23rd National Information Systems Security Conference

October 16-19, 2000

Baltimore Convention Center

Baltimore, MD

Back to Baltimore!

Campaign For Security

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

National Computer Security Center
National Security Agency
U.S. Department of Defense

23rd National Information Systems Security Conference

October 16—19, 2000, Baltimore Convention Center, Baltimore MD

Located next to the Inner Harbor of Baltimore
Post-Conference Workshops—October 19, 2000

Sponsored By

Information Technology Laboratory
National Institute of Standards and Technology
National Computer Security Center
National Security Agency

Program Council

Program Hosts

Mr. Lawrence G. Martin
Director, National Computer Security Center
National Security Agency

Dr. William Mehuron
Director, Information Technology Laboratory
National Institute of Standards and Technology

Mr. Timothy Grance
Group Manager, Computer Security Division
National Institute of Standards and Technology

Conference Chairs

Jack Holleran, *NCSC*
John Wack, *NIST*

Program Chairs

Wendy Jarmon, *NCSC*
Mark Wilson, *NIST*

Program Committee

David Balenson, *NAI Labs at Network Associates*
Edward Borodkin *(retired)*
Murray Donaldson, *CESG, UK*
Karen Ferraiolo, *Arca Systems, An Exodus Communications Company*
Greg Gage, *USDA*
Janice Green, *GSA*
Jim Litchko, *Litchko & Associates, Inc.*
Russ Mundy, *NAI Labs at Network Associates*
Dr. Fran Nielsen, *NIST*
W. Joy Prangley, *USDA*
Gene Troy, *NIST*
Dr. Rayford Vaughn Jr., *Mississippi State University*

Administration

Charlene Gassaway, *NCSC*
Peggy Himes, *NIST*
Kathy Kilmer, *NIST*
Marianne McGinty, *NCSC*
Patrick O'Reilly, *NIST*
Pat Purkey, *NCSC*
Katie Shuggars, *NIST*
Casey Smith, *NCSC*
Sara Torrence, *NIST*
Teresa Vicente, *NIST*
Kelly Watkins, *NIST*

Contents

Campaign for Security

Special Features

Lieutenant General Michael V. Hayden, United States Air Force, Director, National Security Agency/Central Security Service (NSA/CSS), Fort George G. Meade, MD. As the Director of NSA/CSS, he is responsible for a combat support agency of the Department of Defense with military and civilian personnel stationed worldwide.

Dr. David J. Farber is the Alfred Fitler Moore Professor of Telecommunication Systems at the University of Pennsylvania, holding appointments in the Computer Science and Electrical Engineering Departments. He was a principal in the creation and implementation of CSNet, NSFNet, BITNET II, and CREN, and was instrumental in the creation of the NSF/DARPA funded Gigabit Network Testbed Initiative.

Dr. Eugene H. Spafford is a Professor of Computer Science at Purdue University. Spafford is director of the Purdue CERIAS (Center for Education and Research in Information Assurance and Security). He has authored several books and many publications dealing with Internet-related computer security. He is respected worldwide for his work in computer ethics and vulnerability analysis.

Mr. Mark Rasch is Vice President of Global Integrity Corporation in Reston Virginia. In this capacity, he advises banks, insurance companies, entertainment companies, and other Fortune 100 companies on legal and policy issues relating to doing business in Cyberspace. He has written and lectured extensively on computer crime, privacy, trademark and trade secret issues on the Internet, and has been featured in the *New York Times,* ABC's Nightline, PBS' Technopolitics, CNBC, and NPR as an expert on computer law and policy.

Mr. Michael Jacobs, *Deputy Director For Information Systems Security, National Security Agency*

Mr. Simon Gauthier, *Deputy Chief, Information Technology Security, CSE, Canada*

Dr. William Mehuron, *Director, Information Technology Laboratory, NIST*

The Closing Plenary will be a North American Panel Discussion on issues relevant to Information Assurance, Technology, and Security. The speakers will discuss common goals and needs for the future of their respective countries.

Schedule

Monday, October 16, 2000

Earlybird Sessions

8:30am—10:30am

Rooms 301—303

Killer Apps—and You're Dead Meat (The Code That Shagged Me) (p. 475)
G. Mark Hardy, *Guardent, Inc.*

As our computing model shifts from a well-controlled client-server model to that of the active desktop, a flood of dangerous and malicious code is now coursing through enterprise networks. From Melissa to ILOVEYOU to the next attack, our traditional means of screening out malicious code seem to be letting a lot through. We'll take a look at the most significant attacks of this past year, see how well (or poorly) the security infrastructure responded, and provide recommendations as to how you can better protect yourself in the future.
Technical Degree of Difficulty = 2

Room 324

Conference Overview—Welcome Newcomers
Mark Wilson, *NIST*

The NIST Program Chair for this year's Conference will welcome newcomers to the 23rd NISSC and help them navigate their way through their many choices during the next 3.5 days.

Room 330

Paper Session: Student Papers
Session Chair: (TBD)

The Competitive Intelligence and National Security Threat From Website Job Listings
Jay Krasnow, *Georgetown University*

The Case for Beneficial Computer Viruses and Worms—A Student's Perspective
Greg Moorer, *Mississippi State University*

Subliminal Traceroute in TCP/IP
Thomas E. Daniels, *Purdue University*

Rooms 331—332

Incident Response Fundamentals
Eric Winterton, *Arca Systems, An Exodus Communications Company*

This session will introduce the student to the basic definitions, concepts, and procedures of, or relating to, incident response. By the end of the session, attendees will be able to answer the following questions:
- Who can help me respond to an incident?
- What are the main elements of an incident response team?
- How do I REACT to a perceived incident (anomaly)?
- How does the Incident Response Team RESPOND to a reported anomaly?
- How do I RECOVER in the wake of an incident?

Technical Degree of Difficulty = 1

10:30am—12:00noon

Rooms 307—310

Opening Plenary
Opening Plenary Keynote Speakers:

Lieutenant General Michael V. Hayden, *USAF, Director, National Security Agency/Central Security Service (NSA/CSS)*

Dr. David J. Farber, *Alfred Fitler Moore Professor of Telecommunication Systems at the University of Pennsylvania*

National Computer Systems Security Award Winner:
The NIST Information Technology Laboratory and the NSA National Computer Security Center present the 2000 National Computer Systems Security Award to **Dr. Eugene H. Spafford,** *Professor of Computer Science at Purdue University.*

Don't miss the Awards CEREMONY

Ceremony: 5:30 p.m., Room 310
Reception: 6:15 p.m., Pratt Street Lobby

1:30pm—3:00pm

Rooms 301–303

The Systems Security Engineering Capability Maturity Model (p. 503)
Karen Ferraiolo, *Arca Systems, An Exodus Communications Company*

The Systems Security Engineering Capability Maturity Model (SSE-CMM) was developed with the objective of advancing security engineering as a defined, mature and measurable discipline. The model and its accompanying appraisal method are currently available tools for evaluating the capability of providers of security engineering products, systems, and services as well as for guiding organizations in defining and improving their security engineering practices.

This tutorial describes the SSE-CMM and its appraisal method. In addition, a discussion of the application of the SSE-CMM looks at issues as they present themselves throughout a system acquisition, from RFP, through development, and to system operation.
Technical Degree of Difficulty = 3

Room 307

Future of Information Security (p. 489)
Chair: G. Mark Hardy, *Guardent, Inc.*
Jeff Moss, *DEF CON Communications*
Winn Schwartau, *Interpact Associates*
Peter Shipley, *OneSecure, Inc.*
Ira Winkler, *Information Security Advisors Group*

Back by popular demand, this was one of last year's most popular panels. Here's a great opportunity to meet with five of the most experienced security experts in the industry today: Jeff Moss, Winn Schwartau, Peter Shipley, Ira Winkler, and G. Mark Hardy. These experts will discuss their vision of the future of information security, what roles corporate, hacker, technical, and penetration experts will play, and offer recommendations on how you can benefit from this insight.
Technical Degree of Difficulty = 2

Note:
Numbers in parenthesis following session/paper title point to page in Conference Proceedings.

Room 308

AES and Beyond (p. 490)
Chair: Elaine Barker, *NIST*
Jim Foti, *NIST*
(TBD)—Submitter of the selected AES algorithm
Bill Burr, *NIST*
Marcus Leech, *Nortel Networks*

The end of the AES development process is now in sight. The algorithm has been selected, and the draft standard is ready for public comment. After nearly four years of intensive effort, what has been accomplished? What has been learned? What would we do differently? What are the next steps in making AES the international standard that was intended? And—what lies beyond AES? NIST is in the process of initiating a number of other cryptographic activities, including a standard specifying modes of operation for symmetric key block ciphers (e.g., AES), an HMAC standard, a key management standard, a new and enlarged hash function that is consistent with the AES key sizes, and an increase in key sizes for the Digital Signature Algorithm (DSA).
Technical Degree of Difficulty = 2 to 3

Room 309

NIAP/Common Criteria Scheme Presentations
Chair: Tom Anderson, *NSA*

Room 310

Effective Risk Analysis (p. 494)
Thomas Peltier, *Netigy Corporation*

The dictionary defines RISK as "someone or something that creates or suggests a hazard.. In today's environment, it is one of the many costs of doing business or providing a service. Information security professionals know and understand that nothing ever runs smoothly for very long. Any manner of internal or external hazard or risk can cause a well running organization to lose competitive advantage, miss a deadline, or suffer embarrassment. This session will review the current practical application of cost-effective risk analysis.
Technical Degree of Difficulty = 3

Rooms 327–329

The Secret and Below Interoperability (SABI) Process—Continuing the Discovery of Community Risk (p. 492)
Chair: Mark Loepker, *NSA*
Curtis Dukes, *NSA*
Charles Schreiner, *NSA*
Willard Unkenholz, *NSA*
Corky Parks, *NSA*
Dallas Pearson, *NSA*
Warner Brake, *DISA*

Secret and Below Interoperability (SABI) is an Information Assurance initiative mandated by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD/C3I). SABI improves the security posture of all secret and below DoD systems by using a community-based risk acceptance approach. During the discussion about the current status of the SABI program, the panel will focus on the progress and impact of the National Information Assurance Certification and Accreditation Process (NIACAP), NSTISSI 1000.
Technical Degree of Difficulty = 2 to 3

Room 330

Paper Session: Intrusion Detection
Session Chair: (TBD)

Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection (p. 13)
Susan M. Bridges, *Mississippi State University*

Next Generation Intrusion Detection: Autonomous Reinforcement Learning of Network Attacks (p. 1)
James Cannady, *Georgia Institute of Technology*

Multiple Self-Organizing Maps for Intrusion Detection (p. 32)
Brandon Craig Rhodes, *Georgia Institute of Technology*

Rooms 331–332

Themes and Highlights of the New Security Paradigms Workshop 2000 (p. 515)
Chair: Steven J. Greenwald, *INFOSEC Consultant*
Simon N. Foley, *University College, Cork, Ireland*
Cynthia Irvine, *Naval Postgraduate School*
Kai Rannenberg, *Microsoft Research Cambridge, UK*
Emilia Rosti, *Università degli Studi di Milano, Italy*

This panel will highlight a selection of some of the most interesting and provocative papers from the 2000 New Security Paradigms Workshop (NSPW), held September19–21 in Ballycotton, County Cork, Ireland. In keeping with the NSPW philosophy, this panel will challenge many of the dominant paradigms in information security. It will be highly interactive; we expect lively exchanges between the panelists and the audience. Come prepared with an open mind and a willingness to question and comment on what our panelists present and be sure to strap on your seat belt! The panel will consist of four authors selected with great pain and difficulty from the great papers presented at the last NSPW.
Technical Degree of Difficulty = 3

