concerning very specific diseases, drug abuse tests and HIV tests.

## 6.4 Interviews with data, financial and archive departments.

These interviews have given some interesting views. However the most remarkable result is that in at least one of the counties some invoices contained full information such as the identity of the patient as well as the DRG related information. This was clearly privacy threatening. Actions have already started to overcome this problem.

### References

- [DI1993:1]           Datainspektionen "ADB-säkerhet för personregister"  
[DI1993:2]           Datainspektionen "ADB-säkerhet för personuppgifter vid  
                          telefaxöverföring"  
[SFS1973:0289]       Datalagen = The Personal Records Act (The Swedish Data Act)  
[SFS1978:1472]       Smittskyddslagen = The Act Concerning Contagious Diseases  
[SFS1980:0011]       Tillsynslagen = The Health Care Supervision Act  
[SFS1980:0100]       Sekretesslagen = The Secrecy Act  
[SFS1982:0763]       Hälso- och sjukvårdslagen = The Swedish Health Care Act  
[SFS1984:1140]       Lagen om insemination = The Insemination Act  
[SFS1985:0562]       Patientjournalagen = The Medical File Act  
[SFS1988:1474]       Lagen om undersökning beträffande hiv-smitta i brottmål  
[SFS1989:0713]       Sekretesslagen = The Secrecy Act (new edition)  
[SFS1991:0187]       Datalagen (ändring/change)  
[SFS1991:1129]       Lagen om rättspsykiatrisk vård = The Act Concerning Forensic  
                          Psychiatric Care  
[SoS1993:20]         Socialstyrelsen "Råd och föreskrifter angående patientjournalagen"

## COMPUTER CRIME ON THE INTERNET

The panel on Computer Crime on the Internet will approach the issue of Internet connectivity from a practical standpoint in terms of risks. Much has been made of the advantages in connecting a government system to the Internet. Without doubt, some advantages exist. However, risks to computer systems exist as well.

Attendees to this panel should walk away with specific information regarding the basic types of vulnerabilities often experienced after an organization connects to the Internet. Examples of specific problems and solutions will be given. The purpose of this approach is to give computer professionals the tools they need in order to prepare for a connection to the Internet and to anticipate potential difficulties. In addition, pointers on obtaining user cooperation and upper management support for computer security will be outlined.

Perspective comes from a broad overview of the problem in question, highlighted with specifics. This panel will provide that overview of computer crime on the Internet by addressing the issue from several different angles.

The panel will begin with a presentation of a research paper entitled "How To Solve the Hacker Problem," setting the stage for a further look into combatting computer crime from other perspectives. Next, computer crime will be discussed from the perspective of someone investigating computer crime. The specifics of what types of information are required for a successful case to be made against a computer criminal will be given at this time. After that presentation, a federal computer systems manager will discuss specific computer security problems his agency experienced after permitting Internet connections. Ideas will be proposed in terms of preventative measures and selling computer security to upper management. Next, a representative from the Computer Emergency Response Team will discuss their role and initiatives in dealing with Internet computer crime. The presentation will provide a summary of current trends and highlight their impact on managers, systems administrators, and users. Lastly, two representatives from a major Internet access provider will speak on the subject of Internet computer crime, from a management and technical viewpoint.

Mr. Donn Parker -

Mr. Parker, a senior management consultant, has spent 24 years in the computer field at SRI International working in information security. He is the founder of the International Information Integrity Institute (I-4), continuously serving more than 60 of the largest multinational corporations in the world for over eight years in the protection of their information assets. Mr. Parker has led National Science Foundation grant-funded studies on ethical conflicts in computer science, technology, and business in 1977 and 1987. He is a world renowned consultant, lecturer, writer, and researcher on computer crime and security and has addressed, for example, the Commonwealth Club of San Francisco. He has written five books on computer crime, ethics, and information security management. Mr. Parker is the Consulting Editor of The Journal of Information Security published by Auerbach starting in 1992. He was awarded the 1992 ISSA Individual Achievement Award, the 1994 National Computer Security Award from the NIST/NCSC, and the Aerospace Computer Security Associates 1994 Distinguished Lecturer Award.

Mr. Parker will discuss in detail the psychological motivations of malicious hackers. He will describe the different types of individuals who engage in malicious hacking, and their respective motivations. His presentation will also address specific solutions to this problem, based on his research.

Mr. Mark Pollitt -

Mr. Pollitt is a Special Agent with the Federal Bureau of Investigation. He is assigned to the Baltimore Field Office where he serves in two capacities. He is assigned investigative responsibilities for Computer Crimes and Copyright Violations. Agent Pollitt is a Field Examiner for the FBI Laboratory's Computer Analysis and Response Team. As such, he conducts laboratory examinations of digital evidence in the full range of FBI cases.

Mr. Pollitt will discuss the roles and responsibilities of the victim organization and the investigator. The investigative process and the essential elements of an investigation will be discussed. Particular emphasis will be placed on Internet related crimes.

Mr. Ted Chambers -

Mr. Chambers is the Manager of Scientific Computer Support Team at the Center for Food Safety and Applied Nutrition (Food and Drug Administration). His office is responsible for handling computing for lab networks and equipment, and math modeling. He acquired responsibility for Internet security at the FDA after a scientific workstation was the first FDA computer to be hit with a virus.



Experiences and challenges of the FDA with Internet security will be presented. Both technical and non-technical issues will be discussed in addition to some of the resulting security procedure modifications required by Internet connectivity. This will encompass issues such as system validation prior to Internet connections, and measures to help prevent future incidents. Issues such as administrative procedures and getting upper management commitment to security, user cooperation, and dealing with a limited budget will also be addressed during this presentation.

Ms. Barbara Fraser -

Ms. Fraser is the manager of the Security Improvement Program for the Computer Emergency Response Team Coordination Center (CERT), located at Carnegie Mellon University, in the Software Engineering Institute. Her responsibilities include the planning and development of security-related products. Ms. Fraser has given many talks and classes on CERT and Internet security, and she has worked with many organizations to help them understand security issues as they relate to the Internet.

Ms. Fraser is active in the security area of the Internet Engineering Task Force and was one of the authors of RFC 1281, "Guidelines for the Secure Operation of the Internet."

Mr. Martin Schoffstall -

With the emergence of the Internet as a public data network, privacy and security has been moving towards the top of the list of concerns for the network manager. Performance Systems International (PSI) has been providing Internet services since January of 1990 and has been providing security solutions to its customers from the start.

