
NBS TECHNICAL NOTE **827**

U.S. DEPARTMENT OF COMMERCE / National Bureau of Standards

# Controlled Accessibility Workshop Report

## NATIONAL BUREAU OF STANDARDS

The National Bureau of Standards[1] was established by an act of Congress March 3, 1901. The Bureau's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the Nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau consists of the Institute for Basic Standards, the Institute for Materials Research, the Institute for Applied Technology, the Institute for Computer Sciences and Technology, and the Office for Information Programs.

**THE INSTITUTE FOR BASIC STANDARDS** provides the central basis within the United States of a complete and consistent system of physical measurement; coordinates that system with measurement systems of other nations; and furnishes essential services leading to accurate and uniform physical measurements throughout the Nation's scientific community, industry, and commerce. The Institute consists of a Center for Radiation Research, an Office of Measurement Services and the following divisions:

Applied Mathematics — Electricity — Mechanics — Heat — Optical Physics — Nuclear Sciences[2] — Applied Radiation[2] — Quantum Electronics[3] — Electromagnetics[3] — Time and Frequency[3] — Laboratory Astrophysics[3] — Cryogenics[3].

**THE INSTITUTE FOR MATERIALS RESEARCH** conducts materials research leading to improved methods of measurement, standards, and data on the properties of well-characterized materials needed by industry, commerce, educational institutions, and Government; provides advisory and research services to other Government agencies; and develops, produces, and distributes standard reference materials. The Institute consists of the Office of Standard Reference Materials and the following divisions:

Analytical Chemistry — Polymers — Metallurgy — Inorganic Materials — Reactor Radiation — Physical Chemistry.

**THE INSTITUTE FOR APPLIED TECHNOLOGY** provides technical services to promote the use of available technology and to facilitate technological innovation in industry and Government; cooperates with public and private organizations leading to the development of technological standards (including mandatory safety standards), codes and methods of test; and provides technical advice and services to Government agencies upon request. The Institute consists of a Center for Building Technology and the following divisions and offices:

Engineering and Product Standards — Weights and Measures — Invention and Innovation — Product Evaluation Technology — Electronic Technology — Technical Analysis — Measurement Engineering — Structures, Materials, and Life Safety[4] — Building Environment[4] — Technical Evaluation and Application[4] — Fire Technology.

**THE INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY** conducts research and provides technical services designed to aid Government agencies in improving cost effectiveness in the conduct of their programs through the selection, acquisition, and effective utilization of automatic data processing equipment; and serves as the principal focus within the executive branch for the development of Federal standards for automatic data processing equipment, techniques, and computer languages. The Institute consists of the following divisions:

Computer Services — Systems and Software — Computer Systems Engineering — Information Technology.

**THE OFFICE FOR INFORMATION PROGRAMS** promotes optimum dissemination and accessibility of scientific information generated within NBS and other agencies of the Federal Government; promotes the development of the National Standard Reference Data System and a system of information analysis centers dealing with the broader aspects of the National Measurement System; provides appropriate services to ensure that the NBS staff has optimum accessibility to the scientific information of the world. The Office consists of the following organizational units:

Office of Standard Reference Data — Office of Information Activities — Office of Technical Publications — Library — Office of International Relations.

---

[1] Headquarters and Laboratories at Gaithersburg, Maryland, unless otherwise noted; mailing address Washington, D.C. 20234.
[2] Part of the Center for Radiation Research.
[3] Located at Boulder, Colorado 80302.
[4] Part of the Center for Building Technology.

# Controlled Accessibility Workshop Report

Edited by

Susan K. Reed and Dennis K. Branstad

Systems and Software Division
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

Contributing Authors

D. K. Branstad, P. S. Browne, C. G. Maple,
W. H. Murray, and C. Weissman

A Report of the NBS/ACM Workshop
on Controlled Accessibility
December 10-13, 1972
Rancho Sante Fe, California

Howard H. Campaigne, Chairman



U.S. DEPARTMENT OF COMMERCE, Frederick B. Dent, *Secretary*
NATIONAL BUREAU OF STANDARDS, Richard W. Roberts, *Director*

Issued May 1974

Library of Congress Catalog Number: 74-600078

National Bureau of Standards Technical Note 827

Nat. Bur. Stand. (U.S.), Tech. Note 827, 86 pages (May 1974)

CODEN: NBTNAE

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1974

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402
(Order by SD Catalog No. C13.46:827). Price $1.25

TABLE OF CONTENTS

# CONTROLLED ACCESSIBILITY WORKSHOP REPORT

Susan K. Reed and Dennis K. Branstad, Editors

A report has been prepared of the NBS/ACM Workshop on Controlled Accessibility, December 1972, Rancho Santa Fe, California. The Workshop was divided into five separate working groups: access controls, audit, EDP management controls, identification, and measurements. The report contains the introductory remarks outlining the purpose and goals of the Workshop, summaries of the discussions that took place in the working groups and the conclusions that were reached. A list of participants is included.

Key Words: Access control; computer security, controlled accessibility; EDP management control; identification; measurement; security audit.

## 1.0 INTRODUCTION

In 1972, the Institute for Computer Sciences and Technology of the National Bureau of Standards and the Association for Computing Machinery agreed to sponsor jointly a series of technical meetings in subjects of concern to the computer community. These included performance evaluation, software engineering, manpower, privacy, and controlled accessibility. The National Science Foundation concurred in the need for such meetings and provided funding for their planning.

The planning panel for controlled accessibility believed strongly that a workshop of individuals with known expertise and interest in computer security, divided into small working groups with assigned topics, could come up with fundamental principles of application and implementation, and where necessary, definitions within those topics. The topics selected were access controls, audit, EDP management controls, identification, and measurements.

Invitations were sent to a list of names proposed by the panel for specific working groups. The list represented private industry, universities, Federal and state government, trade associations and professional societies. Each individual who accepted was asked to prepare a brief position paper dealing with the subject of his assigned working group to serve as a basis for discussion at the Workshop.

The format of this report reflects the arbitrary division of the subject of controlled accessibility into five topics, but reading all five will reveal the overlap that exists and the interdependence of many techniques and solutions. The summaries of the separate working groups were originally prepared by the chairmen, assisted in some cases by others of their group.

The National Bureau of Standards would like to acknowledge the very considerable contribution of the members of the planning committee, the innovative efforts of the working group chairmen toward the success of the Workshop and the continued encouragement and optimism of Walter Carlson.

## 1.1 PLANNING COMMITTEE

| | |
|---|---|
| Douglas L. Hogan (Chairman) | National Security Agency |
| James M. Adams, Jr. | Association for Computing Machinery |
| Peter S. Browne | State Farm Mutual Auto Insurance (now at General Electric Company) |
| Robert H. Courtney, Jr. | IBM Corporation |
| Dr. R. Stockton Gaines | Institute for Defense Analyses |
| Dr. Lance J. Hoffman | University of California, Berkeley |
| S. Jeffery | National Bureau of Standards |
| Susan K. Reed | National Bureau of Standards |
| Dr. S. L. Stewart | National Bureau of Standards |
| Clark Weissman | Systems Development Corporation |

## 1.2 WORKING GROUP CHAIRMEN

| | |
|---|---|
| Access Controls<br>Clark Weissman | System Development Corporation |
| Audit<br>William H. Murray | IBM Corporation |
| EDP Management Controls<br>Dr. Clair G. Maple | Iowa State University |
| Identification<br>Dr. Dennis K. Branstad | National Security Agency (now at National Bureau of Standards) |
| Measurement<br>Peter S. Browne | State Farm Mutual Auto Insurance (now at General Electric Company) |

# 2.0 OPENING REMARKS

## 2.1 DOUGLAS L. HOGAN, CHAIRMAN, PLANNING PANEL

Good morning, and welcome to the NBS/ACM Workshop on Controlled Accessibility. As we will hear from Walter Carlson later, we are, in fact, the first of a set of four workshops. Earlier this year, a group of us got together at the request of Walter Carlson and Ruth Davis, and tried to decide if we could have a meaningful and useful workshop in this area called controlled accessibility. We spent a day and a half discussing the subject and decided that we could, indeed, have a useful exchange of information. It would involve small working groups which could interact well with each other trying to develop some meaningful thoughts out of these areas.

Primarily we would like the output of this workshop to be a fairly positive indication of what we know and what we don't know, and of some of the things that really need to get done as they affect all of us in our different roles -- whether it be government, industry, users, or others.

The average man-on-the-street would probably be confused if someone talked to him about controlled accessibility. Imagine a cab driver, for example. If you told him you were going to a workshop where more than half-a-hundred computer professionals would meet to find ways to keep programmers' hands out of the computer system and its files, he would have replied, "Why bother? It takes six weeks to change a computerized address for a magazine subscription and six months to get a faulty statement out of a billing file."

I am reminded of another story, perhaps apocryphal, because it goes back many years, of the programmer in a new installation who suspected that after all the programs were written, he would be fired. Therefore, he imbedded a tiny algorithm in an obscure corner of the payroll program to check for the presence of his name in each run. As predicted, he was "let out" in a year or so, when management thought the development work was complete. His computer program printed his final check, including his accrued benefits, and removed his name from the active-records file. During the next run, when he was well on his way to greener pastures, the imbedded algorithm didn't find his name. Whereupon, it branched to an "expunge" routine and deleted all the other records from the payroll files.

The key point of this story is, perhaps, just as human nature lives on, controlled accessibility solutions must be the best that man can devise. This area is a very important one at this time. It is one that needs attention. We are here to give it that. I don't want to say very much more except to introduce our General Chairman, Dr. Howard Campaigne.

## 2.2 DR. HOWARD CAMPAIGNE, GENERAL CHAIRMAN

There is a new book coming out this month called "Data Banks in a Free Society," which has to do with controlled accessibility in a sense, although it's from the social sense. It isn't directly applicable to our work here, but I recommend it to you as an interesting book. The group of contributors visited 55 big computer installations. One of them was a company which I don't think I'd ever heard of before, but probably some of you have. One of the interesting aspects of this company is their attitude on privacy. They say that they are not involved, that everything in their data bank is a matter of public record, and that they never put anything in there which is at all sensitive. They do, as a matter of policy, expunge from their list anybody who asks that his name be removed. Of the millions of records, 250 people have asked to have their names expunged. This is evidence that they are not treading on anybody's privacy.

Another place that was of great interest was a bank in Chicago. This bank does data processing, not only for themselves, but for other banks as well. Their's is a large operation -- 11,000 reels of data and 2 million transactions a day. We picked up a story of how an employee embezzled from their computer system. He modified the stock dividend file so that it sent him some dividends, although he wasn't entitled to them. In fact, he got $55,000 in dividends and his method worked perfectly. They never caught onto it except that in cashing the checks, he aroused suspicion, and they investigated and caught him.

The technique he used was very simple. He was a programmer and he knew that the stock dividend records as they came to them depended on being in sequence order -- strict sequence order. All that he did was interchange two of those cards. When it came to them, the processor ground to a halt and refused to respond to the operators, so they had to call for the maintenance programmer who, of course, was he. He then went into a long study of the situation and was able to introduce his own records. Then, of course, as the last step, he interchanged those two cards again, and they patted him on the back, gave him a raise, and were very pleased with his performance, temporarily.