3:30pm—5:00pm

Rooms 301—303

The National Security Agency's Use of the Systems Security Engineering Capability Maturity Model (SSE-CMM) (p. 529)
Chair: Mary D. Schanken, *NSA*
Paul W. Boudra, *NSA*
Charles G. Menk III, *NSA*

NSA began the effort to develop a CMM for security engineering in 1993, with the hopes that the security engineering community would become involved to help define the criteria against which they might be assessed in the future. Learning from the past, NSA believed this approach would be more successful and accepted than if NSA were to issue it as a requirement. Over 50 government, industry, and academic organizations developed the Systems Security Engineering Capability Maturity Model (SSE-CMM) and its appraisal methodology. This panel will address a few of the ways that the National Security Agency is using the SSE-CMM.
Technical Degree of Difficulty = 2

Room 307

Evaluation Scope:
Does One Size Fit All? (p. 522)
Chair: John Doody, *CESG, UK*
David Hodges, *CESG, UK*
Adrian Price, *Ministry of Defence, UK*
Bill Simpson, *Borderware*
Janet Scruby, *Syntegra CLEF*

Every evaluation has a scope, what is included in the evaluation and what is not. The scope of any evaluation depends on the developer, his customers and the scheme under which the product is to be evaluated. They all have different requirements and perspectives of what the scope of evaluation should be. These differences have always existed, but growth of distributed applications, such as e-commerce, and the diversity of secure products needed to support them is forcing the evolution of what is an acceptable evaluation scope. The panel will examine the issues associated with evaluation scope from the perspective of the developer, his customers and the UK's Scheme.
Technical Degree of Difficulty = 2

Note:
Numbers in parenthesis following session/paper title point to page in Conference Proceedings.

http://csrc.nist.gov/nissc/

Room 308

State of Key Recovery:
Government and Industry
Chair: Santosh Chokhani, *CygnaCom Solutions/an Entrust Technologies Company*
Donna Dodson, *SSA*
Diane Dunshee, *NSA*
Santosh Chokhani, *CygnaCom*
Craig Shelton, *The Mitre Corporation*
Sekar Chandersekaran, *Microsoft*

As Government agencies use PKI technology for confidentiality (i.e., encryption of communicated messages), key recovery will play an increasingly important role. The well designed key recovery system ensures that the authorized managers within the organization can decrypt the communication while the employee is not available. The purpose of this session is to provide a status of the various key recovery initiatives in the Government and to provide a description of the capabilities in the commercial products.
Technical Degree of Difficulty = 3

Room 309

National Information Assurance Partnership—2001
Chair: Ron Ross, *NIST*
L. Arnold Johnson, *NIST*
Gene Troy, *NIST*
Peter Mell, *NIST*

The National Information Assurance Partnership (NIAP) is a U.S. Government initiative originated to meet the security testing needs of both information technology (IT) consumers and producers. This session will provide updates on several high visibility NIAP projects to include smart card security specification, security in healthcare systems, automated security testing, development of security specifications for critical information technologies, specification tools and techniques, and the Common Criteria evaluation and validation program.

Room 310

Network-Based Contingency Plans
Thomas Peltier, *Netigy Corporation*

Attempting to complete an organization-wide or even a data center disaster recovery plan can be a daunting task. However, by using some tested project management techniques, the process can be divided into a manageable undertaking. In this session we will review the process used by successful DRP developers and how they break down the processes and then prioritize the tasks. By identifying what needs to be done first, the efforts of the DRP team can be concentrated on those elements that will provide the organization with the quickest return on its investment.
Technical Degree of Difficulty = 3

Rooms 327—329

Department of Defense (DoD) Wide Information Assurance Program (DIAP): Current Initiatives (p. 525)
Chair: Captain J. Katharine Burton, *USN, DoD*
Terry Bartlett, *DIAP*
George Bieber, *DISA*
Jim Christy, *DIAP*

This panel will begin with an overview of where the DIAP stands today and what activities/initiatives have been accomplished in the past year. Following that will be presentations on three areas where significant effort is currently being spent: IA Metrics, IT/IA Professionalization and Law Enforcement. Each presenter will discuss where that initiative currently stands, what activities are going on within DoD and the various services/agencies, and what the activity will contribute to the improvement of the IA posture of the Department.
Technical Degree of Difficulty = 3–4

Room 330

Paper Session:
Practices, Curses, and Risks
Session Chair: (TBD)

Best Security Practices:
An Overview (p. 56)
Guy King, *Computer Sciences Corporation*

The Curse of Service: Civil Liability for Computer Security Professionals (p. 43)
Arthur J. Wylene, *New College of California School of Law*

Visualizing Risks: Icons for Information Attack Scenarios (p. 71)
Hilary H. Hosmer, *Data Security, Inc.*

Rooms 331—332

Security and Source-Available Systems: Risks and Opportunities (p. 531)
Chair: Peter G. Neumann, *SRI International*
Jay Beale, *Bastille Linux*
Crispin Cowan, *WireX Communications, Inc.*
Eric Raymond, *Open Source Initiative*

Today's mass-market proprietary closed-source software seriously impedes efforts to improve installed systems in response to recognition of new vulnerabilities and risks. Source-available software provides a potential alternative, enabling open collaborative efforts, widespread review of source code, rapid generation and acquisition of fixes, and a broad community of collaborators. Additional benefits also accrue from well-defined open requirements and open specifications. This panel will explore the source-available alternatives and how they might best contribute to the development and operation of meaningfully robust secure systems.
Technical Degree of Difficulty = 2 to 4

8:30am—10:00am

Rooms 301—303

Aspects of InfoSec: The UK View (p. 562)
Chair: John Doody, *CESG, UK*
Roger Griffin, *Civil Service College, UK*
Terry Wells, *Department of the Environment, UK*
John Laskey, *Home Office, UK*
John Peters, *Ministry of Defence, UK*

In 1997, the UK Government launched a pro-gramme called "Modernising Government." The aim was to have government departments con-nected electronically and allow the UK citizen to access government departments. Part of the Modernising Government initiative was the launch of the Government Secure Intranet (GSI).

The challenge facing the security authorities was how to implement a secure architecture that would allow the safe handling of both classified and unclassified information. This presentation will highlight the development of the GSI, case studies associated with the rules in place to join the GSI and the impact and relevance of BS7799 in setting security standards.
Technical Degree of Difficulty = 3

Room 307

Certified vs Secure (p. 533)
Chair: Jon David, *Lehman Brothers*
Sarah Gordon, *IBM*
Tim Polk, *NIST*
Dan Woolley, *Global Integrity Corporation*
Fred Kolbrener, *Xacta Corporation*

Proper products and processes are necessary to secure systems and operations, but this implies the ability to accurately differentiate between alterna-tives. Few of us have either the ability or time to attempt formal comparative evaluations. We look to outside certifiers, but how good are they, how hon-est are they, how do their results apply to specific requirements? This session examines the implica-tions of various types of certification, and suggests ways to best use what's available.

Room 308

Achieving Global Trust in an e-World (p. 536)
Chair
Richard G. Wilsher, *the Zygma partnership, GB*

Panelists
Michael S. Baum, *VeriSign inc., US*
Caelen King, *Baltimore Technologies plc., IE*
Helmut Kurth, *atsec GmbH, DE*

The ISSC has a long and respected heritage as an important event in the field of information security. However, in recent years the influence of 'infosec' has spread pervasively into the com-mercial domain; in that time its scope has also become fundamentally international. This panel has come about because its members believe

that it is appropriate for the ISSC to now adopt a broader approach and to reach out to a much wider international audience. This session will bring to a largely US audience some specific European perspectives and awareness of ongo-ing work. It is intended to be interactive, even provocative: members of the audience will be invited to respond and debate the issues in terms of the relevance of this work to the US business environment and exploring ways in which joint cooperation could be fostered.
Technical Degree of Difficulty = 3.5
(Business-focused; not for pure techies.)

Room 309

Common Criteria Tools: A Status and Demonstration (p. 588)
Chair: Kris Britton, *NSA*
Gary Grainger, *Mitretek Systems*
Jim Williams, *Independent Consultant*

This panel will provide a demonstration of the Common Criteria Toolset (i.e., CC Toolbox™, CC Profile Knowledge Base™) developed by the National Information Assurance Partnership for information security professionals responsible for writing and justifying security requirements. It will include an explanation of the latest updates as well as a plan for its continued devel-opment in 2001.
Technical Degree of Difficulty = 3

Room 310

Preparing for Intrusion Detection (p. 553)
Thomas Peltier, *Netigy Corporation*

Systems and networks are subject to attacks both internally and externally. The increasingly frequent attacks on Internet-visible systems could be attempts to steal your company jewels, personal employee and customer information, or use of your computer resources. Intrusion detection systems collect information from a variety of vantage points within the operating systems and networks. This session will examine intrusion-detection and vulnerability-assessment technologies that will allow your organization to protect the enterprise from losses associated with network security problems. We will review how intrusion detection and vulnerability assess-ment products fit into the overall security archi-tecture; case histories; and product features.
Technical Degree of Difficulty = 3

Rooms 327—329

Progress of the Best Security Practices Subcommittee (p. 550)
Chair: James P. Craft, *United States Agency for International Development (USAID)*
Marianne Swanson, *NIST*
Mary Schanken, *NSA*
Marty Poch, *EPA*
Michael T. Hovey, *Computer Sciences Corporation*

The CIO Council's Best Security Practice (BSP) project fills the security knowledge gap between episodic professional classroom training and disor-ganized electronic bulletin board discussion threads by providing a structured capability for all Federal IT professionals to share first-hand infor-mation regarding their security implementation experiences. Upon accessing the BSP website (http://bsp.cio.gov) users can easily obtain infor-mation most relevant to their unique needs.
Technical Degree of Difficulty = 2

Room 330

Paper Session: Access Control
Session Chair: (TBD)

Push Architectures for User Role Assignment (p. 89)
Venkata Bhamidipati, *George Mason University*

A Role-Based Delegation Model and Some Extensions (p. 101)
Ezedin Barka, *George Mason University*

Generalized Role-Based Access Control for Securing Future Applications (p. 115)
Michael J. Covington, *Georgia Institute of Technology*

Rooms 331—332

Security and Quality of Service Interactions (p. 583)
Chair: Susan Hinrichs, *Cisco Systems, Inc.*
Klara Nahrstedt, *University of Illinois*
John McHugh, *CERT Coordination Center*
Partha Bhattacharya, *Cisco Systems, Inc.*

Security and quality of service (QoS) are two critical network services in today's inter-networked world. Security mechanisms are used to provide proof of identity, preserve protected information, and ensure that information received has not been tampered with. Quality of service enables multi-media and other real-time services to use public data networks instead of more expensive dedicated networks. This panel session will be geared for attendees interested in network management and design. In particular, this session will be of interest to attendees responsible for the security and/or quality of service aspects of network design and management.
Technical Degree of Difficulty = 4

Note:
Numbers in parenthesis following session/paper title point to page in Conference Proceedings.

http://csrc.nist.gov/nissc/

10:30am—12:00 noon

Rooms 301—303

Security in Business-to-Business e-commerce (p. 598)
Chair: Jeremy Epstein, *webMethods*
Igor Balabine, *Netfish*
David Burdett, *CommerceOne*
Frank Jaffe, *Clareon*

Business-to-Business (B2B) e-commerce has become one of the hottest topics this year. This panel will discuss some of the key areas for security in B2B today and in the future, including: reliance on PKI in a world of billion dollar transactions; keeping attackers at bay when ordering systems are online; privacy in an international context with import/export regulations; knowing that a transaction is properly authorized; sharing with trading partners without becoming vulnerable; audit trails; managing security in a world of rapidly changing standards; electronic payments; privacy implications of B2B; solving business-to-government, government-to-business, and government-to-government challenges.
Technical Degree of Difficulty = 3

Room 307

PKI—Sham or Salvation? (p. 589)
Chair: Jon David, *Lehman Brothers*
Padgett Peterson, *Lockheed-Martin*
Tim Polk, *NIST*
Fred Cohen, *Sandia National Laboratories*

PKI is touted as the thing that will make the Internet in general, and e-commerce in particular, secure. Just what is PKI, though? Is it as good as the vendors say it is, or is it just another ploy of the marketroids to foist pseudo-solutions on an unsuspecting user base? This session looks at these questions, and answers them. This session will set forth the intended purposes of PKI, and the related equipment, techniques, protocols, etc. It will detail the benefits it offers, and show how the various components interact to provide the security/authentication/non-repudiation/etc. associated with it.