Mr. Schoffstall is a recognized national leader in networking design, engineering operations, and technology. Currently, he is Vice President and Chief Technical Officer for PSI. His engineering experience at Bolt Beranek & Newman during the Internet's formation, his degrees in computer science from Rensselaer Polytechnic Institute, and his work with selected computing and networking start-up companies, give him unequalled insight in how to manage and market technology. He was co-founder and Vice President for Research and Technology of NYSERNet, the New York State education and research regional network. In 1991, Mr. Schoffstall was named as one of the top 25 "network visionaries" honored by Communications Week, a trade publication of the telecommunications and networking industry.

Mr. Mark Fedor -

Recently, Performance Systems International (PSI) started providing Internet service over a CATV system in Cambridge, MA. In an environment such as this, security is a major concern since all CATV subscribers potentially have access to all data being sent over the CATV system. The issues regarding the provision of secure Internet data over a CATV system will be explored.

Mr. Fedor is currently the Special Projects Manager at Performance Systems International. This entails the research and integration of new technologies into the PSINet. Prior to joining PSI in 1990, Mr. Fedor was a member of the technical staff at NSYERNet where he co-authored the Internet Standard Simple Network Management Protocol (SNMP). From 1986 through 1987, he was a member of the networking group at the Cornell Theory Center which developed and operated the first phase of the NSFNet backbone. While there, Mr. Fedor designed and implemented the first multi-routing protocol process for the NSFNet backbone which is still in use today. Mr. Fedor has a BS in Computer Science from the State University of New York at Oswego.

Do You Have the Skills to be Future INFOSEC Professionals?

Panel Members

Dr. William (Vic) Maconachy (**Chair**)  
Deputy Director  
INFOSEC Professionalization  
Center for Information Systems Security

Mrs. Genevieve Burns  
Manager, Data Security  
Monsanto Corp.  
(President ISSA)

Mr. Robert Morris  
Senior INFOSEC Advisor  
Information Systems Security Organization  
National Security Agency

Dr. Corey Schou  
Director, SIMPLOT Decision Support Center  
Idaho State University

**ABSTRACT:** INFOSEC is changing in ways that profoundly affect the skills required of persons who consider themselves professionals. The work force of tomorrow will be smaller, and each individual will carry increased levels of responsibility. This panel examines the types of skills that will be needed to cope with the changing work environment, and what types of individual initiatives are required to keep up with advancing technologies and management challenges.

-----

A Recognized Problem

*The Commission Also believes that there is a need to improve the quality and number of information systems security professionals and to increase training and awareness programs for management and non-security personnel.<sup>1</sup>*

The above statement by the Joint Security Commission is both an indictment and a challenge. The finding is an indictment because it echoes findings of past reports. It presents a challenge because analyzing, defining, developing and delivering education and training in the INFOSEC arena is inexorably tied to the pace of

---

<sup>1</sup>Joint Security commission. Redefining Security: A Report by the Joint Security Commission. Washington, D.C. Feb. 28, 1994.

technology turn over. This challenge is also coupled to additional corporate and government concerns. The 'rightsizing' and 'downsizing' within both government and industry has placed an increasingly heavy emphasis on organizational quality. One of the basic precepts of organizational quality is 'do the Right Job - Right'. To do this, the right job must be identified and the process to do it the right way must be codified.

In the area of information systems security this identification and codification has been difficult since there has been little consensus about either the job or the process. This lack of consensus is attributable to a fundamental conflict - information systems security is frequently viewed as antithetical to the primary function of information systems. Corporate and government information managers must balance their obligation to make information available to all authorized users - while maintaining confidentiality, integrity and trust during transmission, storage and processing. Organizations want ubiquitous and unobtrusive information security measures. The information systems security professional must have some way of meeting that objective while maintaining an open system. His/her security measures have been categorized as encompassing three dimensions (1) policy and practice, (2) technical measures, and (3) education and training.<sup>2</sup> His or her first, and perhaps the least expensive, way of meeting the organizational INFOSEC objective is through work force awareness, training, and education.<sup>3</sup>

#### The Increasing Scope of the Problem

*An Electrical failure knocked out computers supporting the over-the-counter stock market here two weeks ago and brought trading to a virtual standstill for 1 1/2 hours.*

*Network World, Dec. 21, 1987 p 15*

*During the Persian Gulf War a British Royal Air Force Officer left a notebook computer in his automobile and went shopping. The notebook was stolen along with the data in it - including a copy of preliminary Allied invasion plans.*

*Datamation, March, 1992 p 43*

The information systems security problems facing organizations are constantly increasing in both scope and complexity. For

---

<sup>2</sup>McCumber, John. Proceedings of the 14th National Computer Security Conference. National Computer Security Center. p 334, October, 1991.

<sup>3</sup>Maconachy, W.V. "Computer Security Education, Training, and Awareness: Turning a Philosophical Orientation Into Practical Reality." Proceedings 12th National Computer Security Conference. National Computer Security Center, pp 557 A-I. October, 1989.

example, as the frequency with which American business and its industrial base enter international markets, new opportunities will arise. Mitchell<sup>4</sup>, as quoted in Computers At Risk predicts:

*Through open systems interconnection (OSI), business will rely on computer networks as much as they depend on the global telecom network. Enterprise networks will meet an emerging need: they will allow any single computer in any part of the world to be accessible to users on any telephone. OSI networking capabilities will give every networked computer a unique and easily accessible address. Individual computer networks will join into a single cohesive system to form one global service.*

These opportunities also represent new threats and problems for management. Although Mitchell discusses the future, our increasingly high dependence on networks and interconnected systems has already begun. One prime example of growing interdependence is INTERNET, the unclassified network of national (30 countries) computers and networks that has over 2,300,000 hosts worldwide representing 30,000 domains. There may be as many as 25 to 27 million users at the moment. In addition, there are over 15 million data packets on the NSFNET of over 5,000 networks. The interconnection of these computers and networks will have over 50 million computers by 1995. Collectively these networking activities form the base for the much discussed National Information Infrastructure (NII). The NII has been described by some as 'INTERNET times 1,000'.

It is critical that information systems security professionals and their colleagues in other areas, such as accounting, convey, through corporate IRM activities, the importance of information resources security to all employees and other individuals with access to organizational information resources. The entire information systems staff must be involved in the reaction of new organizational paradigm for information resources security - it must not be just a set of rules and procedures; it must become an integrated component of corporate culture.