Another incident which has aroused a lot of interest lately, is that of the fellow up in Santa Clara County, whom you have read about, I am sure. It's an important case because precedents are being based on it. I think it's not technically terribly interesting, but you remember this fellow wanted a copy of a program which resided in someone else's file. He didn't have access to it. He knew the name of the file in which it was stored. He knew their valid account number and he knew a valid terminal identification number. With this, he was able to get into their file from the remote terminal and requested a punched card copy of this program. Now at this point I'm puzzled, because I don't understand why he expected the center to send him the punched card copy. When the computer center gets cards like that, it looks at the account number and sends them to that customer, which

was the legitimate company. So when he didn't get his cards, he asked for a print-out.

If I had been in their place and had gotten that deck of cards, I would have said, "That damn computer center -- here they are messing things up again," and thrown them away. But they didn't. Their suspicions were aroused immediately and they checked and figured out where it must have come from. They swore out a search warrant for this man and described the computer print-outs they were looking for. This man's business was programming and he had lots of computer print-outs, so they had to describe the print-out accurately enough on the warrant to identify it. Now, of course, it has hit the newspapers and it's a big thing. Now there's a six million dollar suit for stealing a trade secret. It is an important case. For one thing, it may establish programs as trade secrets or, maybe, unestablish them as trade secrets. For another, it's the first time, I think, that a computer print-out has been incriminating.

Furthermore, it illustrates one point which is of great interest to us -- it illustrates the value of an audit trail. It's the audit trail that turned out to be very useful in this case. They could establish what terminal it came from, what account number, what he got out, and that he got a print-out. It does, of course, bring to mind that the identification of the person and the identification of the terminal are both tremendously important in this audit trail if it is going to be useful. If he had been able to spoof that it came from a different terminal, possibly the audit trail would have been useless. I think this is one of the points we want to address here: how do you do identifications of this kind?

Another point of tremendous importance, of course, is the cost of security. People may want to have their privacy, but when they find out how much it will cost, maybe they won't want to pay for its protection. I would recommend that we not worry too much at this workshop about cost. We're not close enough to a solution yet, but we should keep in mind that we are going to have to account for costs sometime.

I want to turn over the meeting to Dr. Ruth Davis, who is Director of the Institute for Computer Sciences and Technology at the National Bureau of Standards.

## 2.3 DR. RUTH DAVIS

We are privileged that the Bureau of Standards is a co-sponsor of this meeting. I am sure that we shall be very proud of its output. I want to remind all of us, in this regard, that the initial stimulus and continued persistence of Walter Carlson have helped propel us in this effort.

The context for the topic, controlled accessibility, and its relation to our program at the Bureau of Standards is an important input to this meeting. About a year and a half ago we decided, in line with our obligations under both our specific legislative charter (PL 89-306) and our Department of Commerce charter, to ascertain the principal problems in computer utilization within the government (federal, state, and local), industry, and the private sector. The eight major problem areas found centered on software or the use of software in computer systems. The sources we used to find these current problem areas were: 1) consumer groups (such as that of Virginia Knauer's at the White House); 2) several congressional committees which conducted hearings on such varied topics as the numerical-control tool industry, increased productivity in the service areas, costs of environmental monitoring and sensing, Medicare, Medicaid; 3) GAO reports; 4) the ACM; and 5) the large computer services.

The three major problem areas causing the most pain nationwide were found to be: 1) controlled accessibility (both for keeping people away from and allowing people to get at a data bank; 2) documentation of services and products (for proper consumer information); and 3) production of application programs (for usable, correct, documented, and cost-effective software).

Our NBS program, CAPSIT (Computers Applied to Public Services and Industrial Technology) embodies our efforts towards improvement of computer utilization in these problem areas. These projects are directed towards some 80% of the uses of computers in the country, leaving out academic and non-profit organization needs.

As a result of our program, a set of four areas of urgent interest to both the ACM and ourselves was selected for workshops such as this one. These areas are controlled accessibility, performance measurement, privacy, and computer manpower. Two other areas of interest to us in line with our mission in the Department of Commerce are: 1) the use of computers to improve productivity in the industrial sector; and 2) the role of the computer and computer services in the international arena. A workshop in the first area will be held in New Hampshire in the summer. The second topical area covers commodities (saleable, exportable, or importable) in the computer industry as well as the improvement of our competitive status in the international scene.

Our hope for this particular conference is to have a product translatable into action, hopefully, immediately by the private sector, the ACM, government (federal, state, and local) and large trade or industry associations. The copious material on controlled accessibility needs organizing, focusing, coalescing, and direction with priorities so that we can recommend actions for making computer systems either more controllable or make their access directly handled by control mechanisms which we understand.

The authority and responsibility we have that allows us to make this commitment to action stem from legislation under which GSA and the Department of Commerce operate. This legislation allows the federal government to operate as the single largest computer customer in the United States with the leverage of having 7.8% of the computers in the country; it requires that we recommend federal government-wide computer-related policy, which often is followed by similar state and local government policy. (State and local governments possess an additional 10% of computers in the United States); it requires that we work with the industrial sector and large trade associations which then filter their suggestions down to the computer manufacturers for adoption by the computer industry and the customers; and, finally, the legislation mandates that we develop standards for compliance by the federal government which are also frequently adopted as national voluntary standards within the ANSI community.

We hope that this conference will result in some concrete recommendations concerning: a coherent terminology (necessary for any technology and its documentation, be it a user's primer, legislation, or executive orders); non-trivial experimentation with operational systems in a controlled environment (covering technical areas such as identification, measures, and audit); and managerial considerations necessary to implement the technical innovations.

We are very pleased and privileged to co-sponsor this meeting. We are most anxious to help you see your recommendations become actions both in government and the private sector. The sponsors are grateful to the National Science Foundation for their financial support of the planning panels for this and the other workshops.

I would now like to introduce the other sponsor of this workshop, the Association for Computing Machinery, and its President, Dr. Anthony Ralston who is at the State University of New York.

## 2.4 DR. ANTHONY RALSTON

I am very pleased that ACM is a co-sponsor on this workshop. I think, perhaps, ACM's aims are somewhat less specific than the Bureau of Standard's because our mission is different from that of the Bureau but I feel very strongly that ACM should be involved in this type of thing.

The guiding lights behind this workshop, and the other ones which have been mentioned, have certainly been Ruth Davis and Walter Carlson. Nevertheless I'm very happy to be here and to have the chance to tell you that from ACM's point of view, I'm very pleased about these workshops. It is not just because we're involved with the Bureau of Standards in this way, but also because the topics involved are just the kinds of things that ACM should be involved with. We

are accused from time to time, perhaps reasonably enough, with having less social responsibility inside ACM than we should have. It is this kind of topic on controlled accessibility, and for example one on privacy which is coming up later, which are just the things which I believe ACM should be very strongly involved with as we move into the future and the organization, perhaps, changes some of its directions.

In looking through the submitted working papers for this workshop, I noticed such things as cost of security, management apathy, and things like this. It occurred to me that there is an important negative way of looking at this whole topic. That is the cost of not doing what you are talking about. I think this is particularly important in the management area. It may be right that management is apathetic about things like controlled accessibility, but this apathy, perhaps, is more apparent than real.

In any kind of management situation and certainly in computing management where there are lots of pressures of all kinds on the manager, the kinds of things in which he really interests himself, and which he really spends time on, are just those things which have a direct benefit to him (and I suggest to you that in terms of EDP management, there is very little benefit to be derived from better controlled accessibility), but the things that also concern him are those things that if he doesn't do them have a direct cost to him, and a significant one. That, of course, is not the kind of thing we've had at all in the past in areas like security and privacy. There has been almost no cost to the management of computer installations, and EDP management more generally, of not having good controls on privacy and security.

If we are going to achieve these kinds of things in the future, then somehow we have to meet that cost. We're going to have to make it very clear (and I have no particular words of wisdom on how to do that) to managers that not to implement the tools they have been given is to incur, at least potentially, a very severe cost. Although some of these tools will be hardware and software, some of them in fact will be management tools.

Let me just say again that from ACM's point of view, we are very happy indeed to co-sponsor this meeting. I hope that what will come out of it will not be just a series of individual papers, but some cohesiveness about this topic which will lead us forward to doing something in these areas. I wish you all a good three days of hard work and good results.

Now I would like to ask my predecessor as President of ACM to speak to us, too. Inasmuch as he and Ruth were the moving force behind this series of workshops, I'm sure he has some advice to offer. I introduce Walter Carlson from the IBM Corporation.

## 2.5 WALTER CARLSON

I would like to embellish some of the objectives that we have in our minds and lay them in front of you: what some of us think is possible, what some of us think is desirable, and what some of us think is undesirable in terms of the activity in which you are now engaged.

There are really five questions.

First: What are the fundamentals (or the first principles) of controlled accessibility? In other words, we want this group to agree as a group, not as individuals, but as a total congress, on a ratification of those first principles here and now.

The second question is: What measuring tools do we have for determining what's going on with respect to controlled accessibility today?

The third question is: What do these measurements show us today? Are we in good condition, are we in poor condition? How do we know what is good, what is poor?

The fourth question which then logically follows is: What improvements are required?

Finally, and not at all least: Who is responsible for providing these improvements?

Ruth has emphasized the word "action." It becomes fairly clear to me, looking at this list of questions, that the recipe for action logically follows from an attempt to answer these questions. I don't propose these as the only questions to be raised, but I think a meeting of this sort deserves some suggestion of structure and this is one form of structure that I recommend to you.

The second thing I would like to draw your attention to is that while there has been discussion of a product or report from this workshop, it is not at all clear in my mind that there is only a single product to be brought out. You people are going to have a profound influence in and among yourselves as to what the product of this activity will be.

Just to suggest some structure, strictly in the form of a set of trial suggestions for you to try on, I can see that there might well be three or four different, highly different, kinds of products from this endeavor. The first one might well be just a listing of the fundamentals that you all agree upon as applying to this area of activity. This product might be a handy pocket reference for the manager to look at, and use as a test for people who parade in front of him as to

whether they know what they are talking about. That might be a very short document, just a few pages, in fact.