Note:
Numbers in parenthesis following session/paper title point to page in Conference Proceedings.

http://csrc.nist.gov/nissc/

Room 308

Guideline for Implementing Cryptography in the Federal Government (p. 594)
Annabelle Lee, *NIST*

The purpose of the *Guideline for Implementing Cryptography in the Federal Government* (SP 800-21) is to provide guidance to Federal agencies on how to select cryptographic controls for protecting Sensitive Unclassified information. *The Guideline* focuses on Federal standards documented in Federal Information Processing Standards Publications (FIPS PUBs) and the cryptographic modules and algorithms that are validated against these standards. This guideline was written for federal employees who are responsible for designing systems, and procuring, installing, and operating security products to meet identified security requirements. The purpose of the presentation is to provide an overview of this guideline.
Technical Degree of Difficulty = 3

Room 309

Innovative Uses of the Common Criteria (p. 613)
Chair: Terry Losonsky, *NSA*
Jack Sherwood, *USN,DoD*
John Mildner, *USN, DoD*
Peter Sargent, *COACT Inc.*

The session introduces the audience to innovative ways the Common Criteria is used to solve Information Assurance (IA) challenges.
Technical Degree of Difficulty = 3

Room 310

Privacy in the Information Age (p. 597)
Chair: Blaine W. Burnham, *University of Nebraska at Omaha*
Jeffrey Hunker, *National Security Council*
John Hale, *University of Tulsa*
David L. Sobel, *EPIC*
Simpson Garfinkel, *Information Security Specialist*

One of the most potentially disruptive consequences of the Information Age is the impact on personal privacy. The ability for so many to know so much about everyone is growing at an unprecedented rate. Historically, this accumulation of individual personal information has been perceived by the public as sort of a necessary evil, particularly in the case of the credit reporting services. The extent of the accuracy of that information, the ease or circumstance under which it was gathered, and the extent to which that information was shared or sold was thought to be more-or-less understood by the public and the sense of personal invasion was limited. Now all bets are off. In Cyberspace, technology enables the recording and reporting of actions without any personal knowledge or awareness. The practice of collecting, consolidating, interpreting, and reselling personal information is

for all intents unregulated and, possibly more importantly, not available to the individuals. There is a growing concern for the potential abuses of personal information. This panel attempts to illuminate the many sides to the discussion. What is the government role? What is actually going on—how bad is it out there? What is the commercial sector trying to accomplish?
Technical Degree of Difficulty = 2

Rooms 327—329

Critical Infrastructure Protection for Chief Information Officers or CIP for CIOs (p. 596)
Chair: John C. Davis, *Mitretek*
John M. Gilligan, *Department of Energy*
Col John E. Whiteford, *USAF, NSA*
Linda Burek, *Department of Justice*

Since the signing of the Presidential Decision Directive on Critical Infrastructure Protection (CIP) and the publication of the National Plan for Information System Protection, CIOs have new responsibilities. They must protect the infrastructures of their departments and agencies; help to make the government a model for the private sector; and transition the lessons learned from the successful Y2K effort to CIP. The panel will explore how CIP responsibilities will be accomplished in their organization.
Technical Degree of Difficulty = 2

Room 330

Paper Session: Malicious Code
Session Chair: (TBD)

The Evolving Virus Threat (p. 141)
Carey Nachenberg, *Symantec Corporation*

The Cracker Patch Choice: An Analysis of Post Hoc Security Techniques (p. 154)
Crispin Cowan, *WireX Communications, Inc.*

Antivirus Software Testing for the New Millennium (p. 125)
Sarah Gordon, *IBM Research*

Rooms 331—332

RSA Digital Signature Standards (p. 775)
Burt Kaliski, *RSA Laboratories*

Standards, theory and practice have resulted in a variety of digital signature schemes based on the RSA public-key cryptosystem, including PKCS #1, ANSI X9.31, and the Bellare-Rogaway Probabilistic Signature Scheme (PSS). This presentation describes these schemes and gives a strategy for improving long-term security as well as interoperability of digital signature standards based on the RSA algorithm.
Technical Degree of Difficulty = 4

1:30pm—3:00pm

Rooms 301—303

Protection of B2B Exchanges and Vendor Operations (p. 638)
Chair
Charlie Baggett, *Risk Management Associates, Inc.*

Panelists
Tim Ehrsam, *Oracle Corporation*
Nick Piazzola, *VeriSign*
Gary Secrest, *Johnson & Johnson*

This panel will address the risks and remedies associated with the security of operating business-to-business (B2B) exchanges and vendor web sites. Every new technology and paradigm brings with it new risks, and B2B Internet business is no exception. This panel will discuss the risks associated with this new business area and the remedies which can be applied to reduce those risks. Panelists will come from the commercial sector, defense/commercial industry Internet security, and government.

Room 307

Federal Bridge Certification Authority (FBCA) Demonstration and Panel—Part I (p. 614)
Chair
Richard A. Guida, *Federal PKI Steering Committee*

Panelists
Tim Polk, *NIST*
Stanley Choffrey, *GSA*
Dave Fillingham, *NSA*

This panel will discuss efforts to establish and operate a Federal Bridge Certification Authority (FBCA) to support peer to peer, non-hierarchical interoperability among disparate agency PKI domains. The discussion will cover: (a) how interoperability among Federal agency PKI domains may be effected on a policy and technical level; (b) why the FBCA concept has emerged as the most attractive solution; (c) how the FBCA has been implemented and tested in prototype form; (d) how the production FBCA is being developed; (e) what the principal challenges are on a policy and technical level; and (f) how the FBCA activities will be managed pursuant by a Federal PKI Policy Authority. Part II of this session will follow immediately at 3:30pm. Technical Degree of Difficulty = 3 to 4

Room 308

Incident Response—Stopping Them Dead in Their Tracks (p. 624)
Chair: Jon David, *Lehman Brothers*
Robert Stone, *UUNET Technologies*
Jim Duncan, *Cisco*
Bill Hancock, *Exodus Communications*
Richard Reybok, *Merrill Lynch*

When security fails, as it always has done and will always continue to do, reaction to breaches is of prime importance. This session defines incidents, tells what you can — and can't — expect from your ISP and other upstream providers, gives a real world approach to actual responses, and discusses the involvement of others, from local through an international level, as necessary. (This is the first of a double session on Incident Response. The second session will immediately follow this session at 3:30pm.)

Room 309

The Common Criteria Structures: The Healthcare Response to Security Regulation (p. 652)
Chair: Lewis Lorton, *Forum on Privacy & Security in Healthcare*
Lisa A. Gallagher, *Exodus Security Services*
Paul Zatychec, *EWA-Canada Ltd.*
Leslie Spiece, *University of Wisconsin*
Alan Brown, *McKenna & Cuneo*

This panel will provide an accurate general understanding of how the Common Criteria can order the healthcare industry. Panelists will provide viewpoints from different segments of the community. Topics covered in this panel include: viewpoints of the various industry sectors; benefits to various industry segments; drivers for the use of the Common Criteria; obstacles to completion; relationship to regulatory requirements; and risks to the healthcare industry from an un-regularized security process.

Room 310

Operational Computer Forensics—The New Frontier (p. 632)
Michael J. Corby, *Netigy Corporation*

There can be no doubt that preventing unwanted access to systems is a good thing. But what happens if somehow a chink in the armor is revealed. Computer forensics is a new specialty that can identify the proper procedures for collecting evidence in a manner suitable for use in apprehending and prosecuting security violators. The first part of this session will identify key elements in building an effective Computer Forensics program. The second part will focus on ways to configure clients and servers in a LAN to facilitate forensic data collection.

Room 330

Paper Session: Case Studies
Session Chair: (TBD)

Using B Method to Formalize the Java Card Runtime Security Policy for a Common Criteria Evaluation (p. 179)
Stéphanie Motré, *Gemplus, France*

Penetration Analysis of a Xerox Docucenter DC 230ST: Assessing the Security of a Multi-Purpose Office Machine (p. 167)
Benjamin A. Kuperman, *Purdue University*

Analysis of Terminal Server Architectures for Thin Clients in a High Assurance Network (p. 192)
Cynthia Irvine, *Naval Postgraduate School*

Rooms 331—332

Information Assurance Metrics: Prophecy, Process, or Pipedream? (p. 640)
Chair: Ronda R. Henning, *Harris Corporation*
Michael J. Skroch, *DARPA*
John McHugh, *Carnegie Mellon Center for Survivable Systems*
John Michael Williams, *JMW Trading Company*

Information Assurance has long been considered a "black art"—a good security engineer knows a good security design or implementation by intuition, not by quantifiable measures.

This panel seeks to present four perspectives on information assurance measurement: 1) The perspective of information assurance metrics being attainable in the near term, if a disciplined, scientific approach is applied to the problem; 2) The perspective that service level agreements provide a near term approach to determining the information assurance capabilities of a service provider; 3) The perspective of useful assurance processes with the use of auditing to ensure process execution, with the realization these assurance processes will never replace good, basic assurance mechanisms; and 4) The perspective of the information assurance community learning from the software engineering disciplines and their repeated attempts to turn good software development practices into a quantitative measurement-based science before information assurance metrics take a similar path.

3:30pm—5:00pm

Rooms 301—303

Enterprise Security Infrastructure: A Managed Approach (p. 669)
J. Greg Hanson, *Telos Corporation*
This presentation will define the demands and issues related to centralized management of security technologies, then clarify the advantages of providing centralized management of security infrastructure under the same enterprise management system as used for the enterprise IT network.

Room 307

Federal Bridge Certification Authority (FBCA) Demonstration and Panel—Part II
Chair: Richard A. Guida, *Federal PKI Steering Committee*
Tim Polk, *NIST*
Stanley Choffrey, *GSA*
Dave Fillingham, *NSA*
This panel will discuss efforts to establish and operate a Federal Bridge Certification Authority (FBCA) to support peer to peer, non-hierarchical interoperability among disparate agency PKI domains, and ultimately with PKI domains external to the Federal government. The discussion will cover: (a) how interoperability among Federal agency PKI domains may be effected on a policy and technical level; (b) why the FBCA concept has emerged as the most attractive solution; (c) how the FBCA has been implemented and tested in prototype form at the Electronic Messaging Association Challenge 2000 conference in April 2000; (d) how the production FBCA is being developed; (e) what the principal challenges are on a policy and technical level (including directories and clients); and (f) how the FBCA activities will be managed pursuant by a Federal PKI Policy Authority.
Technical Degree of Difficulty = 3 to 4

Room 308

Incident Response—Tracking Them Down—Part II
Bill Hancock and Charles Neal, *Exodus Communications*
Ok, you've found out you've been attacked, cracked or hacked (depending upon your definition). You may even have stopped it successfully—for now. The problem remains: what do you do about finding out where the attacker is coming from and what can you do to mitigate damage in the future or deal with the attacker in real-time when it happens again. The speakers in this session have been there and done that. Both have many years in tracking down, literally, hundreds of hackers, crackers, cyberterrorists, extortionists and other manners of cybercriminals. This session will provide insight on how to properly track incoming attacker activities, the use of technologies such as "clean" Trojan Horse programs to deceive attackers, the use of "honey pot" and other "attractor" techniques, evidence collection and preservation, chain of custody issues, what law enforcers need and want on prosecutions, and the myriad of other information needed to successfully track attackers to their lair and get law enforcement engaged to prosecute.