#### Making Information Security Part Of The Organizational Culture

To be effective, information security must become part of the organizational culture. In addition, it must be developed by using a structured model that allows management to make sound decisions based on complete information. Practitioners in almost any area frequently believe that the view of their profession from the academic white tower is clouded at best, and that the government provides more interference than help. Recent cooperative

---

<sup>4</sup>\_\_\_\_\_. 1991. Computers At Risk: Safe Computing In The Information Age.

activities may change those perceptions. Over seventy-five individuals from government, industry, and academia have worked directly with a process called an electronic DACUM (Design A Curriculum) to assist all information security professionals by developing effective and efficient methods for improving the information security of all organizations.

The first step in developing a structured model has established a working definition of the elements of the problem. The DACUM groups used the ETCORP<sup>5</sup> process first to create a structure for analysis and then to complete the details. The DACUM activities have provided:

- .a point of departure for organizations needing to improve their information security
- .a recognized philosophical framework for operations
- .a potential arbiter of bureaucratic lines of control; and
- .a tool for planning awareness, training, and education activities appropriate for differing levels of learning.

Further, a structured model helps managers differentiate between security awareness, training and education in programs early in the campaign for excellence in security behaviors. To aid management in acting on AT&E recommendations, the DACUM groups have applied an extension known as Instructional Systems Design (ISD). This technique is an iterative analysis, design, implementation and quality control process and has proven cost effective for transferring knowledge and skills which is used throughout government and industry.

DACUM sessions have resulted in a new, structured way of looking at the first line of defense. The participants cited information systems and the security associated with them as a "core competency" in business, industry and government restructuring. They accepted the Prahalad and Hamel<sup>6</sup> reference to corporate core competencies as the "Roots of Competitiveness." Once it was agreed upon that information systems security was a core competency, it was important to develop a model for transferring knowledge about the contents of this core competency.

Other DACUMS, compiled, distilled and enhanced existing attempts by a variety of organizations to define a Common Body of Knowledge (CBK) for information systems security practitioners and professionals. The participants then defined a taxonomic structure for the contents of the CBK elements. After the CBK elements were

---

<sup>5</sup>Schou, Corey D., J. Frost, N. Wingert.H. Lafond. "Enhancing Productivity and Quality Using Collaborative Organizational Re-Engineering and Paradigm Change Processes." Proceedings of the Association of Management. Atlanta Georgia, August 1993

<sup>6</sup>C.K. Prahalad and Gary Hamel, "The Core Competence of the Corporation." Harvard Business Review. May-June 1990.

placed in this taxonomy, appropriate knowledge, skills, and abilities (KSAs)<sup>7</sup> were associated with each of the CBK elements. Finally, verbs from Bloom's<sup>8</sup> hierarchy were assigned to each KSA. This step allows for behavioral objectives to be written.

Generally, a common body of knowledge represents a relatively stable body of knowledge encompassing the axioms, lore and methods of the trade. As implemented, a CBK represents that body of knowledge that is integral to the manner in which an information security professional performs his/her job.

The CBK outlined in this report condensed over 1100 individual items into a listing of 385 behavioral descriptions. To do this the DACUM group had to establish a taxonomy. Those descriptions are partitioned into two major taxonomic categories:

- . Things You Need To Know: and
- . Things You Need To Do.

The resulting Unified Taxonomy can be used as a reference point by both curriculum developers and authors. This taxonomy codifies, for the moment, those knowledge, skills and abilities (KSA) which define the core information for all practitioners, regardless of individual areas of expertise. The Unified Taxonomy also serves as a guide to job classification, career development and professionalization activities.

#### Information Systems Security Professionals

The security professional plays a central role in the information intensive environments of today's government and business. He/she has a multi-level task that seems to be associated with complexity and size of the networks controlled rather than any specific position he/she occupies in the organizational hierarchy. The DACUM results have identified that the associated tasks are very technical in nature.

Since the CIO is the top of the responsibility hierarchy. He/she must be made aware that information security serves a critical organizational mission and that it can not be an afterthought. In addition, the CIO must communicate the criticality of information systems security to both peers and superiors in the organization. The CIO should be made aware of the

---

<sup>7</sup>Knowledge- A broad comprehension of a subject that cannot be necessarily be applied. Skill- Comprehension of a subject that is or can be specifically applied. Attribute- personality characteristics which is or can be developed to enhance job performance.

<sup>8</sup>Bloom, Benjamin. Taxonomy of Educational Objectives: Cognitive Domain. New York, David McKay, Co. Fifty-Seventh yearbook. Part II, National society for the Study of Education. Chicago University of Chicago press.

AT&E pyramid and be provided with structured information that allows him/her to allocate resources for information security to AT&E activities in an effective manner.

The first step in renewing and revitalizing an information systems security program should be to review all training completed within the organization in the past two years to see if it meets the basic suggested structure. At a minimum, every organization should have activities available at all three levels of AT&E. The optimal solution is for an organization to be future oriented in its INFOSEC training posture. Our data indicates that INFOSEC professionals must be able to:

- exercise increased interpersonal and business communications skills.
- examine the risks associated with the introductions of new technologies.
- develop reports that are thorough, accurate, and yet readable/understandable by non-technical decision makers.
- practice risk management rather than risk avoidance.

The new technologies, often "riding" the NII, will include migration from existing network technologies to Asynchronous Transfer Mode (ATM) based systems. By 1996 INFOSEC professionals will be coping with sophisticated multi-functional internetworking devices some are terming the fifth generation intelligent hub. These hubs introduce artificial intelligence software in the network management module as well as incorporate wireless technology into the bridge modules. Are you prepared?



## 17th National Computer Security Conference

**Panel Title: Computers At Risk (CAR) Recommendations:  
Are They Still Valid?**

**Panelists:**

Hal Tipton, CISSP, President - HFT Associates (Chairman)  
Will Ozier, President - Ozier Peterse & Associates  
Earl Boebert, Secure Computing Corporation  
Steve Walker, President - Trusted Information Systems

**Panel Summary:**

The Computer Science and Telecommunications Board of the National Academy of Science formed the Systems Security Study Committee in response to a fall 1988 request from the Defense Advanced Research Projects Agency (DARPA) to address the security and trustworthiness of U.S. computing and telecommunications systems. The committee report, Computers At Risk (CAR), issued in December 1990 contained six recommendations designed to increase the levels of security in new and existing computer and communications systems.