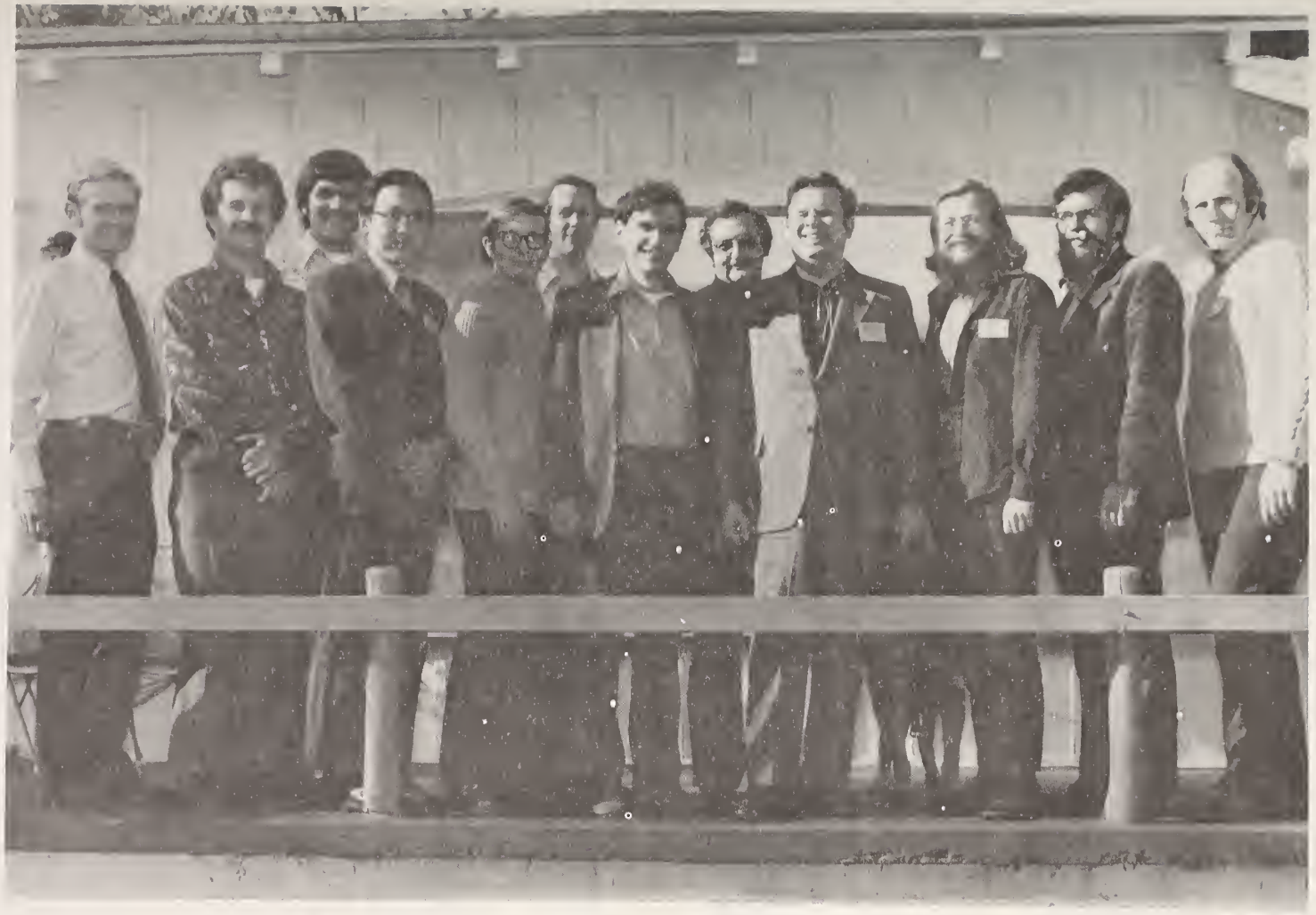
A second product is one that Ruth has alluded to. This would be a listing of the issues which are unresolved and which you people have defined and hopefully have crisply written down. Along with that set of issues and a description of them, there would be a fairly formal listing of who has the action, and who is responsible for resolving those issues. I don't mean necessarily an individual company or an individual government agency, although that may in some instances be part of the answer, but maybe an institutional concept such as the government, or the profession, or the industry, or what have you, or some combination of them.

The third logical product from this endeavor, of course, would be a distilled summation of the working papers and the reports that come from the five working groups here, as well as a summary statement of the accomplishments of the meeting. This would tend to be more like the traditional proceedings of a conference but would avoid trying to expostulate what individuals have said or have tried to prove. It would be much more a group kind of product and would represent the authority of this entire body.

Given the prospects of having those types of products, there might be a fourth product which I think might be admissible. You may also wish to go far enough to set forth a plan of attack. What technologies have to be brought to bear? What kinds of research and experimentation might be undertaken, to illuminate the issues and bring forth conclusions and actions?

As you debate among yourselves on what you know and what you don't know, you may find other forms of products that could be much more useful than the one defined. I would consider that we are almost completely open ended at this moment in terms of what these products are going to be.

I commented to the Chairman last night that this is a big order. But if there is one thing that we are not, it's bashful. We are not inhibited in proposing the range and the scope of the expectations that we have for this particular gathering. Thank you.



3.1 Access Controls Working Group

Richard Conway, G. Edward Bryan, Kenneth Sevcik, David Hsiao, William Inglis, R. Stockton Gaines, Daniel Edwards, Clark Weissman (Chairman), Edward Glaser, Robert Fabry, Michael Casteel, Joel Birnbaum (Recorder).

## 3.2 CONTENT AND OBJECTIVES OF THE ACCESS CONTROLS WORKING GROUP, Clark Weissman

A recent panel [1]qf on computer security stated that a secure operating system must satisfy the following "minimum necessary" conditions:

1. There must be a central computer access control mechanism.
2. The access control mechanism must always be invoked (even for itself).
3. Access controls must be tamperproof.
4. Access controls must be certifiably correct (or small enough to be exhaustively tested).

It is the objective of this working group to define the access control mechanism(s) that offer the best (cost effective) solution to these minimum necessary conditions. The working group can challenge, offer alternatives, or add extensions to the minimum conditions; however, it will be preoccupied with the nature, model, formulation, supporting hardware, software, and procedural environments for the access control mechanism.

Models of or relevant to such mechanisms have appeared in the literature during the past few years, and attendees should come prepared to discuss them and whatever practical experience they've had with them. These include but are not limited to:

| Subject | Author | Date |
|---|---|---|
| • Segmentation Addressing Control | Dennis | 1965 |
| • File System Control | Hsiao | 1968 |
| • Multics Rings - Software | Graham | 1968 |
| • ADEPT - Set Theoretic Controls | Weissman | 1969 |
| • Cryptographic Controls | Skatrud | 1969 |
| • Cryptographic Controls | Van Tassel | 1969 |
| • Dynamic Structures Model | Lampson | 1969 |
| • Cryptographic Controls | Carroll & McLellan | 1970 |
| • File System Control | Friedman | 1970 |
| • PRIME-Distributed Machine Approach | Fabry | 1971 |
| • Formulary Model | Hoffman | 1971 |
| • Multics Rings - Hardware | Schroeder & Saltzer | 1972 |
| • Capabilities Matrix Model | Graham & Denning | 1972 |
| • Supervisory Computer Concept | Gaines | 1972 |

[1] Figures in brackets indicate literature references at end of section.

Newer models and formulations are welcome. Attendees wishing to present new approaches should prepare a brief of their model, including a clear statement of the system security requirements they are attempting to satisfy, the identification of subjects and objects of security interest and their rights and privileges (i.e., security profile). Questions of practical implementation and representation will be considered.

The session will produce as its output a concise description, suitable for open publication, of the model(s), surrounding assumptions and definitions of the access controls developed. It will also produce a brief statement of the rationale used to arrive at the model(s), including statements of the limits and practical constraints of such models. Dissenting opinions will also be reflected.

## 3.3 ACCESS CONTROLS WORKING GROUP REPORT, Clark Weissman

### GOAL

A secure-resource sharing computer system differentiates, mediates, and controls access to sensitive information and services. The goal of this working group is to define the nature of an access control mechanism and technology involved in ensuring secure computer system operation.

### THREAT

Access controls apply at three distinct, often hierarchical, system levels: 1) the internal end-user application software and data; 2) the internal hardware and software services; and 3) the external environment of hardware, people, and software libraries. Internal and external computer system control apparatus are mutually supportive and needed to ensure controlled accessibility to user data. Though external-facility "good housekeeping" operation is necessary, it is not sufficient to ensure security from planned, intelligent, hostile attack against internal control apparatus. System security is most threatened by the vulnerability of the internal access control mechanism to unauthorized modification by subversion of normal internal system services or exploitation of system weaknesses (e.g., coding errors, incomplete design).

### ASSUMPTIONS

The operating system is the principal context for access controls. Though data management systems and other applications software must also contribute to controlled access, they are secondary defenses dependent on the uncorrupted services of the operating system. Controlled accessibility is exacerbated by requirements to satisfy heterogeneous multi-level user sensitivity levels common for military, public, and private resource sharing systems. Dedicated

(single level) access controls are presently achievable and, therefore, are not discussed.

Systems always evolve; modifications repair flaws, improve performance, adapt to new equipment, and increase capabilities. In such a changing environment errors are inevitable and security violations will occur.

It requires upwards of six years to analyze, specify, design, and implement a major operating system -- one composed of hundreds of thousands of machine instructions. The design phase is the proper time for considering the access control mechanism. As each phase passes, the security options of the access control mechanism become fewer. We often worry too late -- after the system is delivered for operation -- about how to make it secure. Such retrofit may be futile and will not be considered here.

## SECURITY DESIGN CRITERIA

The foremost design criterion is for the system to satisfy its requirements, with nothing hidden. As such, capability, performance, and cost are paramount. To that list, we now add security.

Defensive system design is mandatory. Routines must be suspicious of their callers and always validate a caller's identity and data and control parameters.

Control mechanisms should be formal and always invoked, and never bypassed for "efficiency" or other rationalizations. The design should encourage proper use by making these mechanisms rational, easy and efficient to use.

Since flaws will exist and violations will occur, the design must minimize system compromise and data loss as well as minimize time to recovery.

Design must accommodate evolution, easy system maintenance and configuration management for controlled modification.

The principle of "least privilege" should be widely applied to all internal and external system components. It states that a component should know about and control only those resources necessary for its job.

System complexity is best dealt with by breaking the system into a structure of subsystems and developing a conceptual model of an access control mechanism. A strict process structure -- hierarchy, tree, graph -- aids access controls mediation of shared resources, process access rights, and system services. Interprocess communication design must be completely specified and enforced. Models permit representation of complex behavior with predictive abilities to show logical completeness of design and to serve as specifications for implementation.

## TOWARD CERTIFICATION

Any access controls design must adopt as its underlying strategy the ability of the system to certifiably satisfy the design criteria. That requires assurance of the logical completeness of the system design, the correctness of the system implementation, and sound system operation based upon proven EDP facility management principles.

1. Access Control Design Models. Modeling is currently the best available technique we have to check the design for logical completeness. Unfortunately, most existing models are more nearly conceptual requirement descriptions than they are analytical or simulation models used for prediction.

### Dimensionality

A complete model must be at least four dimensional. It must:

a. Define security subjects and objects of interest (e.g., users, files, terminals),

b. Describe capabilities (i.e., access rights) of each to each (e.g., read permission, execute only),

c. Formalize rules for access determination and enforcement (e.g., address bounds checking, address mapping, interpretation of capability descriptors), and

d. Make explicit rules for modifying objects and capabilities (e.g., capability delete, object creation, control table entry reset).

While a host of innovative "models" have appeared in the literature in recent years, few are fully satisfactory for a complete determination of design. The "matrix" model [13,18] is the most general since it combines "capability-list" models [8,17,28] and the access list models [6]. In the matrix model, subjects and objects are defined on the rows and columns. Entries in the intersecting cells define the allowable access rights, e.g., ability to execute, write, read. Other models either limit themselves to special operating system functions [7,11,16], or deal with implementation techniques [4,10,12,14,15,23,25,27].

### Message Model

It is suggested that a "message" model, where interprocess communication is only by regulated message exchange, is the most primitive access control mechanism, and by Turing-extension, rich enough to allow composition of the most complicated model, e.g., the matrix model. The

idea may be theoretically sound but impractically expensive in operational overhead, except for limited purposes, such as user-level transaction systems.

Terminology

In dealing with access controls, the following terms are defined and found useful:

- Process: Mechanism which exercises access rights.
- Domain: A collection of objects and access rights to them.
- Address Space: Lexical name-space for a process.