Room 309

The Healthcare Vertical Turns Its Eyes on Security—The Impact of HIPAA and other Legislation on Security Engineering (p. 671)
Lisa A. Gallagher, *Exodus Security Services;* and Lewis Lorton, *Forum on Privacy and Security in Healthcare*
This session will provide an accurate and general understanding of relevant healthcare legislation, and will provide specific understanding of patient rights and the requirements for use, disclosure and authorizations for patient records. Topics to be covered in this session include: a history of privacy and security regulations for healthcare, HIPAA and administrative simplification, relevant regulations that flow from HIPAA, how this affects security engineering, compliance issues, and implications of noncompliance.

Room 310

Information Systems Survivability: Protecting Critical Systems (p. 656)
Chair: Robert J. Ellison, *CERT Coordination Center*
Richard C. Linger, *CERT Coordination Center*
John McHugh, *CERT Coordination Center*
Increasing societal dependence on large-scale, distributed information systems amplifies the consequences of intrusions and compromises. It is vital that these critical systems survive to provide essential functions even when operating under adverse circumstances. The objective of this tutorial is to describe practical techniques for survivability analysis and design that attendees can apply in their own environments. In particular, the tutorial introduces the Survivable Network Analysis (SNA) method developed by the SEI's CERT/CC, as a means to assess and improve survivability and security characteristics of planned or existing information systems. The SNA method introduces concepts of mission survivability, essential services, intrusion scenarios, intrusion resistance, recognition and recovery (the three R's), and Survivability Maps. The tutorial will present a case study of survivability analysis, and will discuss survivability research activities.
Technical Degree of Difficulty = 3

Rooms 327—329

Access Certificates for Electronic Services (ACES)—Enabling Government to Citizen Interaction via the Internet (p. 654)
Chair: Judith Spencer, *GSA*
David Temoshok, *GSA*
Stanley Choffrey, *GSA*
The Access Certificates for Electronic Services (ACES) program utilizes industry partners providing COTS solutions designed to facilitate secure on-line access to Government information and services by the Public through the use of a PKI. The ACES vision is that a single member of the public or a business representative would have one digital signature certificate with which he or she could do business with a variety of Federal agencies, including the electronic signing of forms prior to submission. This panel will discuss the value of public key technology and digital signatures for doing business on the Internet, present actual case studies, and provide a live demonstration of an ACES transaction.

Room 330

Paper Session: Common Criteria Issues
Session Chair: (TBD)

Thoughts and Questions on Common Criteria Evaluations (p. 203)
Kenneth G. Olthoff, *NSA*

Towards the Formal Modeling of a Secure Operating System (p. 408)
Dan Zhou, *Florida Atlantic University*

The Open Platform Protection Profile (OP3)—Taking the Common Criteria to the Outer Limits (p. 211)
Marc Kekicheff, *Visa International Services Association*

Rooms 331—332

Issues in High Performance Computing Security (p. 657)
Chair: Rayford B. Vaughn, Jr., *Mississippi State University*
Yvo Desmedt, *Florida State University*
Douglas Engert, *Argonne National Laboratory*
Jesse Pollard, *DoD*
This panel is composed of researchers and practitioners in the area of high performance computing (HPC) security and its purpose is to address whether or not HPC represents new security issues or whether traditional solutions apply. This topic has been addressed at the NISSC for the past two years in the form of technical papers—but the opportunity has not yet been presented for a panel discussion on the topic. This panel seeks to close that gap and to describe not only positions associated with this interesting topic, but to also describe current research in the field.

8:30am—10:00am

Rooms 301—303

Guerilla Security: The Martial Art of Infosecurity (p. 699)
Andrew T. Robinson, *net/main InfoSecurity Solutions*

While the basic principles of InfoSecurity have not changed in decades, the needs and realities of the InfoSecurity threat environment have changed radically in the past few years. Many InfoSecurity policies have failed to adapt to this reality. Such inertia means that the InfoSecurity policy does not adapt to the needs of the organization and to new threats. Guerilla Security, also called RAPID (Rapid Policy Innovation & Deployment) is a methodology based on flexibility and rapid response. These characteristics allow an organization to practice conservative InfoSecurity practices while remaining responsive to the needs of the organization and to new InfoSecurity threats.

Room 307

Your Always-On Connection & the Telecommuter (p. 618)
Chair: Peter Dinsmore, *NAI Labs, Network Associates*
Michael St. Johns

Always-on Internet access to the home provided by emerging broadband technologies such as cable modems and DSL is changing the way we live and work. Reasonable bandwidth connections coupled with instant and constant access is integrating the Internet into our lives. This panel will explore the security implications of not only this new technology, but also of the changing work models. What are the risks to a home user? To a telecommuter? What are the risks to corporations that set up virtual offices over the Internet? This panel will also explore the solutions that are available. Do I need a personal firewall? What will a VPN provide? Finally, the panel will explore what the future might hold.
Technical Degree of Difficulty = 4

Room 308

Distributed Denial of Service Attacks—Can We Survive This New Threat? (p. 682)
Chair: Jon David, *Lehman Brothers*
Steve Bellovin, *AT&T Labs Research*
Bill Cheswick, *Lucent Technologies*
Paul Ferguson, *Cisco*

DDoS attacks have recently made headlines by taking down major networks and services. The sharing of attack "enhancements" and the providing of attack tools via the Web makes these attacks a growing threat. This session investigates the nature and elements of DDoS attacks, and presents things to be done by users, sys admins, ISPs, router vendors and the like to best treat this threat. Key areas it will treat are: What is a DDoS attack? How is DDoS different from other threats? Can they be detected in time? What security/network practices need be in place? What user preparation is necessary for DDoS hits? What industry preparation is necessary for DDoS?

Room 309

Understanding FIPS 140-2 Validation (p. 712)
John Morris, *Corsec Security*

Hear a former FIPS 140-1 lab manager explain what these cryptographic module security certifications truly mean, how they affect government purchasers and commercial vendors, and how future validations will change. The session will include an interaction with the audience and candid discussion on FIPS 140-2 and other government security validations. Explore whether current US and Canadian security standards effectively enhance COTS cryptography products designed by international companies.
Technical Degree of Difficulty = 3

Room 310

Single Sign-on: Myth or Reality (p. 685)
Thomas Peltier, *Netigy Corporation*

As enterprise computing becomes more and more complex, with business systems installed across multiple platforms, form mainframe to client-server to PC, the need for a secure way to provide users with a single authentication point becomes more and more important. There are a number of methods and products on the market today with which we will examine what you will need to do to be prepared for secure single sign-on. We will also identify a set of functional requirements for a secure single sign-on methodology, so that attendees will be better able to compare the products available.
Technical Degree of Difficulty = 3

Rooms 324—326

Strong Authentication
Chair: Fred Tompkins, *KTSI*
(TBD)

Strong authentication is characterized by the use of at least two kinds (or pieces) of evidence, at least one of which is resistant to replay. While there is a consensus for this kind of solution among security people, it has been resisted by management as expensive and by users as awkward or burdensome. This panel will demonstrate several desktop-based commercial solutions to this problem. These solutions will be used to demonstrate that the cost is measured in pennies per user per day and that by basing the solution on the desktop, the solutions can be made easy for the user.

Room 327—329

"Hands-On" Approach of Building a Security Program (p. 684)
Bill Hadesty, *USDA*

One of the Federal Government's largest civilian departments has hired you to put a new IT security program in place quickly with limited funding. Where do you start when the goal is to have the Department of Agriculture become a model for computer security in three years? Where do you start when your boss was one of the authors of the Computer Security Act of 1987? This is the challenge faced by Bill Hadesty as the Associate CIO for Cyber Security at USDA. Drawing on experience gained while developing and implementing a similar program at the IRS, Mr. Hadesty will outline strategies for providing executive leadership and direction, ensuring compliance with laws and regulations, establishing and enforcing standards and policies, and providing security expertise and oversight.
Technical Degree of Difficulty = 1

Room 330

Paper Session: Architectures
Session Chair: (TBD)

Chain of Trust in a Digital Signature System Based on a Smart Card (p. 267)
Jean-Luc Giraud, *Gemplus, France*

An Efficient Secure Authenticated Group Key Exchange Algorithm for Large and Dynamic Groups (p. 254)
Jim Alves-Foss, *University of Idaho*

Business Process Driven Framework for Defining an Access Control Service Based on Roles and Rules (p. 234)
Ramaswamy Chandramouli, *NIST*

Rooms 331—332

Information Security Research and Development in Academia (p. 706)
Chair: Susan M. Bridges, *Mississippi State University*
Blaine W. Burnham, *University of Nebraska*
Dipankar Dasgupta, *University of Memphis*
James A. Davis, *Iowa State University*
Cynthia Irvine, *Naval Postgraduate School*

Research and development activities in information security within academia have been rather limited until quite recently. This increase in interest is also reflected in an increase in funding available from government agencies such as NSF, DARPA, and NSA for research in information security and it is likely that more universities will be moving into this area. This panel will present a sampling of the types of research in the area of information security that are being conducted at universities.
Technical Degree of Difficulty = 3

9

Conference at a Glance

Room	8:30–10:00	10:30–12:00	1:30–3:00	3:30–5:00
301–303	Killer Apps—and You're Dead Meat (The Code that Shagged Me)		Systems Security Engineering Capability Maturity Model	Government Use of Systems Security Engineering Maturity Model
307		**Opening Plenary Keynote Speakers: Lieutenant General Michael V. Hayden Dr. Dave Farber** **Systems Security Award: Dr. Eugene Spafford, Purdue University**	Future of Information Security	Evaluation Scope: Does One Size Fit All?
308			Advanced Encryption Standard and Beyond	State of Key Recovery for the Government and Industry
309			NIAP/CC Scheme Presentations	NIAP Projects—2001
310			Effective Risk Analysis	Network-Based Contingency Plans
324–326	**Solutions**			
327–329	An Overview to the Conference		Secret and Below Interoperability (SABI)	Defensewide Information Assurance Program
330 **Papers**	Student Papers		Intrusion Detection	Practices, Curses, and Risks
331–332	Incident Response Fundamentals		New Security Paradigms Workshop 2000	Security of Source-Available Systems

Room	8:30–10:00	10:30–12:00	1:30–3:00	3:30–5:00
301–303	Aspects of InfoSec: The UK View	Security in B2B e-Commerce	Protection of B2B Exchanges and Vendor Operations	Enterprise Security Infrastructure
307	Certified vs. Secure	PKI—Sham or Salvation?	Federal Bridge Certification Authority (FBCA) Demonstration and Panel Part I	Federal Bridge Certification Authority (FBCA) Demonstration and Panel Part II
308	Achieving Global Trust in an e-World	Guideline for Implementing Cryptography in the Federal Government	Incident Response—Stopping Them Dead in Their Tracks	Incident Response—Tracking Them Down Part II
309	Common Criteria Tools: A Status & Demonstration	Innovative Uses of the Common Criteria	The Common Criteria Structures: Healthcare	Healthcare Vertical Turns Its Eyes on Security
310	Preparing for Intrusion Detection	Privacy in the Information Age	Operational Computer Forensics —The New Frontier	Information Systems Survivability: Protecting Critical Systems
324–326	**Solutions**			
327–329	Progress of the Best Security Practices Subcommittee	Critical Infrastructure Protection for Chief Information Officers or CIP for CIOs		Access Certificates for Electronic Services (ACES)—Enabling Government to Citizen Interaction via the Internet
330 **Papers**	Access Control	Malicious Code	Case Studies	Common Criteria Issues
331–332	Security and Quality of Service Interactions	RSA Digital Signature Standards	Information Assurance Metrics: Prophecy, Process, or Pipedream	Issues in High Performance Computing Security