1. Promulgation of a comprehensive set of Generally Accepted System Security Principles, referred to as GSSP, which would provide a clear articulation of essential security features, assurances and practices.
2. A set of short term actions for systems vendors and users that build on readily available capabilities and would yield immediate benefits.
3. Establishment of a system-incident data repository and appropriate education and training programs to promote public awareness.
4. Clarification of export control criteria and procedures for secure or trusted systems and review for possible relaxation of controls on the export of implementations of the Data Encryption Standard (DES).

5. Funding and directions for a comprehensive program of research.
6. Establishment of a new organization to nurture the development, commercialization, and proper use of trust technology, referred to as the Information Security Foundation, or ISF.

The continued validity of each of these recommendations will be reviewed and discussed. Significant progress has been made to achieve the GSSP (Recommendation 1) and this will be reported. Some initial efforts to establish the ISF (Recommendation 6) were underway but slowed due to the weak economy. The status and potential of this recommendation will be discussed.

Ozier Statement:

A group of IT industry leaders, convened at the request of the National Research Council (NRC), determined that a number of measures must be undertaken if Information Security, from both professional and product issues perspectives, was going to cope successfully with the rapid evolution of IT. In their report *Computers at Risk (CAR)*, NRC '90, they made several key recommendations. First among these recommendations was to develop and promulgate Generally Accepted System Security Principles (GSSP's) emulating the GAAP (and international parallels) and its relationship to the accounting profession. As a direct result of that recommendation, the ISSA-sponsored GSSP Committee was formed and has been hard at work for the past two years laying the ground work for this important initiative. This presentation will give you an overview of the background of the initiative as well as its goals, objectives, approach, and current status.

Boebert Statement:

The world has undergone a profound change in the three short years since the recommendations were made in *Computers At Risk*. The disintegration of the Soviet Union, the availability of strong cryptography in the public domain, and the explosive growth in the Internet have all served to make us rethink our work in that document.

Looking back, I find the first recommendation, the establishment of the GSSP, to be even more valid than when it was made. Global interconnection has led to global vulnerability, but we face situations where decision-makers have great difficulty determining what constitutes a basic standard of due care in protecting information assets.

These decision-makers will not be substantially aided by the establishment of government-mandated technical criteria for "secure" computers; indeed, it can be argued that such criteria are counterproductive in that they further the idea that security is something extra, the provenance of a closed priesthood, somebody else's problem. In fact, it is integral to operating a contemporary information system in the Internet era.

Instead, these decision-makers need a GSSP, arrived at by consensus, adapting quickly to technological change, and crisply enunciated. Only then, in my view, will we have enough consistency of practice to enable security concerns to permeate the design and operation of leading networks the way quality concerns permeate the organization and processes of leading corporations.

#### Walker Statement:

In 1990, the Computers at Risk NRC Study Group promulgated six comprehensive recommendations for the information technology industry that have even more relevance today than they did in that very different world. The amazing growth of commercial interest in networking and of the Internet as a focus for the National (and International) Information Infrastructure demonstrates the ever growing need for sound information security principles.

The GSSP as an industry wide statement of reasonable information security practice, akin to the accounting world's GAAP, is desperately needed. The practice of delivering commercial systems to the customer in an "unsafe" manner must be corrected. FIRST, CERT and the various specific crises groups have made progress but much remains to be done. The export control situation for both cryptography and trusted systems has received a lot of attention lately but remains a painful reminder of the issues of balancing the national (and international) economic and security interests. There is always a need for more fundamental research in how to build stronger and more useful systems. The current trends toward more

applied research push progress toward fundamental issues further away. We need to better articulate where and how research progress can be made before we can justify expenditures on the more basic topics that we know we need. And, finally, the need for some sort of organization, outside of the government, that can help oversee all this and provide direction and control is more important than ever.

How we should go about doing all this is a vital topic of the day and I look forward to this panel discussion possibly sparking a new and revived effort to find solutions to these most difficult topics.

**COMPUTERS AT RISK (CAR) RECOMMENDATION: ARE THEY STILL VALID?  
OBJECTIVES AND PROGRESS OF THE GSSP COMMITTEE**

*The ISSA - Sponsored Committee to Develop and Promulgate  
Generally Accepted System Security Principles (GSSP)*

**BACKGROUND:**

The GSSP Committee formation was initiated in mid 1992 in response to Recommendation #1 of the report "Computers at Risk" (CAR), published by the National Research Council in 1990. That recommendation, "To Promulgate Comprehensive Generally Accepted System Security Principles (GSSP)", and its subordinate elements sparked the genesis of a concerted effort to establish a well-balanced committee population representing key elements of the private and public sectors from both the US and abroad. Both professional and product-related principles are being addressed, and, to consolidate all the elements of a rapidly maturing - explosive - industry, links are being established to the Information Systems Certification Consortium and the internationally coordinated effort to develop the Common Criteria (product-related security principles).

In order to effectively consolidate and sustain the value of comprehensive GSSP, the CAR recommendation envisions the creation of an authoritative infrastructure to maintain the GSSP, support their evolution, enforce "compliance", and provide a vehicle for the authoritative approval of reasonably-founded exceptions or departures from GSSP. This authoritative infrastructure would be modeled after those that support and sustain the GAAP and like models of the accounting profession.

The kickoff GSSP Committee meeting was held in conjunction with the 1992 NCSC in Baltimore, MD, and was attended by twenty-five of the leading information security experts from the US, Canada, the UK, France, Germany, the Netherlands, Sweden, and the CEC. Many differing perspectives and agendas were discussed in an open exchange, but at the close of the meeting, it was the consensus that the objectives were important, necessary, and, perhaps most significant, doable.

**APPROACH:**

Rather than another carte-blanc effort, the Committee determined to establish an Authoritative Foundation of existing works and works-in-progress that, through their broad acceptance, have articulated, in one way or another, the GSSP's of the information security profession. Recognizing the hierarchic nature of principles, it was determined to use the OECD Principles as the model for top of the hierarchy - Pervasive Principles - and, through a careful analysis and mapping of the Authoritative Foundation and derivative works, to develop Broad Operating Principles and Functional Principles, as accepted and supported by a consensus of the IT industry and profession.