2. Practical Implementation Techniques. No formal methods exist today for guaranteeing the correctness of hundreds of thousands of lines of code in a modern, complex operating system. The best current techniques utilize selective, structured, empirical testing of the finished code -- first of stand-alone functional units, then of composite functions of a subsystem, and finally of integrated subsystems and hardware. The size of these systems precludes exhaustive testing. Some automated, currently available, aids allow partial logical analysis of program flow, but not of data flow. Both empirical-testing and logical-code-analysis techniques are "after-the-fact" flow finders. They do not build in security quality, they only determine its absence in the finished product. New techniques of logical "proof of correctness" [19, 21] and "constructive correctness" [9, 20, 22] promise to give assurance of more perfect implementation through formal correctness discipline during implementation. Also, double-checks on access control decisions can reduce the impact on security of hardware and software errors [10].

Central Access Control Kernel

Formal correctness proofs have been produced for programs of some complexity and a few hundred lines of source code. Such a technique becomes practical only for well-designed, modularly structured systems of a few thousand total code statements. This practical constraint has led to postulation of a secure system design based on an access controls kernel that is small enough to be certified secure by design completeness and proven correct in implementation. Optimism for this approach is heightened by recent hardware advances in access control [23] which would have the kernel primarily managing that hardware analogous to the matrix model described above. Of course, proof of code correctness is necessary but not sufficient, since code may still be exercised on hardware that is faulty.

## Compartmentalization

A more conservative approach to secure systems is the concept of distributed, compartmented access control. System security, like the buoyancy of a ship, is achieved through the collective strength of individual cells that inhibit propagation of security compromise to adjacent cells.

This approach builds on the growing technical foundation for constructive correctness which requires systems to be designed and implemented modularly from the top down in carefully ordered layers with fully defined interfaces. "Security-tight" domains would be the analog of the watertight cells. The design principle of least privilege applied to processes and their domains assures resistance to propagation of security damage so prevalent in current operating systems.

Security damage propagation is further retarded by strict process ordering by hierarchical layering, and by restricting domain control to only the owning process. Resource (domain) sharing would be achieved by: 1) interpretive interprocess communication; 2) overlapped domains; and 3) the dynamically created "third party" process that owns and manages a shared domain.

## Interpreters

Even the best access control mechanism can be foiled if it does not validate parametric data. Interpreters are the oldest, and still the most flexible approach to satisfying this run-time requirement, since any desired degree of scrutiny can be accommodated. In the past interpretation has been expensive in run-time overhead, and this has limited its application. However, recent hardware advances in high-speed logic and memory, associative memories, microprogramming, and "smart," i.e. programmable, I/O devices and controllers have dramatically improved run-time performance of interpreters, making them quite attractive for access controls consideration and security application. Such applications include mediation of address referencing, interprocess communication, and I/O.

Software interpreters are still attractive for user-level transaction-oriented applications, with hardware interpretation for time-critical situations, as in "field-level" data management system access control [16].

In future compartmented systems built as discrete layered domains, each higher layer could be viewed as a more "abstract machine" with an abstract "instruction set" for interprocess-interlayer communication interpreted in hardware for increased performance.

Hardware interpreters, e.g., microprogrammed machines, make the primitive message model a possibility for implementing a hierarchy of access control, ranging from physical hardware to operating system access controls to user application access controls.

3. . Facility Operations. The subject of each of the other four concurrent working groups of this workshop -- Audit, EDP Management Controls, Identification, and Measurements -- impacts the access controls most visibly in the operations area, where sound facility management is necessary to ensure the integrity of the access control mechanism and its external environment. We dwell here only on those issues that directly affect the access control mechanism, or where the access control mechanism directly affects operations.

The principal vulnerability of the access control mechanism is to tampering that 1) selectively disables control, or 2) adds unauthorized features. Design and implementation paragraphs have already discussed techniques for developing an access control mechanism that is tamperproof from internal operation. The key to successful internal control is to ensure that the access control mechanism is correct and always invoked, even for its own access references. It is imperative then that operations:

a) Ensure the access controls are always invoked;

b) Authenticate that the access control mechanism is the genuine article and has not been illegally modified; and

c) Verify that the access control mechanism has been primed with correct initial data on subjects, objects, capabilities, names, and authenticators.

Careful authentication and controlled storage of all system master programs, libraries, and data are basic to ensure an untampered access control mechanism. Frequent, aperiodic, unannounced audit of the correctness of the master files is required, performed by an independent group. Formal configuration management is needed to ensure currency of records and correctness of all modifications, updates, repairs, etc. to the master files. In a like manner, but more frequently -- even daily -- a team of "security managers" should audit all security data, profiles, and directories. Wherever possible, owners should be required to certify regularly (e.g., weekly) that all transaction logs and permission lists involving their property (i.e., files, programs) are correct.

The facility must establish verification procedures for system startup and bootstrap recovery. The procedures must verify the correct loading of the master system and initialization data. Tools and techniques to perform such verification are non-trivial and require certified utilities or even special hardware.

## RESPONSIBILITY

Secure systems are an industry-wide problem not restricted to any one segment.

1. Manufacturer: Hardware and Software Vendors. The consensus of the working group participants is that the manufacturer has ultimate responsibility for delivering systems that can be operated securely. It was noted that the DOD is the largest purchaser of special-purpose operating systems where the operating system is supplied by other than the hardware manufacturers.

2. Facility Manager. As always, "Let the Buyer Beware" translates into user responsibility for requirements specification, product acceptance, and system operation.

### Requirements Specification

The facility manager can seek help from other agencies to fulfill his responsibilities. For example, DOD Directive 5200.28 defines security requirements for multi-level operation of EDP systems. NBS and trade associations could assist the civil and commercial sectors in like manner, by establishing security policy and requirements for non-DOD systems.

### Product Acceptance

Product acceptance will require application of techniques for certification. The manager today gets mostly "arm waving" from the vendor. Government should play an important role in this arena, possibly paralleling its role in commercial aviation, in which the FAA certifies aircraft as airworthy. Alternatively, "secureworthiness" might be granted by an organization similar to the Underwriters Laboratory.

### System Operations

Secure operation is the manager's responsibility. However, government should provide some regulation and licensing for systems that serve the public at large, such as commercial time-sharing, financial, credit, service bureau, and voting systems. The manager should keep a constant vigil on his system's operation, applying "least privilege" concepts to people throughout his facility.

3. Research Establishments. The university and other research environments must address the serious, still unresolved, technical issues. They should couple to professional societies (e.g., ACM, AFIPS, IEEE) and trade associations (e.g., ADAPSO, CBEMA, DPMA) to educate the industry and promote concern for the problem and its solution.

4. Professional Organizations. With funds from government, the research communities, trade associations, and professional societies should convert technical solutions into design, implementation and operating guidelines, and codes of good practice. The professional societies should organize an annual congress on security with material developed at local and regional special interest groups (e.g., SIGARCH, SIGOPS, SIGBDP, SIGFIDET, etc.).

## 3.4 ACCESS CONTROL BIBLIOGRAPHY


1. Anderson, J. P., "Computer Security Technology Planning Study," U.S. Air Force Electronic Systems Division, ESD-TR-73-51, Vols. I and II, October 1972.

2. Bergart, Jeffrey G., "Computer Security, Access Control and Privacy Protection in Computer Systems," University of Pennsylvania, Philadelphia, Moore School of Electrical Engineering, August 1972.

3. Brown, J. R. and R. H. Hoffman, "Evaluating the Effectiveness of Software Verification -- Practical Experience with an Automated Tool," in 1972 Fall Joint Computer Conference, Volume 41, Part I, (AFIPS Press, Montvale, New Jersey), 1972, AFIPS Conference Proceedings, (LC 55-44701), p. 181-190.

4. Carroll, J. M. and P. M. McLellan, "Fast Infinite-Key Privacy Transformation for Resource-Sharing Systems," in 1970 Fall Joint Computer Conference, Volume 37, (AFIPS Press, Montvale, New Jersey), 1970, AFIPS Conference Proceedings, (LC 55-44701), p. 223-230, 12 refs.

5. Conway, R. W., W. L. Maxwell and H. L. Morgan, "A Technique for File Surveillance," Cornell University, Ithaca, New York, Department of Operations Research, Technical Report 150, May 1972.

6. Daley, R. C. and P. G. Neuman, "A General Purpose File System for Secondary Storage," in 1965 Fall Joint Computer Conference, Volume 27, Part I, (Spartan Books, Washington, D.C.), 1965, AFIPS Conference Proceedings, (LC 55-44701), p. 213-229, 5 refs.

7. Dennis, Jack B., "Segmentation and the Design of Multiprogrammed Computer Systems," Journal of the Association for Computing Machinery, 12:4 (October 1965), p. 589-602, 10 refs.

8. Dennis, J. B. and E. C. Van Horn, "Programming Semantics for Multiprogrammed Computations," Communications of the ACM, 9:3 (March 1966), p. 93-155.

9. Dijkstra, E. W., "The Structure of the Multiprogramming System," Communications of the ACM, 11:5 (May 1968), p. 341-346.

Once loaded, the system should dynamically monitor and audit its own internal operation. Audit should record and reduce data from all security transactions for later examination. Dynamic surveillance continually measures security performance and monitors system integrity and correct operation. Implicit in the secure operation of the access control mechanism is the continual dynamic identification and authentication of security subjects and objects.

## INCOMPLETE DISCUSSIONS

Many issues received inadequate attention during the deliberations of this group. They are noted here for subsequent security groups to resolve.

1. Criteria. Only general metrics were considered, mostly in connection with the design adequacy of an access control mechanism. These included:

   a) Simplicity of access controls. The fewer the distinct types of security objects and their interconnections, the better.

   b) Generality of access controls gives flexibility to system designer but may increase overhead.

   c) Ease of access controls implementation increases "secure-worthiness."

   d) The "gold-mine" effect was noted. The greater the concentration of control in the access control mechanism (gold-mine), the more it is likely to attract attack, and hence the greater the need for multiple countermeasures.

   e) "Secureworthiness" of a compartmented access control mechanism can be measured as a function of the cumulative probability of violating multiple domains and the cumulative security damage resulting therefrom (e.g. the improper availability of access rights).

2. Retrofitting. The nature of this issue is: How to retrofit current systems to provide them with some level of security? This raises secondary questions:

   a) Can security be retrofitted to a current system?

   b) Can a secure subsystem be built that operates on an insecure operating system?

   c) Is security measured on a binary scale (0 or 100%), or is it graded?

   d) Can systems exist with several degrees of security?

3. Characterization of Secure Systems. Some brief attempt was made to characterize a secure system along the following dimensions:

a) Degree of user control, from assembly language, to higher level language, to transaction only.

b) Degree of interprocess communication.

d) Degree of resource sharing.

4. Application-Level Access Controls. No serious consideration was given to access controls at other than operating-system level. "Language envelopes" were noted as one method for keeping a user's capability constrained within the context of a higher-level language system. Interpreters are needed because of the possibility of subverting run-time features. This raises the following unanswered questions.

- Can a secure compiler be built for existing languages?
- If not, can a new, useful language be designed for which a secure compiler can be built?

Encryption may be a useful technique for use in higher level access control mechanisms [4, 5, 25, 27], but was not discussed in depth. There is a tendency to keep keys active for too long a period, thus increasing the probability of compromise. Encryption routines are also subject to unauthorized modification.