Room		8:30–10:00	10:30–12:00	1:30–3:00	3:30–5:00
301–303		Guerilla Security: The Martial Arts of InfoSecurity	Intro to Consequence-Based Risk Assessment	Information Security Year in Review—Technical Vulnerabilities	Information Security Year in Review—Computer Crime
307		Your Always-On Connection & the Telecommuter	Security for High-Speed Internets	DNS Security Ready for Prime Time	Real Security for Standards Based Network Management
308		Distributed DDOS: Can We Survive?	How Do We Prevent Denials of Services	Black Hat—White Hat	Recent Trends in Hacking
309		Understanding FIPS 140-2 Validation	PP for FIPS 140-2: Lessons Learned	Testing of Crypto Modules Against FIPS 140-2	Cryptographic Module Validation Program
310		Single Sign-On: Myth or Reality	Biometrics – Understanding the Architecture, API's, Encryption and Authentication Security for Integration into Existing Systems & Applications	Scorecard for Online Authentication Technologies	The OM-AM Framework and Role-Based Access Control
324–326	**Solutions**	Focused Solutions 2000: Strong Authentication	Focused Solutions 2000: Desktop Security	Focused Solutions 2000: End-to-End Encryption	Focused Solutions 2000: Certificate Based Administration
327–329		"Hands-On" Approach of Building a Security Program	Working on a Shoestring – Dealing with Your Security Problems in the Absence of Funding	Cybersecurity in the Year 2000: Not Just for Administrators Anymore	Professional Certification of Information Security Professionals
330	**Papers**	Architectures	Refocused Views	Information Access Issues	Prefocused Views
331–332		Information Security Research & Development in Academia	Information Security Laboratories in the Academic Setting	Innovations in Biometric Authentication Technologies	Certificates in the Internet: State, Issues, and Futures

Room		8:30–10:00	10:30–12:00	1:00–6:00
301–303		Collusion Detection Las Vegas Style		
307		MLS & Its Evolution	**Closing Plenary Panel Discussion:** Michael J. Jacobs Mr. Simon Gauthier Dr. William O. Mehuron	**Post Conference Workshops:** See pages 16 & 17 for Workshop Descriptions
308		Tracking the Virus Writer: The Legal Ramifications		
309		Anonymity in the Information Age		
310		IA Technologies: 10 Years Past, Present & Future		
324–326	**Solutions**	Best Security Practices: Lowering Quality's Total Cost		
327–329		Computer Security from the Trojan War to Now		
330	**Papers**	Operating Systems and Their Effects on Information Security		
331–332		Smart Card Security Users Group PP & Projects		

10:30am—12:00 noon

Rooms 301—303

An Introduction to Consequence-Based Risk Assessment (p. 738)
George Jelen, *G-J Consulting*
    This tutorial will present the basics steps involved in a consequence-based IT risk assessment, the advantages of a consequence-based approach, and the differences and relationships among threat, vulnerability and risk. It will show how qualitative threat, vulnerability and consequence information can be combined to derive a qualitative value for risk and offer an easy-to-understand graphical way to present risk assessment results. The tutorial will conclude with a brief discussion of uncertainty and risk mitigation.
Technical Degree of Difficulty = 1

Room 307

Security for High-Speed Internets (p. 721)
Chair: Jeff Ingle, *Community Management Staff*
Chris Kubic, *NSA*
    The explosion in the growth of the Internet and private networks has been driving faster network speeds and increased services. New technologies and protocols are fueling this growth and are expected to meet the increasing bandwidth demands. Security could be an enabling factor in this growth, but there are some strong challenges in providing the security and survivability for future networking. Some of the security and survivability challenges in future networking include encryption, authentication, key management, data integrity, the role of firewalls and guards, and scaling network and security management.
Technical Degree of Difficulty = 4

Room 308

How Do We Prevent Denials of Service? (p. 723)
Chair: Peter G. Neumann, *SRI International*
Steve Bellovin, *AT&T Labs*
Virgil Gligor, *University of Maryland*
J.F. Mergen, *Genuity*
Marv Schaefer, *ARCA*
    Subsequent to earlier denial-of-service (DoS) flooding attacks, the flurry of distributed denial-of-service attacks in February 2000 has intensified the realization that the problems we face lie deep in our information infrastructures—inadequate protection and integrity in operating systems, networking, protocols, mailer environments and many other applications, and operational practice. This panel explores what (if anything) can be done to combat denials of service from a total systems/network perspective, hopefully without too seriously compromising the performance that everyone has come to expect.
Technical Degree of Difficulty = 5

Room 309

A Protection Profile for FIPS 140-2, Lessons Learned (p. 740)
Chair: Miles Smid, *CygnaCom Solutions*
Jean Petty, *CygnaCom Solutions*
Shari Galitzer, *CygnaCom Solutions*
Ray Snouffer, *NIST*
    NIST's Cryptographic Module Validation program has been highly successful validating over 95 cryptographic modules as being compliant with FIPS 140-1. Recently, NIST has drafted a revision of the standard (Draft FIPS 140-2) that offers several improvements, but the testing process remains basically intact. This presentation will explore the feasibility of developing a Common Criteria based Protection Profile for Draft FIPS 140-2. The presentation will cover the lessons learned when trying to map a previously existing standard into the Common Criteria and in developing the corresponding protection profile.
Technical Degree of Difficulty = 3

Room 310

Biometrics—Understanding the Architecture, API's, Encryption and Authentication Security for Integration into Existing Systems & Applications (p. 729)
William H. Saito, *I/O Software, Inc.*
    This session will explain how to implement and build biometric technology to augment current security systems while explaining specific issues. We will investigate the major biometric technologies, where they fit, and the questions you should ask when looking at these products.
    Learn how to approach biometric authentication including:
• Seamlessly developing biometrics to enhance your existing security.
• Developing a common methodology for software developers looking to integrate biometrics into their applications.
• Client/Server programming issues to consider.
• User enrollment problems and solutions.
• Developing API's (Application Programming Interface) to implement a secure system.
Technical Degree of Difficulty = 5

Rooms 324—326

Desktop Security
Chair: Oscar Marcia, *Deloitte & Touche*
(TBD)
    For almost four decades now we have worried about Trojan Horse attacks against the mainframe. To date, we have resisted such attacks by recognizing and removing known attack objects. While this worked reasonably well against broad attacks, there is every reason to believe that such defenses will be useless against focused attacks. This panel will present several commercial-off-the-shelf products for securing the desktop. These products may be stand-alone or integrated with strong authentication called for in the first panel. They may permit some user control but permit management to implement policies which users cannot override.

Rooms 327—329

Working on a Shoestring (p. 727)
Chair: David Jarrell, *GSA*
Steve Lipner, *Microsoft Security Response Center*
Shawn Hernan, *CERT Coordination Center*
Kenneth Ammon, *Network Security Technologies, Inc.*
    It is a generally accepted assumption that network and system security solutions require sizeable financial resources to implement. Although this may be true for many options, there are some grassroots fundamentals that, when put into practice, can make an immense difference in the overall security profile of your network or computer system. Understanding the interrelationships for the elements of a computer security program and some basic practices is the key to an effective computer network defense.
Technical Degree of Difficulty = 1

Room 330

Paper Session: Refocused Views
Session Chair: (TBD)

Rethinking Department of Defense Public Key Infrastructure (p. 303)
Jason X. Hackerson, *The Meredith Group*

Corporate Vital Defense Strategy: A Framework for Information Assurance (p. 288)
Bel G. Raggad, *Pace University*

Trends in Government Endorsed Security Product Evaluations (p. 279)
Rick Smith, *Secure Computing Corporation*

Rooms 331—332

Information Security Laboratories in the Academic Setting (p. 739)
Chair: Blaine W. Burnham, *University of Nebraska*
Cynthia Irvine, *Naval Postgraduate School*
Willis Marti, *Texas A&M University*
Deborah Frincke, *University of Idaho*
(TBD), *US Military Academy*
    Developing a hands-on laboratory experience is one of the most challenging aspects of creating an academic program in information security. Several academic institutions are in the process of making that investment in developing and presenting information security lab courses. This panel will have representatives of these colleges describe in some detail the lab development, the context for the lab, overrearching considerations they encountered within their schools, and progress to date.
Technical Degree of Difficulty = 1

1:30pm—3:00pm

Room 301-303

Information Security Year in Review—Technical Vulnerabilities (p. 766)
David Kennedy, *ICSA, Inc.*

A 90-minute review of the major technical vulnerabilities discovered in systems during the previous 12 months (Oct 99–Sep 00). The tutorial will include discuss categories of technical problems and draw from CERT advisories, hardware and software vendor's advisories and public discussion forums. The intended audience is Information Security (IS) managers and practitioners who are too busy to monitor all of these forums. The tutorial will provide a snapshot of major problems and trends that have emerged since the last NISSC.
Technical Degree of Difficulty = 5

Room 307

Security for Domain Name System—Ready for Prime Time (p. 743)
Chair: Olafur Gudmundsson, *NAI*
David Conrad, *Nominum/ISC*
Edward Lewis, *NAI*
John Nguyen, *DISA*

A secured Domain Name System is becoming an operational reality with the latest release of the BIND software by the Internet Software Consortium. Besides being able to trust the name-to-address mapping, DNS will offer benefits to other protocols by making public keys available through DNS, and by accommodating certificates.

This panel will be of interest in learning how it can be secured and anyone that wants to make plans to take advantage of DNSSEC.
Technical Degree of Difficulty = 5

Room 308

Black Hat—White Hat (p. 751)
Chair: G. Mark Hardy, *Guardent, Inc.*
Mark Fabro, *Guardent, Inc.*
Ray Kaplan, *Guardent, Inc.*
Ralph Logan
Black Hat One *(name and organization withheld)*
Black Hat Two *(name and organization withheld)*

This panel discussion will feature a lively interaction between several well-known "white hat" security experts, and a number of "black hat" speakers (the "dark side" of the hacking community). The goal of this session is provide a question-answer session for attendees to investigate the latest methods used to protect information assets, and what methods are used to attack them. Warning: the black hat presenters will not hesitate to "tell it like it is."
Technical Degree of Difficulty = 4

Room 309

Testing of Cryptographic Modules Against FIPS 140-2 (p. 768)
Chair: Randall Easter, *NIST*
Annabelle Lee, *NIST*
Ray Snouffer, *NIST*

On July 17, 1995, NIST established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to FIPS 140-1, and other FIPS cryptography based standards. The CMVP offers a documented methodology for conformance testing through a defined set of security requirements in FIPS 140-1 & 2 and other cryptographic standards. The panelists will provide detailed information on the philosophy and goals of cryptographic module testing, the DTR, conformance/compliance testing, and cryptographic module laboratory accreditation.
Technical Degree of Difficulty = 4

Room 310

Scorecard for Online Authentication Technologies
Dow Williamson, *RSA Security, Inc.*

Authentication—the independent validation of the identity of a user, server, or process—is critically important for e-commerce. This session provides a common set of criteria by which to evaluate different mechanisms and an objective "scoreboard" of several popular choices, including username/password, hardware tokens, software tokens, Kerberos, digital certificates, smart cards, and biometrics.
Technical Degree of Difficulty = 4

Room 324—326

End-to-End Encryption
Chair: David Kennedy, *ICSA, Inc.*
(TBD)

The modern network often provides multiple paths between any two points. Such routing improves the probability that a path will be available and may also provide additional bandwidth on demand. However, traffic may not follow the path that management expects. If the traffic is successfully limited to a reliable path, this path may not be the cheapest, most convenient, or even available when needed. This panel will present a number of commercial-off-the-shelf solutions that secure the traffic all the way from the client to the server. These solutions work across arbitrary networks.