Thus, the development of a consensus-building process is central as well to the success of this approach. Other key tasks include the establishment of linkages to the Common Criteria effort currently under way and the Information Security Certification Consortium also currently under way.

Finally, are two elements, the development of which, while clearly essential, will be more evolutionary in nature. Their purpose will be to establish the "glue" that effectively binds the consolidation internationally of these complex issues. The first of these is the definition and establishment of an authoritative infrastructure or governing body (bodies?). Second is the development of models for legislative/regulatory initiatives that have the support of the profession, industry, and government.

#### **OBJECTIVES:**

- o The international harmonization of culturally neutral information security.
- o The elimination of artificial barriers to the free flow of information world-wide.
- o The definition and implementation of a principled foundation for an industry, the success of which is critical to the future of the Information Age and its ramifications for privacy and security.
- o Provision for the rapidly evolving nature of information security methods, issues, and technology, and their articulation in principle.
- o Recognize and address related management issues.

#### **WHAT THIS MEANS IN THE CONTEXT OF DEVELOPMENTAL ASSURANCE:**

- o Broad substantiation of a common array of control principles in the world-wide IT community.
- o World-wide acceptance of the common array of controls.
- o Elimination of artificial barriers that may arise from independently developed control structures.
- o Improved manageability of IT control for privacy and security.
- o More efficient and cost/effective development and implementation of controls.
- o Professionalization of the field of Information Security - at an opportune time.
- o Better understanding of information security issues between users/owners, custodians, and auditors.

## **CURRENT STATUS:**

The Vice President's NPR Task Force has recommended that NIST (a Committee member), with advise from NSA (also represented) and OMB, develop GSSP for the Federal Government. The Committee and NIST have met with ARPA and prepared a joint proposal and project plan to secure funds that will enable the Committee to accelerate its efforts and develop GSSP that NIST, in turn, can adapt in response to its NPR task. The GSSP Committee is meeting here in conjunction with this workshop to review/approve the plan/proposal. A grant administrator as well as working Committee members have been identified and are standing by. Draft Pervasive Principles based on the OECD Principles have been developed and are being submitted to the Committee for review/approval, as is a fully articulated Outreach and Awareness Program.

Core tasks of the project in this phase are as follows:

- o Execute the Outreach and Awareness Program
- o Research and Complete the Authoritative Foundation
- o Map the Authoritative Foundation
- o Extract and Define Broad Operating Principles and Functional Principles and Map to Draft Pervasive Principles
- o Define the Consensus Process as I (Intra-Committee) and II (IT Community)
- o Define/Establish Linkage with the ISC<sup>2</sup>
- o Define/Establish Linkage with the Common Criteria Project
- o Define the framework for an Authoritative GSSP Infrastructure
- o Plan Execution of Consensus II for GSSP's - Outyear 1
- o Plan Development of Detailed Principles - Outyear 1

## **TIME FRAME:**

This will include a brief discussion of the time frame within which this phase of the GSSP Project will be executed and expected time frames for out-year tasks and plans:

### **1994:**

- o Initiate and maintain Outreach and Awareness
- o Research and Complete the Authoritative Foundation

- o Define Consensus Process I and II
- o Define/Establish Linkage with ISC<sup>2</sup>
- o Secure Funds/Support for Accelerated Activity

**1995:**

- o Map Authoritative Foundation to Draft Pervasive Principles
- o Extract and Define Broad Operating Principles and Functional Principles and Map to Pervasive Principles
- o Define the Framework for an Authoritative GSSP Infrastructure
- o Plan Execution of Consensus II for GSSP's
- o Plan Development of Detailed Principles

**1996:**

- o Execute Consensus II on GSSP's
- o Initiate Development of Detailed Principles
- o Infuse/Fund Authoritative Infrastructure



# NCSC/NIST National Computer Security Conference Tutorial Series On Trusted Systems & Operational Security

Presented by:

*R. Kenneth Bauer*  
*Joel Sachs*  
*Dr. Eugene Schultz*  
*Dr. Gary Smith*  
*Jeff Williams*  
ARCA Systems, Inc.  
8229 Boone Blvd.  
Vienna, VA 22182  
703-734-5611

*Chris Bressinger*  
DoD Security Institute  
8000 Jefferson Davis Hwy.  
Richmond, VA 23297  
804-279-3174

*Dr. Charles Abzug*  
*LtCdr Alan Liddle, Royal Navy*  
Information Resources Management College  
National Defense University  
Fort Lesley J. McNair  
Washington, D.C. 20319  
202-287-9321

## Schedule

	Tuesday 11 Oct 1994	Wednesday 12 Oct 1994	Thursday 13 Oct 1994
0900 -1030	Opening Plenary	Trust Concepts <i>Dr. Charles Abzug, IRMC</i>	Unix Security <i>Dr. Eugene Schultz, ARCA</i>
1100 - 1230	Opening Plenary	Trusted Networks <i>R. Ken Bauer, ARCA</i>	Windows NT Security <i>Jeff Williams, ARCA</i>
1400 - 1530	Security & the Future <i>LtCdr Alan Liddle, IRMC</i> <i>Joel Sachs, ARCA</i>	Trusted Databases <i>Dr. Gary Smith, ARCA</i>	System Security Engineering & System Certification <i>Joel Sachs, ARCA</i>
1600 - 1730	Risk Management <i>LtCdr Alan Liddle, IRMC</i>	Criteria Comparisons <i>Dr. Charles Abzug, IRMC</i>	Info System Security Officer's Challenges <i>Chris Bressinger, DoDSI</i>

## Description

These tutorials are based on courses and seminars given by ARCA, the DoD Security Institute, and the Information Resources Management College of the National Defense University. ARCA's Information Security Seminars focus on security engineering and operational security administration based on Arca's actual applied experiences. The DoD Security Institute (DoDSI) provides resident, field, and correspondent courses in countermeasures and administration for information system, physical, and procedural security. The Information Resources Management College (IRMC) includes security in its information management courses, particularly through an intensive Automated Information Systems Security Course which is taught at the graduate level.

The tutorials will be presented in lecture format with question and answer periods. While there is a logical flow between the tutorials, each tutorial will be presented as a separate unit so that conference attendees can attend any or all of them. The tutorials are intended to introduce many and varied security topics as opposed to exploring them in-depth. Brief descriptions of the scheduled tutorials follow:

**Security in the Future** takes a view ahead to changes with security and its role in enterprises, applications, and information infrastructures; with general threats to information systems; and with the roles of security disciplines (operational, communications, computer, physical, administrative).