5. Secure Networks. No attention was given to one of the most serious consequences of insecure operating systems: their weakening of the security of any computer network they join. With the growth of computer networks, the damage to military, public, and commercial security is increased manifold, since the security weakness of a given node propagates to all nodes in the net.

6. Security Hardware. The need exists for an efficient method to validate interprocess communication. Since objects and capabilities are named entities in the address space, hardware that assists address mediation is of high priority. Virtual memory is of considerable value in this regard, since it simplifies and generalizes interprocess communication. Associative memory for dynamic address translation makes virtual memory management and domain control fast and efficient. Segmented memory addressing that permits hardware checking of software-controlled "descriptors" (e.g., extra "flag" bits per address domain) has been successful in equipment from major manufacturers and is the basis of MULTICS' protection rings [23].

No other discussions of substance on hardware took place, though it was observed that microcode or ROM versions of the access control mechanism make the central access controls kernel security strategy very attractive.

10. Fabry, R. S., "Dynamic Verification of Operating System Decisions," P-14.1/CSRP, " University of California, Berkeley, Computer Systems Research Project, December 1972.

11. Friedman, T. D., "The Authorization Problem in Shared Files," IBM Systems Journal, 9:4 (1970), p. 258-280, 18 refs.

12. Gaines, R. Stockton, "An Operating System Based on the Concept of a Supervisory Computer," Communications of the ACM, 15:3 (March 1972), p. 150-156, 5 refs.

13. Graham, G. Scott and Peter J. Denning, "Protection-Principles and Practice," in 1972 Spring Joing Computer Conference, Volume 40, (AFIPS Conference Proceedings, (LC 55-44701), p. 417-429, 20 refs.

14. Graham, Robert M., "Protection in an Information Processing Utility," Communications of the ACM, 11:5 (May 1968), p. 365-369, 2 refs.

15. Hoffman, Lance J., "Formulary Model for Flexible Privacy and Access Controls," in Fall Joint Computer Conference, Volume 39, (AFIPS Press, Montvale, New Jersey), 1971, AFIPS Conference Proceedings, (LC 55-44701), p. 587-601, 33 refs.

16. Hsiao, David, "A File System for a Problem Solving Facility," University of Pennsylvania, Philadelphia, Ph.D. Dissertation in Electrical Engineering, Library No. 54220, 1968.

17. Lampson, B. W., "Dynamic Protection Structures," in 1969 Fall Joint Computer Conference, Volume 35, (AFIPS Press, Montvale, New Jersey), 1969, AFIPS Conference Proceedings, (LC 55-44701), p. 27-38, 6 refs.

18. Lampson, B. W., "Protection," in 5th Annual Princeton Conference on Information Sciences and Systems, Princeton University, Princeton, New Jersey, Department of Electrical Engineering, 1971, p. 437-443.

19. Linden, T. A., "A Summary of Progress Toward Proving Program Correctness," in 1972 Fall Joint Computer Conference, Volume 41, Part I, (AFIPS Press, Montvale, New Jersey), 1972, AFIPS Conference Proceedings, (LC 55-44701), p. 201-211, 56 refs.

20. Liskov, B. H., "A Design Methodology for Reliable Software Systems," in 1972 Fall Joint Computer Conference, Volume 41, Part I, (AFIPS Press, Montvale, New Jersey), 1972, AFIPS Conference Proceedings, (LC 55-44701), p. 191-199, 15 refs.

21. London, Ralph L., "The Current State of Proving Programs Correct," in Proceedings of the ACM Annual Conference, (Association for Computing Machinery, New York), 1972, p. 39-46, 55 refs.

22. Mills, Harlan, "Top Down Programming in Large Systems," in Randall Rustin (Ed.), Debugging Techniques in Large Systems, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1971, p. 41-55, 15 refs.

23. Schroeder, Michael D. and Jerome H. Saltzer, "A Hardware Architecture for Implementing Protection Rings," Communications of the ACM, 15:3 (March 1972), p. 157-170, 17 refs. (Presented at the Third ACM Symposium on Operating Systems Principles, Palo Alto, California, October 18-20, 1971.)

24. Sevcik, K. C., J. W. Atwood, M. S. Grushcow, R. C. Holt, J. J. Horning and D. Tsichritzis," Project SUE as a Learning Experience," in 1972 Fall Joint Computer Conference, Volume 41, Part I, (AFIPS Press, Montvale, New Jersey), 1972, AFIPS Conference Proceedings, (LC 55-44701), p. 331-338, 29 refs.

25. Skatrud, R. O., "A Consideration of the Application of Cryptographic Techniques to Data Processing," in 1969 Fall Joint Computer Conference, Volume 35, (AFIPS Press, Montvale, New Jersey), 1969, AFIPS Conference Proceedings, (LC 55-44701), p. 111-117, 3 refs.

26. Srinivasan, C. V., "A Framework for a Theory of Protection," Rutgers--The State University, New Brunswick, New Jersey, Department of Computer Science, Hill Center for Mathematical Sciences, DCS Technical Report 16, May 1972.

27. Van Tassel, Dennie, "Advanced Cryptographic Techniques for Computers," Communications of the ACM, 12:12 (December 1969), p. 664-665, 7 refs.

28. Weissman, Clark, "Security Controls in the ADEPT-50 Time-Sharing System," in 1969 Fall Joint Computer Conference, Volume 35, (AFIPS Press, Montvale, New Jersey), 1969, AFIPS Conference Proceedings, (LC 55-44701), p. 119-133, 20 refs.

4.1 Audit Working Group

Robert Daly, Donal Burns, William Brown, Ralph London, William Murray (Chairman), Alfred Basinger (Recorder), Richard Mills, Bruce Peters, Douglas Hogan (not shown).

## 4.2 GOALS AND OBJECTIVES OF THE WORKING GROUP ON AUDIT, William H. Murray

It is suggested that the working group on audit draft statements on the following:

a) Working definition of audit.

b) The role of audit in the accomplishments of broad management objectives.

c) The role of audit in accomplishing specific objectives related to the control of data.

d) The functions of an audit trail.

e) The measures of adequacy for an audit trail.

f) Impact of data storage media and/or technology on the audit function.

g) Roles of the internal and external auditor.

These suggestions are subject to the review and acceptance of the members of the working group. Participants are requested to prepare notes on these items or to be prepared to suggest alternatives and/or additions.

## 4.3 AUDIT WORKING GROUP REPORT, William H. Murray and Alfred L. Basinger

### PURPOSE

It is the purpose of this paper to identify technical considerations and provide guidance in the examination of the adequacy and effectiveness of controlled accessibility measures. It is not intended to be a proceedings of the NBS/ACM Workshop, but rather a synopsis and consensus of thought resulting from the three days of meetings. Every attempt has been made to eliminate the specialized terminology and acronyms which so often appear in papers written by data processing professionals. It is hoped, that although not written by auditors for auditors alone, it will be usable by them as well as by the data processing community. This paper only scratches the surface of a complex subject, but it is hoped that it will provide a beginning to better auditing of controlled accessibility measures.

### STATEMENT OF THE PROBLEM

Access control measures are needed because information systems tend increasingly to be repositories of data which represent significant value or sensitivity. There is a corollary need for independent verification that adequate controls are operative on those access control measures.

Certain technical factors affect the problem. First, the storage media of modern digital computer systems are increasing in capacity and speed. This increases the amount of data which can be stored, and decreases the elapsed time to access it. Second, remote terminals ease the access to stored data by persons who are not at the actual computer site. This capability aids anonymity and makes more difficult the gathering of evidence concerning data access. And third, as systems are automated, there is a tendency to depend more on automated controls and less on human controls.

There are management factors which also affect the problem. A distinction must be made between the "classical audit" and the "internal audit." Also, the basis of control over the information system must shift from being document-oriented to being information-oriented. Regardless of the source of the information or its originator, the control of information must be based on what it represents. The value of data is its content, not its origin or media.

APPROACH

The approach of the workshop was first to define the scope of the problem to be dealt with. Next, some assumptions and definitions were agreed upon and some basic principles were developed. Finally, some areas which deserve more attention and action were identified.

POSITION

In the context of the NBS/ACM Workshop on Controlled Accessibility, the scope of discussion of audit will be limited to computer-based information systems with a need for access controls.

TERMINOLOGY

As in many other technical areas, the entire subject of controlled accessibility suffers from a lack of well defined terms. This is particularly true concerning that portion of controlled accessibility referred to as "audit." Webster lists two forms and four definitions for the word "audit." The noun form and transitive verb form each have two definitions.

- Noun Form:

  1. a) A formal or official examination and verification of an account book.

     b) A methodological examination and review.

  2. The final report of an examination of books of account by auditors.

- Verb Form:

  3. To examine with intent to verify.

  4. To attend (a course) without working for or expecting to receive formal credit.

Definition 1a) refers to that type of audit which is most well known, the audit of an account book. More generally, this refers to a financial audit which in today's business world is considered a necessity. This type of audit is formally defined and carried out by auditors who are either external to the company being audited, or internal to the company but independent of the organization being audited. The key to the financial audit is that it is independent and objective. These same attributes must be maintained when defining audit in terms of controlled accessibility.

Definition 1b) does not refer to a specific object of an audit. Within this definition, we may regard the controlled accessibility methods themselves as the object of an audit. This definition also gives us another attribute which must be present, that is, a methodical examination and review.

Definition 2 refers to the output of definitions 1a) and 1b). An audit of the controlled accessibility methods must be conclusive. It must either state that the methods appear to meet their objectives, or must recommend actions to be taken. This means that the audit must have sufficient information on the methods themselves and what has actually occurred within the information system. This leads to the conclusion that an audit trail is necessary in an information system to be audited. This concept will be discussed in more detail.

Definition 3, for the verb form, indicates that an audit must verify some occurrence. Within the context of controlled accessibility, the access control mechanisms must be verified.

Definition 4 refers to the audit of a course of study. This definition does not concern us other than the fact that this type of audit is a long-term proposition, not just a one-time event. As we consider audit with regard to controlled accessibility, we must bear in mind that it too should be a continual process, of which formal events and actions will be only a part.

Each of these definitions is reflected in the formal definition of audit chosen by the workshop.

DEFINITION OF AUDIT

An independent and objective examination of the information system and its use (including organizational components):

a) Into the adequacy of controls, levels of risks, exposures, and compliance with standards and procedures.

b) To determine the adequacy and effectiveness of system controls vs. dishonesty, inefficiency, and security vulnerability.

The words "independent" and "objective" are key to the definition. They imply that audit complements the normal management inspection, visibility, and reporting system. It is an essential adjunct to, but neither a part of, nor a substitute for, line management.

ASSUMPTIONS

Several assumptions are made concerning the ability to achieve such an audit capability. First, it is assumed that the other components of controlled accessibility exist. They are the access control mechanism, an adequate method of identification, and a means of measuring exposure. And second, it is assumed that audits of the access control methods are necessary.

REQUIREMENTS

In order to implement an audit capability as defined above, three requirements have been determined. Certainly, there are other requirements, and surely these can be expanded and/or refined.