Room 327—329

Cybersecurity in the Year 2000: Not Just for Systems Administrators Anymore (p. 752)
Chair: Richard Shullaw, *HHS*
Danny Markley, *HHS*
Robyn Large, *The Center for Support of Families*
Marianne Swanson, *NIST*

This panel will look at the issues of cybersecurity as they affect child support enforcement programs. At the Federal and State levels of government, this program provides substantial benefits to single parents and their children. National information systems support State efforts to increase the amount of child support collected. Because of the scope of the data, and the sensitivity of the information, we have taken active steps to ensure privacy and security of data.
Technical Degree of Difficulty = 1

Room 330

Paper Session: Information Access Issues
Session Chair: (TBD)

Controlling Primary and Secondary Access to Digital Information (p. 351)
Marshall D. Abrams, *The MITRE Corporation*

A Query Facility for Common Intrusion Detection Framework (p. 317)
Sushil Jajodia, *George Mason University*

Secure X.500 Border Directory Proxy Server
Karen M. Goertzel, *Wang Government Services, Inc.*

Room 331—332

Innovations in Biometric Authentication Technologies (p. 766)
Chair: Jeff Dunn, *NSA*
Cathy Tilton, *SAFLINK*
Fernando Podio, *NIST*

With the advent of the new century, it has become apparent that there is a great need for biometrics. Utilized alone or integrated with other technologies such as smart cards, encryption keys, and digital signatures, biometrics are set to pervade nearly all aspects of the economy and our daily lives. The need for biometrics can be found in commerce, in Federal, State and Local governments, in the military and in commercial applications. Trustworthy electronic commerce and electronic government, for example, can be achieved through the utilization of strong personal authentication procedures. Trust in these electronic transactions will be essential to the healthy growth of the global economy.
Technical Degree of Difficulty = 4

13

3:30pm—5:00pm

Rooms 301—303

Information Security-Year in Review—Computer Crime (p. 783)
Mich E. Kabay, *ADARIO, Inc.*

A 90-minute review of some of the most significant computer crime incidents of the year (Oct. 99–Sep. 00). The intended audience is Information Security (IS) managers and practitioners who want a short, non-technical summary of case reports drawn from news wires and Web-based news sources. The course materials are often useful to update the participants' own security awareness presentations; electronic (PowerPoint and Acrobat) versions of the course materials are made freely available to all participants by the author.
Technical Degree of Difficulty = 2

Room 307

SNMPv3 with Security and Administration (p. 770)
Chair: Jeffrey D. Case, *SNMP Research Inc.*
Russ Mundy, *SNMP Research Inc.*

The Internet-standard management framework, based on SNMP, has become a global standard for managing Internets and Intranets. As a result of these application environments, there are requirements for strong security for the management function in many environments. This panel session will describe SNMPv3 from the standards view, the vendor view, and the user view. The session will also address the security architecture, layering, and operations, including key management and coexistence and transition issues.
Technical Degree of Difficulty = 4

Room 308

Recent Trends in Hacking (p. 771)
Chair: Peter Mell, *NIST*
Tom Longstaff, *CERT*
Jeff Moss, *DEFCON*
Andy Balinsky, *Cisco*
Chris Rouland, *ISS*

If hacking techniques remained constant, the problem of computer security would have been solved long ago. Instead, previously unseen hacking paradigms emerge each year that take advantage of new features in software and circumvent security mechanisms. This panel will begin with a history of hacking events and developments starting from the 1970s to the present day. Then, experts from the hacking community, an incident handling organization and a security vendor will discuss emerging hacking trends from their unique vantagepoint.
Technical Degree of Difficulty = 4

Room 309

The Cryptographic Module Validation Program: FIPS 140–2…The Next Generation (p. 790)
Chair: Annabelle Lee, *NIST*
Ray Snouffer, *NIST*
Tom Casar, *CSE, Canada*

In the Fall of 1998, FIPS 140-1 entered a regularly scheduled 5-year review to consider new and/or revised requirements needed to meet technological and economic change. A revised draft standard was produced based on the public comments received, previously issued implementation guidance and a "line by line" review by the NIST, CSE, and testing laboratory staff. Completion of the FIPS 140-1 update to FIPS 140-2 is anticipated by October 2000.
Technical Degree of Difficulty = 2

Room 310

The OM-AM Framework and Role-Based Access Control (p. 600)
Ravi S. Sandhu, *George Mason University*

Cyberspace security is fundamentally about control of authority and trust. We don't know what form future systems will take, but they will surely be very different from today's. We can postulate they will be large-scale, highly decentralized, pervasive, cross organizational boundaries and evolve rapidly. Current security doctrine cannot deal with this complex and fluid environment that is inevitably emerging. This tutorial will discuss the speaker's recently proposed OM-AM framework as a promising approach to security engineering in this brave new world.
Technical Degree of Difficulty = 3

Rooms 324—326

Certificate-Based Access Control and Administration
Chair: Bill Murray, *Deloitte & Touche*
(TBD)

Historically, access control data, that is the rules of user access or privileges and capabilities, have been stored on or near the target system. The data has been trusted because these systems have resisted arbitrary changes to the data. This panel will present a number of commercial-off-the-shelf systems where user credentials, privileges, and capabilities are stored on the desktop and administered from a single (central) interface. The credentials, privileges, capabilities are signed by the issuer and trusted because of where they were issued rather than because of where they have been stored. Because a target system need trust only credentials, privileges, and capabilities that it (or its management) issued, the target and the user need not be in the same domain of trust. In other words, these systems can be expected to scale beyond the enterprise.

Rooms 327—329

Professional Certification of Information Security Professionals (p. 773)
Chair: Lynn McNulty, *RSA Security*
James Wade, *Air Touch Cellular*
William Murray, *Deloitte & Touche*
Shirley Malia, *Critical Infrastructure Assurance Office*
Joan Hash, *Social Security Administration*

This panel will focus on the current status of efforts to elevate the status and effectiveness of information security specialists through the development of professional certification programs. Recent changes to the Federal Government's information technology occupation series recognize that information security has become a separate and distinct career field. The Office of Personnel Management recognizes Professional certification as being one of the criteria for qualifying for government information security positions. The members of the panel will discuss various aspects of professional certification.
Technical Degree of Difficulty = 1

Room 330

Paper Session: Refocused Views
Session Chair: (TBD)

Database Security 2000 (p. 388)
John R. Campbell, *NSA*

Privilege Management of Mobile Agents (p. 362)
Wayne Jansen, *NIST*

Towards XML as a Secure Intelligent Agent Communication Language (p. 371)
Alexander D. Korzyk, *Sr., Virginia Commonwealth University*

Rooms 331-332

Certificates in the Internet: State, Issues, and Futures (p. 784)
Andrew Nash, *RSA Security, Inc.*

This presentation examines current progress, issues, and future directions in IETF work on Internet certificate usage. A certificate profile and operational protocols have been published. Current topics include high assurance qualified certificates; management protocol alternatives, application integration (e.g., S/MIME, IPsec), time stamping, and attribute certificates for authorization.
Technical Degree of Difficulty = 4

8:30am—10:00am

Rooms 301—303

Collusion Detection Las Vegas Style (p. 813)
Jeff Jonas, *Systems Research & Development*
    Protecting an organization's assets is becoming an increasingly complex task. The back-and-forth war between attack and defense invariably means creating more sophisticated policies, procedures, and controls. However, even the most advanced protection measures can be rendered useless by collusion. Collusion Detection Technology (CDTECH) provides organizations with a new weapon against the insidious threat of collusion.
Technical Degree of Difficulty = 2

Room 307

Multi-level Security (MLS) and Its Evolution to Date (p. 792)
Chair: G.R. "Greg" Clingan, *Impact Innovations Group, LLC*
Christian Cooke, *Impact Innovations Group, LLC*
Thomas Bess, *Impact Innovations Group, LLC*
    This panel will discuss the evolution of MLS starting with early efforts in the middle of the last millennium, early use of mechanical ciphers to maintain levels of data security. The panel will go on to discuss MLS in a computerized age taking a look at systems developed for the government and in the private sector.
Technical Degree of Difficulty = 3

Room 308

Tracking the Virus Writer—The Legal Ramifications (p. 794)
Chair: Christine M. Orshesky, *IFsec, LLC*
Chengi "Jimmy" Kuo, *Network Associates, Inc.*
Jessica Herrera, *Department of Justice*
Sarah Gordon, *IBM Research*
(TBD), *FBI*
    The growing prevalence of denial of service virus attacks has brought law enforcement attention to the computer virus and malware situation. This panel is composed of law enforcement professionals and those that assist in virus investigations and as such can provide insight into the legal requirements and ramifications of virus writing and virus distribution. It is the aim of the panel to provide the online community with ways to effectively address this threat and affect decisions made about appropriate punitive or restitution matters.
Technical Degree of Difficulty = 2/3

Room 309

Anonymity in the Information Age (p. 827)
Chair: Blaine Burnham, *University of Nebraska*
Tony Bettini, *Guardent Technologies*
Ed McPherson, *PWC*
Hans von Spakovsky
Robyn Wagner

    Anonymity in the information age is positioned to be one of the most contentious issues to be resolved. This panel will explore the issues of just what is the notion of anonymity, how does this notion translate/relate to processes on the Internet, what are some of the available mechanisms and how do they work, who are the stakeholders and what is their take on the status of the discussion.
Technical Degree of Difficulty = 2

Room 310

Information Assurance Technologies: 10 Years Past, Present, & Future (p. 810)
Chair: Jack Murphy, *Electronic Data Systems*
Gary Moore, *Entrust Technologies, Inc.*
Tom Haigh, *Secure Computing Corporation*
Robert Giovagnoni, *iDEFENSE*
Ronda Henning, *Harris Corporation*
    In the next decade Information Assurance will dominate the attention of many CIOs. Simple amateurish e-mail viruses continue to plague CIOs. Professional hackers are becoming more sophisticated every year in identifying and exploiting network, host, and application vulnerabilities. Rapid, effective response to these threats is one of today's biggest problems. This panel consists of five representatives of the Information Assurance industry who will discuss the evolution of Information Assurance technologies and solutions over the next 10 years.
Technical Degree of Difficulty = 2-4

Rooms 324—326

Best Security Practices: Lowering Quality's Total Cost of Ownership in an Age of Growing Complexity (p. 626)
Chair: James P. Craft, *United States Agency for International Development (USAID)*
Tom Burke, *GSA*
Jack L. Brock, Jr., *GAO*
Guy L. Copeland, *Computer Sciences Corporation*
Robert E. Giovagnoni, *iDEFENSE*
    Best practices efforts have provided useful benchmarks to guide users embarking into areas of new endeavor. The CIO Council's Best Security Practices website takes this idea to a new level. The Federal government is facing enormous costs to secure its IT infrastructure. Avoiding some of these costs will take a new definition of best practices.
Technical Degree of Difficulty = 2