**Risk Management** focuses on the importance of an overall risk management perspective to information system security stressing risk tolerance as opposed to risk avoidance. Topics include: risk models and differentiation; asset, threat, vulnerability, and risk analysis; and technical vs. operational decisions.

**Trusted Concepts** focuses on the fundamental concepts and terminology of trust technology. It includes descriptions of the Trusted Computer System Evaluation Criteria [TCSEC] classes, how these classes differ, and how to determine the appropriate class for your operational environment.

**Trusted Networks** focuses on basic points in network security and gives an overview of the TNI. Topics include network security concerns and services, trusted network components, the TNI and its Evaluation Classes, system composition and interconnection, and cascading.

**Trusted Database Systems** focuses on security from a "database view" and gives an overview of the TDI. Topics include DBMS specific security requirements, vulnerabilities, and challenges; database design considerations; implementation issues; and use issues.

**Criteria Comparisons** focuses on the differences and similarities of the national and international criteria of Canada, the United States, and Europe. They are compared and considered, both in the context of value to security engineering today and as foundations for the Common Criteria.

**Windows NT Security** focuses on operational security with distributed PC-based computing, using Windows NT as an example. It discusses security from the perspectives of both clients and servers: exposures and vulnerabilities, appropriate control measures, and recommended policies and practices.

**Unix Security** focuses on operational security with operating systems in an internetworked environment, using Unix as an example. It includes an understanding of security weaknesses, methods for improving security, and ways to detect and respond to attacks on UNIX systems.

**ISSO Challenges** focuses on the continued protection and accreditation of operational information systems. Topics include: virus prevention and eradication; access control evaluation and configuration; media clearing and purging; intrusion detection and handling; and accepting increased risk.

**System Security Engineering, Certification, & Accreditation** focuses on engineering and assessment issues in integrating MLS solutions using trusted products, developing the certification evidence, and the accreditation process. Topics include system security, assurance, trade-offs, and methodologies.

**SECURITY INFORMATION FOR THE ASKING:  
THE UNTAPPED INFORMATION POTENTIAL  
AWAITING THE SECURITY PRACTITIONER**

There is a need for information about information technology (IT) security by the computer security community. While much information exists, awareness of its existence and knowledge about how to access it is often lacking. This represents under-utilized resources and untapped potential. This panel will provide the security practitioner with an overview of both the electronic and non-electronic information available.

We live in a time when service-orientated information from various government and private organizations can be available to anyone for the asking. This is one of the goals of the National Information Infrastructure (NII), popularly know as the "information super highway," which plans to make information available via computers in public places, such as libraries and shopping malls.

Panelists: Kathie Everhart - NIST  
Marianne Swanson - NIST  
Bob Lau - NSA  
Nickilyn Lynch - NIST

**Kathie Everhart, National Institute of Standards and Technology (NIST)**

Limited resources can best be leveraged if we share our information with others. A major issue with nearly all sources of information is that information decays rapidly. This involves a commitment to be an active participant in the process. NIST has developed the Interagency Information Sharing Center (IISC). The IISC maintains a variety of information systems security documentation for the purpose of sharing with other federal agencies. The types of information maintained and how to be an active participant will be discussed.

**Marianne Swanson, National Institute of Standards and Technology**

The National Performance Review has recommended that the National Institute of Standards and Technology (NIST) develop a national crisis response clearinghouse to promulgate better security information to the existing group of agency crisis response teams. This clearinghouse is now operational and available not only to agency crisis response teams but to the public as well. The clearinghouse disseminates information about incidents government-wide and serves as a broker of computer security crisis information and of computer security resources. The clearinghouse concept has been implemented through our efforts in establishing and maintaining the NIST Computer Security Bulletin Board and with our active involvement in the Forum of Incident Response and Security Teams (FIRST). the contents of the clearinghouse and how it can be accessed will be discussed.

**Bob Lau, National Security Agency**

DOCKMASTER was developed by the National Security Agency's (NSA) National Computer Security Center (NCSC) in 1985 as an unclassified bulletin board system. DOCKMASTER serves as the focal point for the nation-wide dissemination and exchange of information security data. Customers of DOCKMASTER have access to information security data through electronic mail and through electronic bulletin boards. Users retrieve data, such as available training courses, upcoming INFOSEC conferences, and the evaluated Products List. Online access to information systems security products and services will be discussed.

**Nickilyn Lynch, National Institute of Standards and Technology**

There are numerous discussion forums and newsgroups available for participation and information. Several of the more popular forums are available for viewing from bulletin boards. VIRUS-L, RISKS FORUM, and PRIVACY FORUM are just three of such newsgroups. Discussion on format, risks concerning the use of information technology, and analysis of issues relating to the general topic of privacy will be provided.

## **PANEL SESSION**

### **INTERNATIONAL HARMONIZATION THE COMMON CRITERIA -- PROGRESS & STATUS**

#### **Chair:**

Eugene Troy, NIST, US

#### **Panelists:**

Chris Ketley, European Commission (UK)

Yvon Klein, European Commission (France)

Hartwig Kreutz, European Commission (Germany)

Andrew Robison, CSE, Canada

Mario Tinto, NSA, US

The Common Criteria Project is an international project to align the existing IT security criteria of North America and Europe. The project is a joint activity of the governments of the US and Canada, and the European Commission. Six IT security representatives from these bodies were nominated in mid-1993 to form the Common Criteria Editorial Board (CCEB), and have been developing the CC since that time. All six are members of this panel.

The first major milestone of the CC project will be met with a draft scheduled for completion in late 1994. After project sponsor review, the CC will be released to IT security experts worldwide for review and comment. An earlier draft prepared in April 1994 was subjected to internal review by a large panel of selected experts from many nations. After public review and revision, the draft CC will be made available for use in international trial evaluations.

This panel will give the six members of the CCEB a forum to discuss the project from their own perspectives. They will describe the nature of the project, the input documents, the timetable, and the public review process. In addition, the panel members will provide the first public overview of the draft CC document contents.

The following fact sheet, developed by the CC sponsors at the inception of the project, will provide further information.

## **NORTH AMERICA AND EUROPE AGREE TO DEVELOP COMMON CRITERIA**

### **SUMMARY (June 2, 1993)**

North America and Europe have agreed to develop a "Common Information Technology Security Criteria" (CC).