Requirements for Auditability of an Access Control Mechanism

a) The rules for access should be expressed in terms which can be understood by an auditor. An access control mechanism is not auditable if it requires the access criteria to be stated in terms understood only by programmers or others having a high level of technical expertise (such as set-theoretical notation). The auditor must be confident that he understands the data access criteria as they are stated to the computer system.

b) The audit trail should permit the determination of three kinds of information.

- First, it should permit the auditor to determine who is accountable for a change to the data access criteria. It should be possible to determine the individual who made the change and should pinpoint the time when the change was made.

- Second, it should permit the auditor to determine what the access control criteria were at any point in time. The

auditor must be able to verify that the access control mechanism has been operating properly at any time in the past.

- And, third, the auditor must be able to verify that no access was allowed which did not meet the access control criteria.

Requirement for the Audit Trail

a) The audit trail must be adequate to fix accountability for each variance. A variance is an event where the access control mechanism detected and responded to an action which did not meet the access control criteria. The record of the variance must contain information sufficient to identify the individual responsible for the variance and to pinpoint the time when it occurred.

b) The audit trail must be maintained in such a way as to achieve the desired probability that each variance will come to light. It is probable that a large amount of information will be recorded in the audit trail, much of which may never be used, but all of which must be accessible and presentable in a meaningful way. It must be possible to extract from this mass of data information concerning variances from the access control criteria and to present it in such a way that the variances may be readily recognized.

Requirements for Auditability of an Information System

These requirements are applicable to the manual and organizational components of the system as well as to the computer-based portion.

a) The information system must be divisible into discrete, isolatable components. The auditor must be able to concentrate on one component of the system at a time. It is unreasonable to assume that an adequate audit of the system can be performed on a global basis. Modern information systems tend to be sufficiently complex that no single individual can comprehend all of a system's detailed functions from an overall point of view.

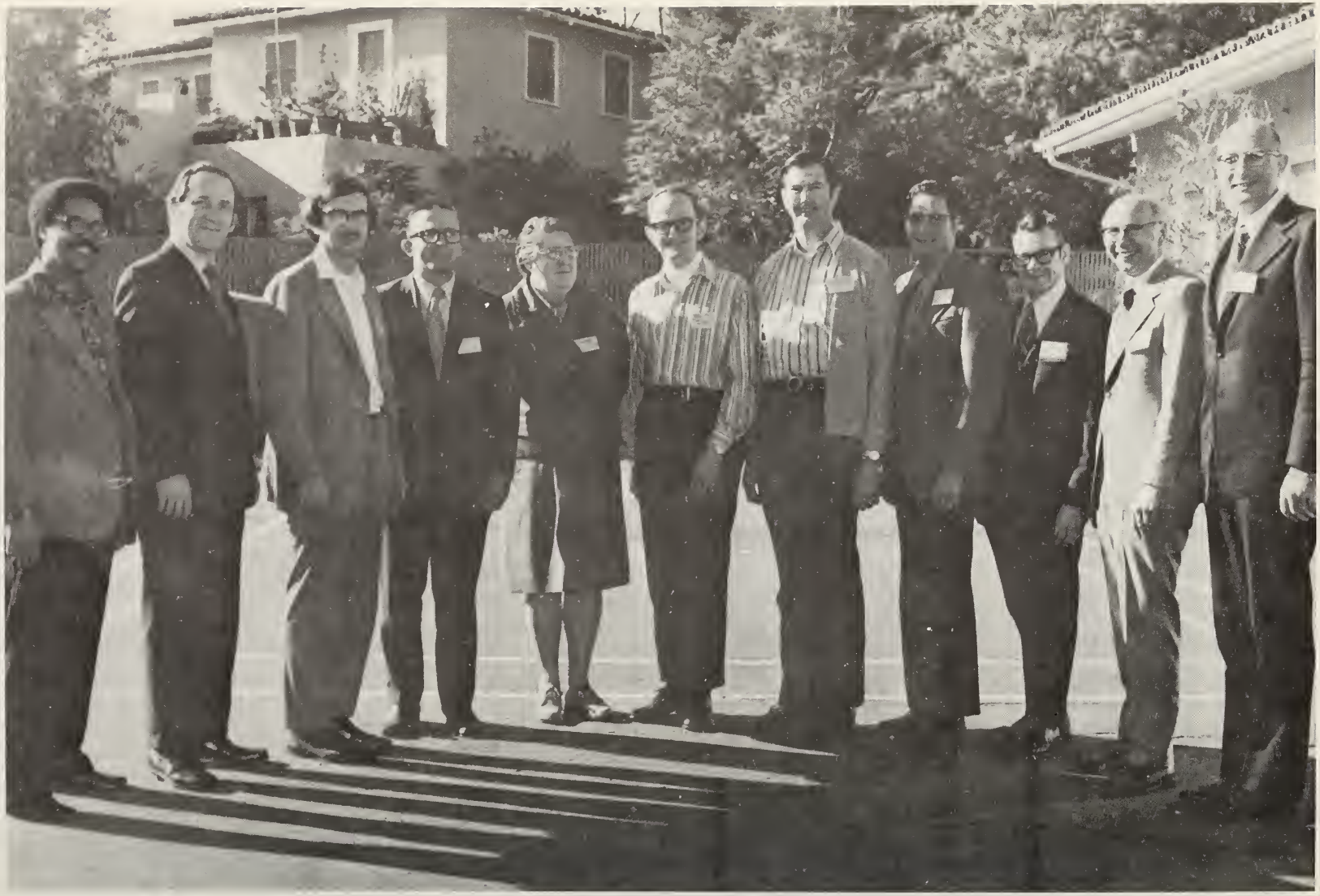
b) The system components must communicate across limited and predictable interfaces. The transfer of information between the components must be understandable. In order to be understandable, the number of interfaces must be limited, they must be readily identifiable, and they must allow only predictable actions to occur. The data which are allowed to be transferred across these interfaces must be defined as to format and content.

c) It must be possible to record up to 100% of the data transferred across the interfaces between system components. In order to verify that the access control criteria are being properly followed, it must be possible to trace the flow of information in the system.

d) The components of the system must have been produced in conformance with approved standards. All modifications to the components must also be done in conformance with approved standards. The standards themselves must be auditable.

RECOMMENDATIONS

1. Joint Activity. The Association for Computing Machinery and other professional socieities (of auditors in particular) should undertake a joint activity to produce more auditable systems and more useful audits. The implications of several system design criteria are contained in the foregoing discussion of audit. However, the ultimate definition of such design criteria should be based on dialogue fostered by professional groups of the data processing field, the internal auditing field, and the independent auditing field.



5.1 EDP Management Controls Working Group
Robert Abbott, Ruffin Cooper, Walter Simonson, E. Rex Krueger (Recorder), Isabelle Crawford, Robert Scott, Philip Enslow, John Joyce, Douglas Thompson, Clair Maple (Chairman), Donn Parker.

## 5.2 GOALS OF THE EDP MANAGEMENT CONTROLS WORKING GROUP, Clair G. Maple

The group will examine the technical management factors of EDP installations pertaining to the security of data and programs which influence the design and implementation of computer systems that offer both communications and data processing services. The goal of this study will be to set forth the design criteria and implementation procedures to insure maximum security, with due consideration being given to reliability, efficiency, and economy of operations, the ease of use, and the ability to share particular information with specific people. When there are trade-offs possible, we will examine the range of possibilities in an attempt to determine the influence other factors have upon security. We will examine the impact on current computer systems that security requirements will cause and attempt to answer the question as to whether these problems can be anticipated far enough in advance to provide guidance in the formulation of appropriate criteria to be specified to resolve such problems.

It is generally agreed that current operating systems do not provide adequate security mechanisms. What should be our stance with respect to add-on's to present operating systems with the intention of providing increased security? Should the operating systems be completely redesigned, taking security requirements into consideration? How much efficiency and economy of operation can we trade-off for increased security?

Another area which we will address is the question of physical security, in an attempt to formulate criteria to insure the physical security of a computer facility including the communications associated with teleprocessing. In this same general area, there are questions concerning personnel policies of the operational people and systems analysts as well as the programming staff. Who should design, code and maintain security mechanisms? Who should be responsible for the communication facilities after they leave the computer room? How do we deal with the outside world in handling classified information?

## 5.3 EDP MANAGEMENT CONTROLS WORKING GROUP REPORT, Clair G. Maple

Since the computer is a relatively new device, the application of the general principles of management to computer installations has been evolving quite rapidly and we are still seeing major changes taking place in an attempt on the part of management to keep up with the changes in computing procedures brought about by the rapid changes in computer technology. The question of data privacy and security in computerized information systems had not been a major concern of EDP management until the last few years. Undoubtedly, this concern about

the security of private data files was generated by the increased capabilities introduced into computer processing when it was realized that computers could be quite cost effective in areas other than numerical calculations.

The Congressional committee hearings on the National Data Bank concept and Credit Bureau information systems which took place in the late sixties brought the privacy question to the attention of the general public as well as the computer community. This in turn raised questions concerning systems integrity and computer security in the minds of computer specialists. Currently data security design and implementation remains more of an art than a science and will until adequate theoretical foundations are developed.

## GENERALIZED APPROACH

One of the objectives that management should pursue relative to controlled accessibility is the fostering of theoretical work in this area, to be followed by the development of analytical tools for use in the general area of data security assurance. In particular, there are needs for measures for evaluating the extent of the problem itself. Once the extent of the problem has been determined, we should then develop measures which will determine the risk involved and the cost and impact of the potential loss. This should be done in a manner that will present management the information required to make a judgment as to whether the cost of avoiding the risk is justified which will lead to a cost/benefit analysis and identification of technical considerations which must be taken into account before a management decision can be made as to which is the proper direction and to what extent measures for computer security should be implemented in the given environment of the computer installation.

EDP management controls span the range of people problems, technical problems, and political problems, for which there is usually incomplete information available. Nevertheless, when a proposal to implement computer security is presented to management, a decision must be made as to whether it is in the best interest of the organization.

## MANAGEMENT INVOLVEMENT

The development of computer time-sharing technology in recent years makes possible simultaneous on-line access by many users at remotely located terminals. This development has exacerbated the problem of protection of users' stored programs and data against unauthorized deliberate or accidental alteration or disclosure to other users.

Considerable technical work has already been done to provide protection against accidental access due to hardware and/or software malfunction under the heading

of systems integrity. However protection against deliberate attempts to gain access to private information has been given too little attention. Only recently has it been discussed and then usually from a philosophical point of view with sporadic attention given to its technical aspects.

It seems that these developments have reached the stage at which it is appropriate for EDP management to ask itself what can be done to protect the users' programs and data files at a minimum cost and inconvenience.

1. The Role of EDP Management. If we restrict our attention to that environment in which the EDP installation is an auxiliary enterprise responsible to a parent organization, then clearly its function is to support its parent by providing appropriate EDP services to that organization. In providing this service, the programs and data which the EDP installation processes are an asset of the parent company which requires proper protection. It, therefore, seems proper for EDP management to make every reasonable attempt to prevent such losses by trying to anticipate the action of offenders, preventing the action, or attempting to apprehend them in the case of a violation. From an even more self-serving point of view, if a violation of security occurs, EDP installation management wants to be in a position to defend its action to its senior management.