Rooms 327—329

Computer Security from the Trojan War to Now (p. 797)
Charles P. Pfleeger, *Exodus Security Services*
    This history of computer and network security has an unfortunate habit of repeating itself. Although one may think that virus attacks are a phenomenon of just the past few years, in fact, they and other computer security problems have

been with us for several decades. But worse, some lessons learned the hard way a long time ago are being relearned today. This talk will cover the highlights of the history of security, with special emphasis on past problems and solutions that should be known by modern computer security professionals. The talk will identify some of the fundamental work in and pioneers in computer security, and show the relationships between their contributions and the current computer security situation.
Technical Degree of Difficulty = 4

Room 330

Paper Session: Operating Systems and Their Effects on Information Security
Session Chair: (TBD)

An Operating System Analog to the Perl Data Tainting Functionality (p. 392)
Dana Madsen, *U.S. Air Force*

A Taxonomy of Organizational Security Policies (p. 225)
Gary W. Smith, *Science Applications International Corporation*

Policy-Enhanced Linux (p. 418)
Paul C. Clark, *Naval Postgraduate School*

Rooms 331—332

Smart Card Security Users Group Protection Profile & Projects
Chair: Kenneth Ayer, *Visa International*
Douglas E. McGovern, *Ray-McGovern Technical Consultants, Inc.*
Fernando Lourenco, *Europay International*
Marc Kekicheff, *Visa International*
    Smart Cards have been around for more than 20 years and are widely used in the financial services and telecommunications industries. They have recently been improved to carry multiple applications, potentially including private keys that can work in conjunction with secure network access. Their security has been assured by proprietary testing and evaluations by their users and the payment associations users have formed to facilitate their common business interests. Recently efforts have been made to bring this security testing in to the Common Criteria (ISO 15408) process. This is not straightforward. This panel overviews the experiences of the Smart Card Security Users Group (American Express, Europay, JCB, MasterCard, Mondex, Visa, and NIAP) in adapting the Common Criteria for the evaluation of smart cards.
Technical Degree of Difficulty = 3

Workshop
Programs

10:30am–12:00 noon
Closing Plenary
Rooms 307–310

Mr. Michael J. Jacobs,
*Deputy Director For
Information Systems Security,
National Security Agency*
Mr. Jacobs is the
Deputy Director for
Information Systems
Security at the National
Security Agency (NSA). Under his leadership, NSA is implementing an Information Assurance (IA) strategy to protect the Defense Information Infrastructure and, as appropriate, the National Information Infrastructure.

Mr. Simon Gauthier,
*Deputy Chief,
Information Technology
Security, CSE, Canada*
Mr. Gauthier began
his career at CSE in
1985, and has held the
roles of Director of
SIGINT Engineering Group and Director, Cryptanalytic Exploitation and Research. On June 29, 1998, he was appointed Deputy Chief, Information Technology Security (DCITS).

Dr. William O. Mehuron,
*Director,
Information Technology
Laboratory, NIST*
Dr. Mehuron is the
Director of the
Information Technology
Laboratory of the National
Institute of Standards and Technology (NIST). He has held a number of senior management and technical positions in the federal government (including civilian, defense, and intelligence agencies) and in high technology industries. In these positions, he has been responsible for research, development and acquisition of information systems, sensor and observing systems, and advanced electronic systems.

16

Thursday, October 19, 2000, 1:00pm—6:00pm

Investigating Computer Virus and Other Malware Incidents

Christine M. Orshesky, *IFsec, LLC*

With the increasing spread of computer viruses and worms that can lurk in an organization, it is no longer feasible to rely solely on single-point detection and repair techniques. Virus-related incidents must be investigated to determine where the virus originated, where it spread, and what damage it may have caused or may cause in the future. This workshop will show you how to make those determinations through effective response and investigation techniques for computer viruses and other malware incidents. The workshop will provide a brief foundation on the functionality of computer viruses and other forms of malware with an emphasis on the ways they can enter an organization, the ways they spread, and the types of damage they can cause. Key techniques in the response and investigation of such incidents will be discussed and demonstrated. You will have a hands-on opportunity to investigate several computer virus and malware incidents.

Staying Ahead of the Hackers: Network Vulnerability Testing

Ken Cutler, *Information Security Institute*

Protecting and auditing Internet-TCP/IP network technology is a major challenge. In this state-of-the-art session, you will learn how to systematically test the security of important security hot spots for entire TCP/IP networks as well as for individual systems. You will receive the necessary guidance to build a versatile and powerful cyberspace audit toolkit to test for serious TCP/IP network security vulnerabilities that are frequently exploited by hackers and other intruders. The session agenda includes: an evaluation of the significance of recent incidents, advisories, and trends in network attacks and vulnerability conditions; a systematic, graduated plan for "discovering" a network and identifying serious vulnerabilities; sources for obtaining vital information and tools associated with detecting serious Internet/Web security exposures; methods for reviewing freeware,

shareware, and commercial tools for auditing the security of individual servers, firewalls, and entire TCP/IP networks, including: network discovery tools, network mappers, port scanners, network security scanning tools, host security scanning tools, and firewall and web server security testing techniques. This session assumes a working knowledge of TCP/IP and client/server technology.

Information System Survival School

Gail Brooks, *Mary Washington College*

Are you just getting started in information security? This course has been designed to help you come up to speed on the significance of computer and network attacks that are directed at your systems! No prerequisites are needed. The axioms of information assurance, confidentiality, integrity, and availability are introduced with examples of real attacks and defensive countermeasures. The most current attacks on the Internet are detailed against an historical backdrop so students can develop a sense of perspective. One attack—the RingZero proxy scanning trojan—is discussed in depth by the analysts who discovered it. This illustrates not just the significance of trojan-based attacks, but the kind of team-based analysis needed to run aground new hacker ploys. A discussion of information warfare at the national level and the issues of infrastructure protection will lead into a "from the trenches" process for incident handling.

Cryptography for Beginners: What Is It and How Can I Use It?

Jim Litchko, *Litchko & Associates, Inc.*

KEY, RSA, PKI, SET, SSL, VPN, PGP...As with all things technical or bureaucratic, these three letter acronyms surrounding e-commerce can present a conundrum to information professionals charged with securing the business transactions of their company. This session bridges the technical, the bureaucratic, and the social. Specifically, the session offers you an explanation of cryptographic basics, concentrating on the tools and methods necessary for privacy for business transactions and their

uses in electronic commerce. This is not a technical presentation to discuss technical characteristics of the schemes. The session is specifically aimed at the individual who cares less about the mathematics behind the techniques and more about the what, why, and how of cryptographic tools for protecting digital information. The word "practical" is key. Using blocks, pens, hoses, rope, and real-world case studies, the instructor will explain what secret key, public, and hashing algorithms are and how they address security problems for electronic commerce and everyday situations. More importantly, you will learn when it is appropriate to use cryptography and when it is not. Examples from such fields as military, banking, Internet gambling, healthcare and more will be featured.

Introduction to the National Certification and Accreditation Approach (The NIACAP)

Mark S. Loepker, *National Security Agency*
Barry Stauffer, *Corbett Technologies, Inc.*

The National Information Assurance Certification and Accreditation Process (NIACAP) establishes a national standard process, a set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the Information Assurance (IA) and security posture of an organization. The NIACAP focuses on the organization's mission and information system (IS) business case. In this workshop you will see that the process is designed to certify that the IS meets well-defined and agreed-to accreditation requirements and will continue to maintain the accredited security posture throughout the system life cycle. You will also see that the NIACAP is adaptable to any type of IS and any computing environment and mission. You will learn how the process can be adapted to include existing system certifications and evaluated products, and how users of the process must align the process with their program strategies and integrate the activities into their enterprise system life cycle. You will see that while NIACAP maps to any system life-cycle process, its four phases are independent of the life-cycle strategy.

Introduction to the Common Criteria (CC), Common Evaluation Methodology (CEM), and Common Criteria Toolbox

Michael McEvilley, Mitretek Systems, Inc.
Gary Grainger, Mitretek Systems, Inc.
Frank Belvin, The MITRE Corporation

With the growing need for an internationally recognized and flexible criteria to specify security requirements and to replace the inflexible Trusted Computer Systems Evaluation Criteria (TCSEC), DoD 5200.28, the Common Criteria for Information Technology Security Evaluation, ISO/IEC Standard 15408 was developed by an International community. This workshop is designed for individuals just becoming familiar with the Common Criteria. Three separate sessions will be offered focusing on the Common Criteria, Common Evaluation Methodology, and Common Criteria Toolbox. Upon completion of the sessions, you will have a greater understanding of the IT 11 functional and nine assurance security requirements in the CC, how to assemble the requirements into protection profiles and security targets that comply with the normative, how to select functional and assurance requirements based on an objective, how the evaluation methodology is employed in the security testing process, and how the automated tools can be used to make the requirements specification process more efficient and expedient. You will learn how the CC offers consumers and producers of commercial-off-the-shelf (COTS) products a flexible and extensible approach for defining security requirements in IT products and systems. You will see that with the need for security enabled and enhanced information technology (IT) to support consumer needs and the critical infrastructure, the CC provides a framework for stipulating requirements and a comprehensive approach for testing IT products and systems using a Common Evaluation Methodology. Thus, the criteria provides an internationally recognized basis for specifying and testing a wide range of technologies such as operating systems, database management systems, PKI, firewalls, smartcards, telecommunications switches, network devices, middleware, and applications. Using the Common Criteria can help:

- Convey consumer security requirements to IT product developers
- Determine if IT product developers produced what was specified
- Improve the ways consumers achieve assurance in IT products and systems
  Slides booklet, CD of the CC, and the Toolbox will be available for each attendee.

Conference Sponsors

National Computer Security Center

In 1978, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence established the Department of Defense Computer Security Initiative to ensure the widespread availability of trusted ADP systems for use within the DoD. In January 1981, the National Computer Security Center (NCSC) was established at the NSA and assumed responsibility for the activities of the Initiative.

Over the past 20 years, the NCSC has been in continuous operation, although its mission has changed dramatically. The early efforts of the NCSC and its important work relative to the Trusted Computer Systems Evaluation Criteria (Orange Book), the Rainbow Series, and the Trusted Product Evaluation Program paved the way for the future. The evolution of the Common Criteria and its international agreement led to the formation of the National Information Assurance Partnership (NIAP) between NSA and NIST. In light of these changes, the NCSC has taken on a new direction in the national Information Assurance arena. That new direction includes promoting awareness, implementation and management of programs established by the National Security Telecommunications and Information Systems Committee (NSTISSC). Additionally, the NCSC aims to partner with NIST, OMB, GSA and others to provide a bridge between the civil side of government and national security programs. As this involvement suggests, the NCSC maintains the responsibility for co-sponsoring the National Information Systems Security Conference with NIST. In its re-emerging national role, the NCSC continues to be a valuable part of NSA's Information Assurance Directorate.

National Institute of Standards and Technology

The National Institute of Standards and Technology, an agency of the Commerce Department's Technology Administration, promotes economic growth by working with industry to develop and apply technology, measurements and standards. Through its Information Technology Laboratory, NIST works to promote the development and use of information technology systems that are interoperable, easily usable, scalable, and secure.

NIST's information technology research concentrates on developing tests and test methods for information technologies that are still in the early stages of development—long before they're available in new products. But once information technology products are available, tests developed by ITL provide impartial ways of measuring them so developers and users can evaluate how products perform and assess their quality based on objective criteria.

Since 1972, NIST has played a vital role in protecting the security and integrity of information in computer systems in the public and private sectors. The Computer Security Act of 1987 reaffirmed NIST's leadership role in the federal government for the protection of unclassified information. NIST assists industry and government by promoting and supporting better security planning, technology, awareness and training. In addition, NIST fosters the development of national and international standards for security technology and commercial-off-the-shelf security products. Finally, NIST has an active, laboratory-based research program in computer and network security with special technical emphasis in cryptography; authentication; public-key infrastructure; internetworking; and security criteria, assurance and testing.