Security criteria are needed to develop trusted information technology (IT) products that can be used to help protect important information of the government and private sectors. IT security criteria common to Europe and North America will help broaden the market for these products and further lead to economies of scale. In addition, common criteria will help achieve the goal of mutual recognition by North American and European nations of IT product security evaluations.

The effort, which is expected to begin in early Fall of 1993 and be completed in 1994, will use the ISO Subcommittee 27, Working Group 3 draft criteria documents (Parts 1-3) as an initial framework. Specific inputs will include the Information Technology Security Evaluation Criteria (ITSEC), the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), the draft Federal Criteria for Information Technology Security (FC), the experience gained to date with the ITSEC in the form of suggested improvements, the comments now being received on the draft FC document, and the results of the FC invitational workshop planned for 2-3 June 1993.

The resulting common criteria are expected to undergo extensive international review and testing by performing evaluations of "real" products against the criteria prior to being fully accepted for use within Europe and North America. When mature enough, the CC will be provided as a contribution towards an international standard to ISO Subcommittee 27, Working Group 3.

### **BACKGROUND**

The agreement grew out of a 4 February 1993 European Commission-sponsored workshop in Brussels on the Federal Criteria that was attended by many European security professionals. The general European response to the workshop was that alignment of criteria between Europe and North America is now both feasible and opportune.

This idea was taken up and endorsed by the EU Senior Officials Group for the Security of Information Systems (SOG-IS) in their meeting on 11 February, clearing the way for EC participation in the work required to achieve common IT security criteria.

As a result of informal meetings held thereafter, a proposal was made to proceed with a joint project to develop common criteria. This proposal was then given preliminary approval by EU member nations and North American government senior officials.

## **PLANNED DEVELOPMENT PROCEDURE -- THE EDITORIAL BOARD**

Current plans call for the establishment of a six member Editorial Board (CCEB) consisting of three members from North America and three from Europe. The CCEB will be composed of senior IT security experts who have had experience designing IT security criteria and have the authority and autonomy to make decisions with regard to the contents of the CC. The CCEB will be requested to complete their work within a six month timeframe. The main tasks of the CCEB are to obtain a clear understanding of the similarities and differences between current criteria and to develop a first-draft CC for presentation to the participating government bodies. The CCEB will be instructed to use the material identified above as the primary material from which to develop the CC. The CC is to represent a synthesis of the best concepts and components contained in the original material. The CCEB is to avoid inventing new criteria.

## **TECHNICAL GROUPS TO PROVIDE SUPPORT**

The CCEB may establish and utilize special Technical Groups (TGs), as needed, to help develop specific technical areas of the CC. These TGs will operate under the direction of the CCEB for the time needed to perform their assigned tasks. They will be staffed in a representative way, in a pattern like that of the CCEB.

## **PUBLIC REVIEW AND TRIAL USE**

Following completion of the first draft criteria, the governments involved will jointly review the CC. When they mutually determine that the CC is ready for further review by the IT security community at large, they will initiate an extensive review cycle to obtain comments from all interested parties. This cycle is expected to result in additional versions until convergence is achieved. The CC will then enter a trial period to allow the specification and evaluation of vendor offerings against the CC. Upon completion of the trial period, the CC will be revised if necessary to gain final adoption by the participating governments.

## **RELATIONSHIP TO ISO INTERNATIONAL STANDARDIZATION**

During the process of CC development and trial use, the associated governments will work through their respective national standards bodies to help keep the ISO draft standard in relative synchronization with the CC. An issue requiring further study and consultation is how to maintain the necessary level of momentum in ISO, yet avoid finalization of an International Standard prior to achieving generally acceptable common criteria for Europe and North America.

SECURITY REQUIREMENTS FOR DISTRIBUTED SYSTEMS  
NCSC Conference Panel Summary

**1. Panel Makeup**

**Chairman:** Robert Dobry, NSA

**Panelists:** Janet Cugini, NIST  
Virgil Gligor, University of Maryland  
Terry Mayfield, Institute for Defense Analysis

**2. Panel Summary**

Much criticism was received after the issuance of the Federal Criteria because the criteria did not include requirements for distributed systems. A technical group, comprised of the members of this panel, was formed to develop a criteria to handle distributed systems. The plan for this distributed systems criteria has evolved somewhat during its development. The initial idea was to incorporate the distributed system requirements into the Federal Criteria and to develop several protection profiles exclusively for distributed systems. As work on the Federal Criteria shifted towards the international Common Criteria effort, it was decided that, like the Federal Criteria, the distributed systems effort would become input to the Common Criteria.

This panel will attempt to explain what is entailed in providing security for distributed systems and how they see their efforts fitting into the Common Criteria. After a brief introduction of distributed systems and an explanation of how, with the aid of several recognized experts in the field, the distributed systems components were developed, the panelists will provide details of the components.

The distributed system technical group was the first to define a detailed set of security functional and assurance requirements in the area of distributed systems. Several of the concepts needed to provide distributed system security have already been well defined and requirements written. For distributed systems these requirements needed only to be enhanced. These include Identification and Authentication, Trusted Path, Trusted Recovery, Audit, Access Control, and Security Management. There were other areas, however, for which new requirements exist and therefore, new components were written. These included means by which the confidentiality, integrity, and availability of the data moving between the nodes of a distributed system could be assured. New distributed systems components were developed for Data Confidentiality, Data Integrity, Data Availability, and Cryptography. Cryptography is the mechanism chosen to insure data moving between the nodes of a distributed system is secure. As new mechanisms are developed requirements can be developed to encompass these.



# THE APPLICATION OF ELECTRONIC GROUPWARE TOOLS TO ADDRESS IT SECURITY CHALLENGES

## Electronic Groupware Tools Demonstration Committee

*Mr. Dennis Gilbert, NIST, Demonstration Coordinator*

*Ms. Genevieve Burns, Monsanto Co.*

*Ms. Dorothea de Zafra, PHS/FISSEA*

*Mr. James Frost, Idaho State University*

*Mr. Herb LaFond, Idaho State University*

*Dr. W. (Vic) Maconachy, CISS*

*Ms. Irene Gilbert Perry, NIST*

*Ms. Joan Pohly, CISS/FISSEA*

*Dr. Corey Schou, Idaho State University*

*Mr. John Tressler, Department of Education*

*Mr. Nathan Wingert, Idaho State University*

Over the past few years, a number of federal, private sector, and professional organizations have responded to a growing awareness of the need for and value of security training for all involved with information technology and the professional development of security practitioners. An important example of this response has been through participation in a series of DACUM (Design-a-Curriculum) workshops at Idaho State University (ISU), the results of which are contributing to the development of security awareness training materials; IT security curricular; a proposal to revise the NIST Training Guidelines (SP500-172) with a more rigorous conceptual model for security training; a unified body of knowledge for security practitioners; and knowledge, skills and abilities (KSAs) and plans of instruction for various security-related job categories.