2. Identifying the Problem. In order to understand the problem of providing security for a computer system, it is necessary to examine the threats to data. Data may be lost due to failures of hardware or the use of incompletely debugged software. However, such losses are more properly the subject of systems integrity and will not be discussed here. It is felt that improvements in hardware reliability and the more recent developments in memory protection schemes are such that we can start with the assumption that the lack of systems integrity is not of major importance in the loss of data. Rather, we will examine the nature of some of the attempts on the part of an intruder to deliberately try to obtain data he is not authorized to have. Such an "intruder" may also be a person or agency making unauthorized use of data or proprietary programs available to him as an authorized user.

Information may be obtained covertly by wiretapping or electromagnetic pickup at any point in the system. In a system which uses a public communications system, that part of the communications system which lies outside the physical boundaries of the EDP facility is the most vulnerable part of the system. Hence, users of such systems who have sensitive information to protect should not entrust that data to a public communications system without providing additional protection such as the use of cryptographic techniques.

Normal access procedures may be used to enter the system to obtain information directly or to alter information in the files by asking unauthorized questions or browsing in the files to see what information resides there. It is quite possible

that normal access procedures may be used by an unauthorized user after he has obtained them through wiretapping, theft or other means.

Access to a system might also be obtained through the personnel associated with the EDP shop. It is entirely conceivable that a disgruntled or unsatisfied employee, such as a systems programmer, operations or maintenance engineer may take advantage of the weaknesses of the system; or deliberately create by-passes of the security system for his own use, or for the use of some accomplice outside the organization.

Special terminals may be tapped into the system to intercept the communications between the user and the processor for the purpose of getting access to the system while the legitimate user is inactive but his line is still open.

Other methods for intruding into the system will occur to the reader and new ways of doing it will undoubtedly be discovered by incipient intruders if the stakes are high enough. One should not discount the ingenuity of would-be intruders nor brush off the threat of information privacy too quickly.

MANAGEMENT RESPONSES

It is the responsibility of EDP management to examine the possible threats that exist in its particular installation and attempt to come up with a realistic assessment of the potential danger that each of the methods of unauthorized access might offer to his shop. Some of the factors that need to be considered involve the goals of the installation, which clearly may differ by industry, academic institution or government installation. The method of collecting data pertinent for a threat analysis in a particular installation, the purpose of such a study, and how to evaluate the results of the study.

1. Threat Evaluation. Once the extent of the threat to security has been established, management must make a judgment of the impact that actual loss of security would have on his organization. For example, if the installation is an academic computer center on a university campus, then possibly the principal type of losses that are to be avoided are the loss of free computer time and the loss of proprietary programs. On the other hand, if the installation is in an industrial setting, there may be files of information worth millions of dollars to the parent company.

Under these circumstances, it is the responsibility of management to place some value on the loss, disclosure, or modification of this information. One approach that has been suggested is as follows: for each file, attempt to determine a gross value for that file in the event of disclosure, modification and destruction from either accidental or intentional causes. Usually the accidental loss of a file will not be as great a loss as an intentional loss, due to the fact that backup files are

kept. In such an instance, the dollar loss is just the cost of recreating the file from its past history. However, the intentional loss of information may decrease or destroy the competitive edge that the parent organization has in its industry.

After a dollar value has been placed on a file, an attempt should be made to determine the probability that the file will be either accidentally or intentionally disclosed, modified or destroyed. Though at first thought this may not seem possible, a rough estimate can be made of the probability that the file in question may be compromised either accidentally or intentionally.

Having put a dollar value on each file and a probability for each type of loss of security, it will then be possible to arrive at a figure representing the impact of the loss of any combination of information files.

2. Controls Evaluation. Once it has been determined that there is a need to implement access control mechanisms, the candidate security measures should be examined to determine their relative effectiveness and cost in the specific environment of the installation. These mechanisms should provide for identification, authentication and authorization. Authorization is given to a user to access the computer facility, certain data files, certain terminals and certain processing resources. A given user may be permitted complete access to certain information while being restricted to read only from another file. Any user attempting to enter the system must first identify himself (and/or possibly his terminal if he is a remote user) and be able to authenticate his identity and access authorization. In turn, if a user is working at a remote terminal, there is a need for the processor to identify and authenticate itself to him in order to assure him that he is actually communicating with the processor he expects, instead of a processor interposed by an infiltrator.

Some methodology needs to be developed for choosing or rejecting a particular access control mechanism in order to arrive at an array of mechanisms adequate to the environment in which it is to be used. Each mechanism should be examined from the point of view of simplicity, generality, ease of implementation, cost and vulnerability to penetration.

One suggestion has been made concerning the way in which a choice of mechanisms may be arrived at. The idea involves creation of a matrix whose rows represent possible mechanisms and whose columns represent the above characteristics. An element $R_{ij}$ of the matrix is a rating, possibly on a scale of ten, of mechanism i with respect to characteristic j. Then a simple row sum gives a relative evaluation of each of the candidate control mechanisms. If certain characteristics are judged to be more important than others, then a weighted row sum could be computed using appropriate weights for the characteristics.

This methodology should also include the costs, both one-time and recurring, direct or indirect for all mechanisms taken into consideration. These costs are accrued in machine overhead, people, and time, but should be reduced to dollar costs as a common base. The costs involved in implementing a control mechanism should include the initial planning and design as well as the initial costs of hardware and software. Recurring costs include operating and maintenance costs and the decrease in computing capability caused by use of the control mechanism.

To date, there is very little information available concerning the cost of access mechanisms, but estimates of costs should be made for each candidate mechanism. Then, combining these cost estimates with the preceding evaluation, it is possible to come up with a cost effectiveness figure for each candidate mechanism.

## MANAGEMENT CONCERNS

EDP management must deal with an array of complex problems that usually far exceed those skills and responsibilities commonly associated with data processing. Demands for sophisticated understanding of comprehensive systems design previously not required imply that management summaries must be made available in order that management be able to make reasonable judgments in the choice of access control mechanisms and understand the operational implications of such devices from the user's point of view.

### Technical Criteria

Some of the topics for which technical solutions should be provided to management include Identification, Access Control, Audit and Measurements, and are the subjects of other sections of this report. These technical publications should include documentation of the critical security criteria and features. In a sense such a procedure would impose a de facto set of standards for the protection of data and computing resources, but conscious effort should be made to guide the evolution of such standards.

The management of an organization must recognize and assign responsibility for the overall flow of its information, including control over the synthesis of sensitive data from non-sensitive data, while at the same time preserving the confidentiality of the individual items of data.

### Policy Criteria

Several additional areas of concern exist with respect to controlled accessibility which we feel are particularly important for the senior data

processing management in any organization. While all management factors should be analyzed and used within the context of computer security, these areas are such that the organization may turn to senior data processing management for leadership in policy determination. Thus, there is a need for detailed study of the relationship among these factors and technical recommendations for the policy makers.

1. Organization. One area of concern centers around the impact that the need to provide access control mechanisms may have on the organizational structure of the data processing installation and its parent organization. Who is to be responsible for the development of policy and the assurance of performance under these policies? There seemed to be agreement that implementation and maintenance of access control mechanisms should be the responsibility of one group but that verification that the system software and hardware performs as specified should be done independently. The verification should include exhaustive initial test of both hardware and software and periodic checks at later times. Any time that a modification is made to a control mechanism, there should be a reverification that it works as intended. Verification of hardware integrity after each modification should be standard procedure and an inspection should be performed to detect any unauthorized changes that might leave an entry into the system which bypasses the access control mechanism. It should be standard policy that all users, including the systems analysts, be required to work within the framework of the control mechanisms. No one should be permitted to bypass the control mechanism simply because it is more efficient to do so for his particular job.

2. Planning. It has been common practice for users of data processing equipment to define their needs and then look to the vendors for an appropriate computer configuration to satisfy those needs in a cost effective way. How should vendor performance in this area be measured? To what extent should we look to vendors for leadership in this area? Currently we find installations that are using vendor supplied control mechanisms and others that are developing their own.

3. Operations. Whenever a new capability is introduced into a computer system, there is a need to educate the user to its functions and proper use, so the question naturally arises as to who is responsible for the education of the users in the need for, availability of, and the use of controlled accessibility techniques. It would seem appropriate that the EDP installation management should assume the responsibility of making access control mechanisms available to the users and of educating them in their proper use. However, the education concerning the security needs and responsibilities of the user may well be done under the aegis of the corporate security management outside the computer installation.

4. Training. If a computer installation determines that access control mechanisms are justified to minimize the loss of confidential data, then certain questions arise concerning the hiring, education and professional development of the employees who perform the operations and technical services associated with this activity. It is almost a truism that the effectiveness of any security system ultimately rests with the individuals who have access to the system so that the integrity of any security system will eventually be resolved at the human integrity level. Since computers, both hardware and software, were developed by man; and since the data stored in them is not useful without human interaction, it is important to develop programs that address personnel problems in a straightforward manner. Thus, it is important that standards be developed for all individuals who interact with the security system and to provide specific training for them. All personnel should be kept informed on a continuing basis regarding the objectives, functions and operational responsibility expected from them. The installation should provide competent supervision so that at no time is there any unresolvable question concerning proper procedures.

5. Government Controls. Another area which EDP management should be aware of concerns the legal issues and legislative action with respect to the requirements for security of computer based data. Existing laws and legal precedents as well as their application affect the selection of access control mechanisms and may vary from state to state. For example, in one state the theft of a program or data may be treated as a larceny whereas in another state it may be treated as wrongfully obtaining trade secrets.

EDP management should be aware of any legal implications associated with the installation of access security methods. What federal, state or local laws or regulations affect the need for controlled accessibility? Several states are currently in the process of developing computerized information systems associated with law enforcement and criminal investigation activities. There are states having no laws controlling what information may or may not be put into such systems. Thus, the question arises as to the role that EDP management should take in stimulating new laws or modifying old ones insofar as they affect the security system.

6. Security Violations. Closely associated with the legal issue is the question of what sanctions should be imposed upon individuals and organizations who intentionally cause losses or violate the security procedures. Clearly, from the system point of view, any violating program must be completely and thoroughly suspended. If a job is divided into concurrent operating activities, all such activities must be terminated. If a task has invoked a sequence of requests, all such requests must be canceled. Violation of security rules must result in complete cancellation of the violating request.

From the management point of view, mere cancellation of a request may not be sufficient penalty to apply to violators to discourage repeated attempts to breach

the security of the system. The additional penalties that may be applied include civil and criminal penalties under existing laws, such as payment of money and other forms of compensation to the victims as well as privately applied penalties which might include loss of employment, demotion, or loss of membership. Precisely what sanctions might be available for use against employees, vendors and users for failure to comply with the security policies is an area of concern that needs additional study.

7. Use of Insurance. Another area of concern for EDP management is the tradeoffs between access control and insurance as a method of protecting data. Insurance can be bought for most risks to data, but never covers intentional destruction. Media insurance can be purchased to cover physical loss or damage to all forms of media, including magnetic tapes, paper tapes, cards, disks, drums, and other forms of information storage associated with computing. Generally there is a distinction made between source documents and input media; it is only the input media which are insured in whole or part.

The most difficult part is determining the proper value for media. There are two methods for valuing media insurance. The insurer can establish a fixed price on each item, such as a reel of tape, or punch card; or he can use the actual cost to reproduce the media in case it is destroyed. It may be appropriate to include not only what it originally cost to produce the data media, but also the additional expenses that will be incurred as a result of loss. Insurance does not appear to be a substitute for good computer security but good computer management and security can result in lower premiums.