General Information

Transportation

Automobile: A map and driving directions are available at the Baltimore Convention Center website: http://www.bccenter. org/about/map.html. However, there is no parking at the Convention Center; but visitors can park in city lots and garages.

Bus: For those attendees not staying in Baltimore, daily bus service will be provided from the parking lot across from the National Computer Security Center (NCSC) Fanx III, 840 Elkridge Landing Road, Linthicum, MD. The buses will run in a round-robin fashion from the NCSC from 7:30am to 8:30am. Buses will return to the NCSC at the end of the sessions each day, following the banquet, and periodically throughout the awards reception. This is a convenient location for attendees staying at hotels near Baltimore Washington International Airport.

Communications

Messages will be taken for Conference attendees between the hours of 8:00am and 5:00pm Monday through Thursday. Messages will be posted on a message board adjacent to the Registration/ Information Area. Attendees will not be called out of a meeting except in emergencies. The phone numbers for leaving messages will be posted on the message board.

Call For Papers

If you would like to participate in next year's conference, see our Call For Papers at http:// csrc.nist.gov/nissc/call.htm

Registration

The Registration Desk will be open from 6:00pm to 8:00pm on Sunday evening, October 15, and will re-open each morning of the conference at 8:00am.

Special Interest Rooms

There are a limited number of rooms available for special interest discussions ("Birds of a Feather," etc.). These rooms may be reserved in one-hour increments and must not be used for commercial purposes. To reserve a room, please stop at the Registration Area.

Food Functions

Coffee service will be provided to all the attendees during registration each morning and at mid-morning and mid-afternoon breaks. Attendees will be free at lunch time to explore the convenient restaurants near the Convention Center and the Inner Harbor. In addition, an awards reception and banquet will be held on Monday and Wednesday evenings, respectively.

Proceedings

A hard copy and CD-ROM of the conference proceedings will be included as part of the registration packet for all attendees.

Awards Ceremony and Reception

On Monday evening, awards will be presented to vendors who have successfully developed IT security product lines that have been approved by the NIST Cryptographic Module Validation Program (CMVP), the NCSC Trusted Product Evaluation Program (TPEP), the NSA Trust Technology Assessment Program (TTAP), the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS), and the System Security Engineering Capability Maturity Model (SSE-CMM). The awards ceremony will begin at 5:30pm, followed by the reception at 6:15pm.
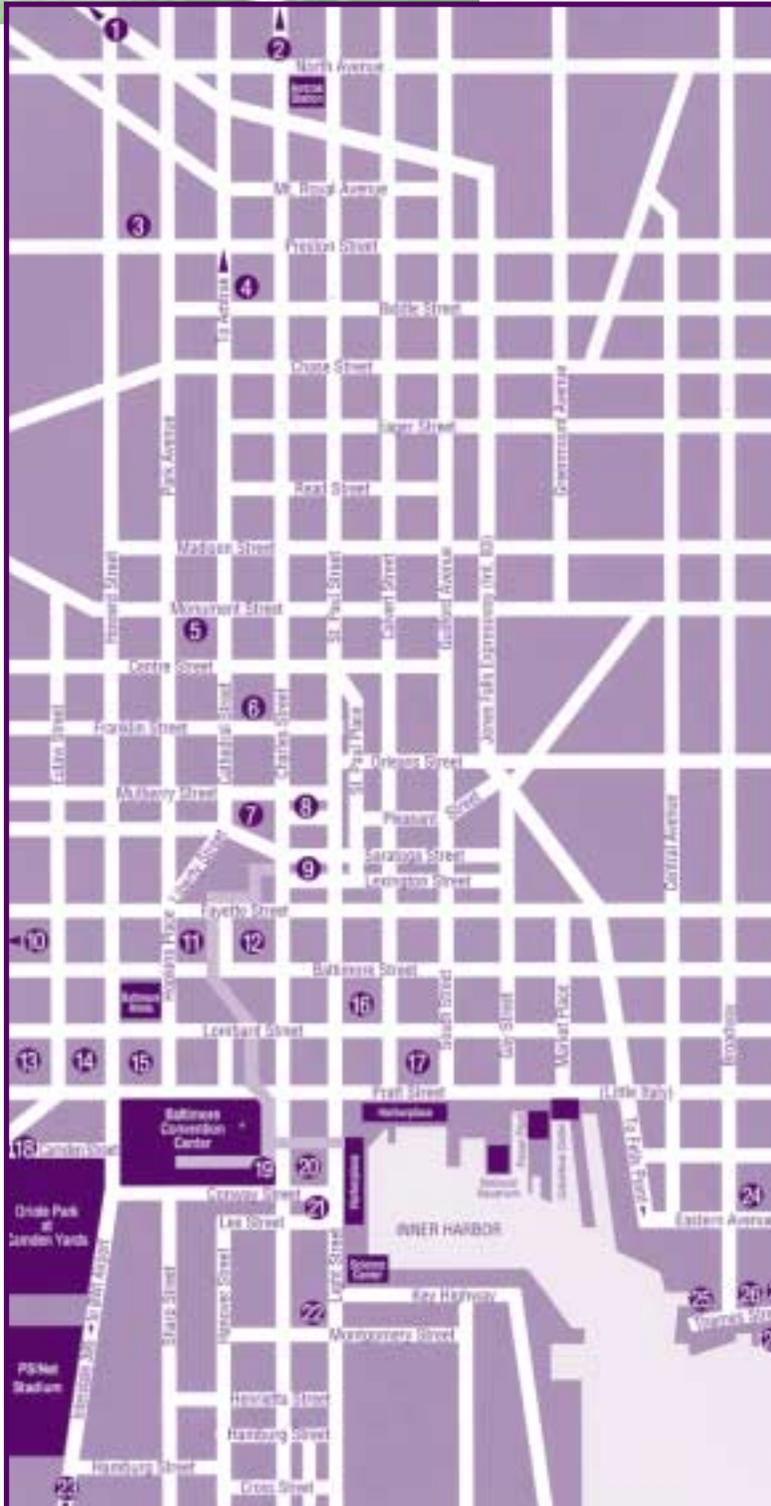
Banquet

The conference banquet will be held on Wednesday evening, beginning with a cash bar reception at 6:00pm, and followed by a dinner at 7:00pm. at the Renaissance Hotel, 202 East Pratt Street, close to the Inner Harbor.

Evaluation Forms

Evaluation forms will be provided in your conference folder for your comments. Please leave the completed forms in the boxes provided at the registration area. We thank you in advance for your comments, since your comments help the committee to develop and improve the Conference program each year. Comments may also be sent to nissconference @dockmaster2.ncsc.mil.
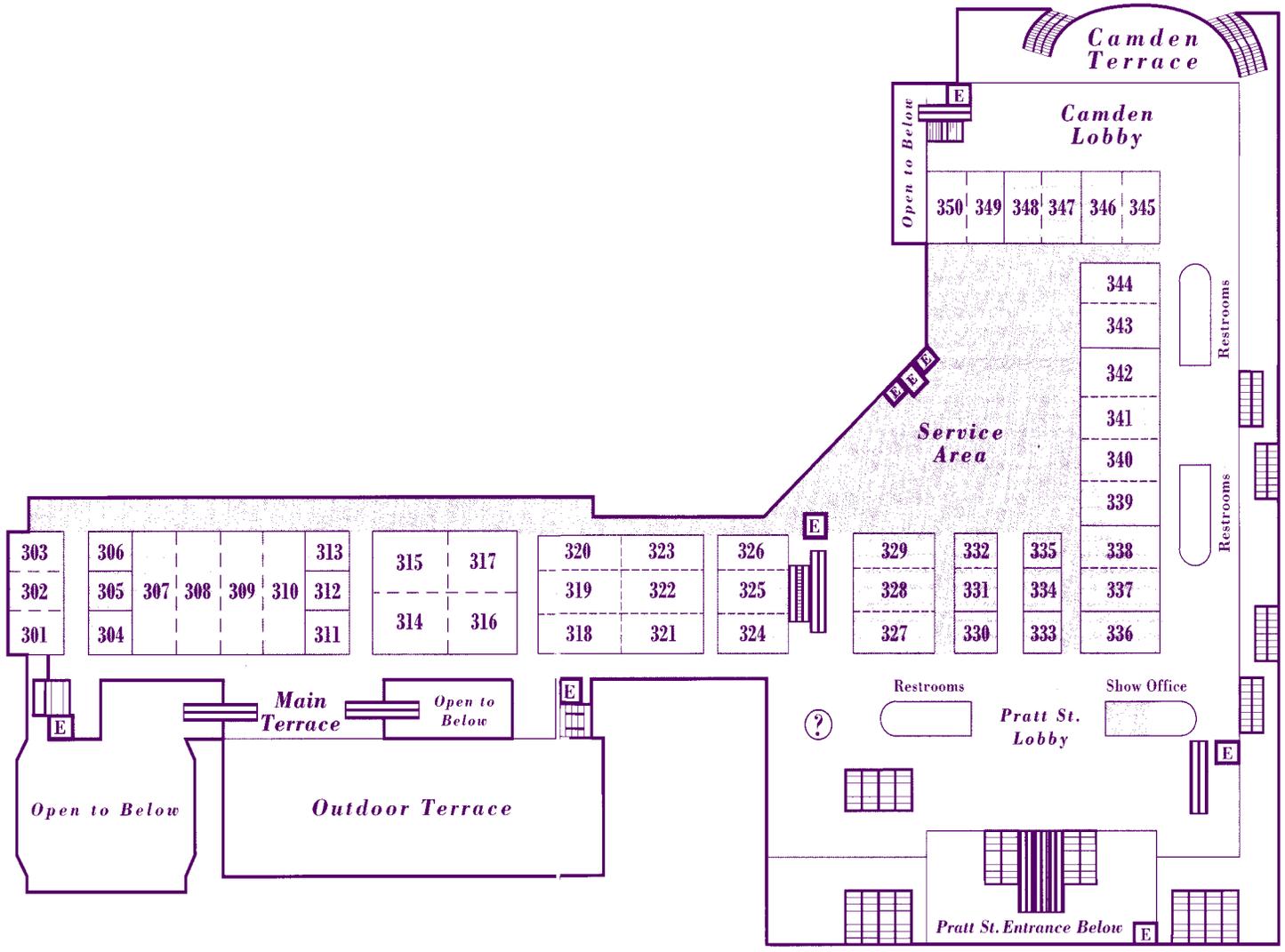
Camden
Terrace

Camden
Lobby

Open to Below

E

350 | 349 | 348 | 347 | 346 | 345

344

343

342

341

340

339

Restrooms

E E E

Service
Area

Restrooms

303 | 306 | | | | 313 | 315 | 317 | 320 | 323 | 326 | 329 | 332 | 335 | 338

302 | 305 | 307 | 308 | 309 | 310 | 312 | | | 319 | 322 | 325 | 328 | 331 | 334 | 337

314 | 316

301 | 304 | | | | 311 | | | 318 | 321 | 324 | 327 | 330 | 333 | 336

E

Main
Terrace

Open to
Below

E

Restrooms

Show Office

Pratt St.
Lobby

?

E

E

Open to Below

Outdoor Terrace

Pratt St. Entrance Below

E

NIST CENTENNIAL
1901-2001

Mark Your Calendar!

24th National Information Systems Security Conference

October 29–31, 2001

Call for Papers, Panels, and Tutorials

Sponsored by
The National Institute for Standards and Technology
and
The National Computer Security Center of the National Security Agency

For details, please visit the Conference Home Page at
http://csrc.nist.gov/nissc/call.htm

For information on submissions, please call (410) 850-0272

For other information about NISSC 2001, please call (301) 975-2775