These efforts have been substantially facilitated by the use of an electronic group decision support system (using the Electronic Technology for Collaboration, Organizational Reengineering, and Paradigm Change, or ETCORP process), developed and managed under the direction of the ISU Computer Information Systems Department chair, Corey Schou. It is the general consensus among those who have taken part in the DACUMs, that the ETCORP technology can be effectively applied to a wider range of information technology security questions, issues, and challenges beyond the DACUM arena.

During this series of demonstrations, which will run throughout NCSC17, attendees will have the opportunity to hear about the technology and to "test drive" the system. In addition to being able to view the results of the DACUM workshops, they will also be able to "brainstorm" and provide opinions on a series of relevant questions and issues, and explore an archive of security-related information which was created to support the DACUMs.

Requests by organizations and other groups to reserve the facility, free of charge, for a session to focus an issue or question of importance will be honored as circumstances permit.

# THE LEARNING TRACK

## Track Coordinators

*Ms. Patricia Black, Department of the Treasury*  
*Ms. Barbara Cuffie, Social Security Administration*  
*Mr. Dennis Gilbert, National Institute of Standards and Technology*  
*Ms. Sadie Pitcher, Department of Commerce*  
*Ms. Joan Pohly, FISSEA Chair*  
*Mr. John Tressler, ETA Workgroup Chair*

## Track Overview

In an environment that is being shaped by both the emergence of the National Information Infrastructure (NII) and increasing pressures to be more productive, there is a renewed appreciation by public and private sector organizations about the need to cost-effectively protect information systems resources. Meaningful security education, training, and awareness for all, and the availability of staff who can ensure that appropriate controls are in place, are increasingly recognized as part of an overall resource management strategy.

This track presents the status of information technology (IT) security awareness, training, and professionalization efforts from organizations playing a key role in seeking a unified government/industry strategy for better defining and improving these areas. Each organization has a mandate or charter related to either IT security education, training, and awareness, or professional development.

"The *Learning Track*" is presented by the Federal Information Systems Security Educators' Association (FISSEA), which is sponsored by the National Institute of Standards and Technology (NIST), and the Information Systems Security Education, Training and Awareness (ETA) Working Group sponsored by the National Security Telecommunications and Information Systems Security Committee (NSTISSC). This track will focus on several efforts throughout the IT security community relating to learning initiatives.

## Panel Session Descriptions

Panel Session 1: ***Training Challenges of the 90'S***  
Chair: Ms. Joan Pohly, FISSEA Chair

The security needs of the information highway will place greater demands on the workforce and the security professional. The security concerns of users, service and information providers must be considered for the National Information Infrastructure to realize its full potential. The focus for the future must be on creative cost-effective solutions. This panel will outline several challenges of complying with training mandates and provide proposed solutions.

Panel Session 2: ***Proposed New NIST Training Standards***  
Chair: Ms. Dorothea de Zafra, Public Health Service

As computer technology advances, new challenges arise in protecting information. Along with this, new training standards must also be set. This panel will review the draft developed by FISSEA that is proposed to replace the NIST training guideline, NIST Special Publication 500-172.

Panel Session 3: ***Computer Security Resources that Work***  
Chair: Ms. Barbara Cuffie, Social Security Administration

There are a variety of computer security resources, including specialized tools, that are reliable and beneficial to those responsible for IT security in government and industry. Panel members will identify and review several of these resources and comment on their experiences using them.

Panel Session 4: ***Effective Marketing of the Computer Security Program to Management***  
Chair: Ms. Joan Hash, Social Security Administration

Garnering management support has long been a primary step in an effective computer security program. This panel will share their experiences in their efforts to secure management support.

Panel Session 5: ***Tools and Methodologies for Delivering Training***  
Chair: Ms. Janet Jelen, Public Health Service

The effectiveness of training depends on the supporting tools and the methodologies used in their delivery. This panel will provide information on tools in use today and successful methodologies that have resulted in effective training. It will also address tools and methodologies being considered for the future to address the evolving information environment.

Session 6: ***Demonstrations on Computer Security Training Tools***  
Chair: Mr. Anthony Stramella, National Cryptologic School

Computer security products available for government-wide use will be demonstrated. These will include computer-based training packages, videos, and interactive learning tools.

Panel Session 7: ***Training Events on a Shoestring Budget***  
Chair: Ms. Sadie Pitcher, Department of Commerce

This panel will discuss the benefits of building training and education mechanisms into

organizational conferences, symposiums, meetings, workshops, and peer group networking. Panel members will share their experiences in developing and sponsoring events that provide quality training opportunities for little or no cost.

Panel Session 8: ***Adult Learning and Information Systems Security Training***

Chair: Dr. Eugene V. Martin, Organization and Education Consultant

Recent developments in methodology offer more effective ways of teaching adults to use technical skills that also require individual judgement. This panel will draw on the research and experiences of employer-sponsored training to examine lessons learned about methodologies in use, the basic concepts of adult learning, and the ways these principles can be applied to information systems security training.

Panel Session 9: ***There will not be a Learning Track presentation during this session.***

Panel Session 10: ***Information Systems Professionalism - Professional Development and Certification***

Co-chairs: Mr. Richard Koenig, Mr. Harold Tipton, International Information Systems Security Certification Consortium (ISC)<sup>2</sup>

There are several initiatives underway to professionalize the community and certify the computer security professional. This panel will discuss both the current status and future directions of these initiatives.

Panel Session 11: ***Computer Ethics for Future Generations***

Co-chairs: Mr. Richard Koenig, (ISC)<sup>2</sup>, TBD

This panel will describe a current initiative sponsored by (ISC)<sup>2</sup> to develop a computer security ethics program for elementary school children. This program focuses on introducing ethics as an integral part of computer literacy curricular during childrens' formative years. Implementation approaches will be discussed.