8. Custodial Responsibility. Given that a computer installation stores sensitive data, a question arises as to the extent of the custodial responsibility for the security of data beyond usual good management practices. Once the data has been stored in the computer system, should the user provide additional security for his data beyond that supplied by the data center? Does the user have any responsibility in determining the acceptability of standards for controlled accessibility?

## CONCLUSION

It appears that there exist threats to information stored in computer systems which have only recently been recognized and only even more recently has the problem been given serious consideration. The development of techniques to provide adequate access control will require some time, and considerable work is still needed to move forward in both theory and practice. It is the responsibility of the computer community to take the possible threats to sensitive information into consideration in systems design. Users must become aware of these considerations and be ready to assign dollar values to the information they entrust to a computer system.

6.1 Identification Working Group

James Tippett (Recorder), A. Michael Noll, Irving Solomon, Francis Quirk, James Burrows, Dennis Branstad (Chairman), Lance Hoffman, Eldred Nelson, Steven Lipner, Hatcher Chalkley, Harvey Bingham, Frederick Way.

## 6.2 GOALS AND GUIDELINES OF THE IDENTIFICATION WORKING GROUP, Dennis K. Branstad

An ACM/NBS Workshop on Controlled Accessibility of Computer Systems Resources will bring together a group of people working in the field of computer security and combine their knowledge in several technical areas of data protection. One of these areas is Identification.

Unique identification of resources and users of a computer system is a necessary but not sufficient condition for controlled accessibility. The numbers and types of resources in a system will grow continually as computer networks grow in size and popularity, and as the numbers of individuals who desire to use a network's service increase. Positive identification of a user is necessary to prevent a person from masquerading as one or more users with different access capabilities. Once a user is identified and verified, various other access controls can supervise the sharing or separation of resources and information in the system.

Various terminals that can access a computer system must be uniquely identified in order to categorize the information that may be presented to them. It may also be desirable to control the types of requests that may be made from them depending on their physical vulnerability. Computers, storage devices and removable storage media, programs, processes, and data files, as well as records and fields within files, may all need to be identified in order for an access control mechanism to function. Controlled items may have to be grouped and these groups identified for efficient access.

1. Goals of the Working Group. The goals of the identification working group include discussing and formulating answers to the following types of questions:

a. What needs to be identified in a computer system and how can it be accomplished? Which identified components need to be authenticated for security?

b. How and where should identification take place?

c. How can an individual be uniquely identified to a computer system without human intervention?

d. How do identification/authentication procedures affect access control within a computer system and within a computer network?

e. How can a wide variety of terminals be uniquely identified in a large network? How can computers be identified? How can operating systems and programs be identified?

f. What level of certainty can and should be placed on identity? Should the methods used for authentication of identity change as a function of time, place, work classification, etc.?

g. What risks are involved in incorrect identification? What is the probability of accepting an incorrect claim of identity? What is the probability of rejecting a correct claim of identity?

In establishing the goals of this working group, it is recognized that authenticating all possible parameters and components in a computer system is a tremendous task. Only a subset will be picked for consideration and only a few aspects within it will be investigated.

2. Guidelines for the Working Group. The only guideline for the working group will be to restrict our attention to the general topic of identification. Our procedure will be to have informal presentations of the technical working papers submitted by the members, followed by group analysis of the effectiveness and cost of implementation and refinement of the problems and their definitions. The emphasis will be on specific examples of identification techniques and how they would be implemented, including the protection of identity parameters in a computer system.

## 6.3 REPORT OF THE IDENTIFICATION WORKING GROUP, Dennis K. Branstad

The purpose of this report is to define the problems that were discussed and to outline the solutions that were presented by the identification working group. It is intended as neither a proceedings nor a transcript of the session, but rather as a unified presentation of the results of the workshop. The paper is designed to be a technical overview of the subject and should serve as a basis for further discussion and research in the area.

The recommendations of this working group must be accepted as only one part of the overall solution to controlled accessibility. These results must be integrated with the results of the other working groups, especially with those of access control, to form a unified solution. Only consistent efforts at defining these various roles and relationships within a computer system will achieve the desired long term goals.

### 1. PROBLEM DEFINITION

Controlling access to the data stored in a computer system consists of a series of processes which result in decisions based upon information available to each

process. Included in the set of information required for various processes is the identity of the:

- Process itself.
- Individual requesting access.
- Device from which the request was made.
- Device or process to which the requested information is to be sent.

Identification of the processes and their parameters is necessary for this sequence to occur, but simple identification is not sufficient for the sequence to be done securely. Some verification of the claimed identity is necessary at each step in the sequence to insure that a false claim of identity does not yield access to information or service that would normally not be authorized.

This verification of a claimed identity is technically called authentication. Thus, controlled accessibility requires not only a claim of identity, but some method of proving this claim. The latter proof is authentication. Its implementation depends on many factors:

- The resource being authenticated
- The risk involved
- The direct cost
- The overhead in reduced utility and efficiency

a. Statement of the Problem. The problem presented to this working group was to specify the general and specific elements of a computer system and a network of such systems that require identification in order for the system to function, and that also require authentication to be secure. The specific solution to each of these problems would depend on implementation considerations. Thus the group concentrated on outlining generic solutions, which included how and when such solutions would be accomplished, and cost versus risk analysis at a primitive level.

b. Approach. The approach used by the identification working group was to divide the large mutual identification/authentication problem into parts and to decide which parts were applicable for further discussion. The twelve people in the working group were divided into subgroups of three and each subgroup was assigned one of four identification areas of interest. The results of the work of these subgroups form Section 2 of this report.

c. The Identification Problem Matrix (Figure 6.1). The identification problem was segmented into several areas in order to direct discussion. A requirement for mutual identification and authentication among certain elements of a computer system suggested a two dimensional matrix. This allowed a pairing of elements resulting from taking all possible combinations of two elements

of the set. The first item in a pair was considered to be the element being identified and the second item as the one doing the identification. The final items chosen were: people, terminals, computers, programs, operating systems, and data. The working group then discussed each of the thirty-six resulting pairs for their applicability in an access control mechanism. Seventeen of the pairs were thought to be worthy of discussion. Figure 6.1 shows the matrix and the checks mark the pairs chosen for discussion.

d. The Expanded Identification Problem Matrix (Figure 6.2). The matrix approach of analyzing the identification requirements for security of computer system elements was found to be very helpful. In discussing proposed solutions which could satisfy these requirements, a second matrix was developed. The checked items of interest from Figure 6.1 were used as the ordinate of a second matrix (Figure 6.2). The abscissa was divided into two sections: identification and authentication. These sections were then subdivided into the questions that needed to be answered in satisfying the identification requirements.

The questions in need of answers are generally the same for the areas of identification (a process normally required in a computer system) and authentication (the process which proves that the identity is correct) except that the question is "why is identification needed?" in the first case and "what is the risk?" in the second.

## 2. SUGGESTED SOLUTIONS

The expanded identification problem matrix (Figure 6.2) yields a very large number of questions to be answered. In order to reduce this number, they were grouped into four areas for solution: people, hardware, software, and data. For the duration of this section, verification will include the processes of identification and authentication.

### a. People

The area of automated personnel identification without human assistance is the area of identification most commonly considered when discussing controlled accessibility. It generally involves the recognition of some characteristic unique to the individual, such as something that he has or some information that only he knows. The questions to be answered in this area fall into the following categories.

#### (1) People Verification (Identification and Authentication) by a Terminal

| Element being Identified \ Identifier | People | Terminal | Program | Data | Computer | O.S. Superviser |
|---|---|---|---|---|---|---|
| People | | ✓ | ✓ | | | ✓ |
| Terminal | | | | | ✓ | ✓ |
| Computer | | ✓ | ✓ | | ✓ | ✓ |
| Program | ✓ | | ✓ | | | ✓ |
| Data | | | ✓ | | | ✓ |
| O.S. Superviser | ✓ | | ✓ | | | ✓ |

Figure 6-1 Identification Problem Matrix

| Element: | Identifier | IDENTIFICATION | | | | | AUTHENTICATION | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | How | When | Where | Why | Cost | How | When | Where | Risk | Cost |
| People by | Terminal | | | | | | | | | | |
| | Program | | | | | | | | | | |
| | Op. Sys. | | | | | | | | | | |
| Terminal by | Computer | | | | | | | | | | |
| | Op. Sys. | | | | | | | | | | |
| Computer by | Terminal | | | | | | | | | | |
| | Program | | | | | | | | | | |
| | Computer | | | | | | | | | | |
| | Op. Sys. | | | | | | | | | | |
| Program by | People | | | | | | | | | | |
| | Program | | | | | | | | | | |
| | Op. Sys. | | | | | | | | | | |
| Op. Sys. by | People | | | | | | | | | | |
| | Program | | | | | | | | | | |
| | Op. Sys. | | | | | | | | | | |
| Data by | Program | | | | | | | | | | |
| | Op. Sys. | | | | | | | | | | |

Figure 6-2 Expanded Identification Problem Matrix

(a) Where: Both identification and authentication must take place at the terminal itself. For example, computer terminals include interactive programming terminals, point-of-sale cash registers, and cash dispensing machines.

(b) How: A specialized mechanical key, badge/card reader, or embedded circuit ID card have all been used for terminal activation.

(c) When: Initially for terminal activation and perhaps continually during usage.

(d) Cost: There should be an operational cost reduction in reducing human supervision of the terminal with a trade-off of increased cost for supplying and controlling the keys, cards, badges, and their associated unlocking mechanisms. For example, magnetic striped cards cost 35-47 cents per card. Hand geometry readers cost $3000 per station.

(e) Risk: Much current security is based on controlling terminals. Access to the terminal gives access to the system or, at least, possible access to the system.

(2) People Verification by an Operating System

(a) What: The identifier of a person to an operating system is usually a name or number, either user-supplied or system-supplied. It is commonly known and hence is only a claim of an identity. An authenticator of a person must be represented as a bit pattern which can be stored and protected by the computer system. It is measured from or supplied by the user and compared with the stored pattern by the operating system.

(b) How: People can be identified by supplying their assigned identifier via the terminal. They are then authenticated by:

- Something the person is: i.e., physical characteristics.
- Something the person has: i.e., key, card, readable badge.

- Something the person knows: i.e., passwords, encryption variables, "handshaking" questions and answers.

Each of these yields a bit pattern that can be transmitted to the operating system and then compared.

(c) When: A person must be identified and authenticated upon initial access to a computer system and should be reauthenticated at random and upon security environment changes, e.g., failure of any part of the computer system. However, the user should not be overburdened with secondary authentication procedures unless the data confidentiality requires it.

(d) Where: Many operating systems have a log-in process, program, or module to perform authentication. In an extensive switchable computer network, this function may be done by a dedicated computer which then switches the connection to the desired system.

(e) Cost: The cost of identification is generally small. Input of a unique character string via a standard input device is often sufficient. However, the cost of authentication of an individual's identity is generally high. The cost of equipment to measure unique human characteristics, such as fingerprints, may be higher than the cost of many types of terminals. Similarly, the cost of badge or credit card readers on a per-terminal basis may also be high. Administrative costs for distribution and protection of authenticator patterns can be significant. System overheads for storage, retrieval, communication, and processing of authenticators will be high in some cases. The operating system may require reauthentication whenever a special access or service request is made. Reduction in operating system efficiency will generally result.

(f) Risk: At best, incorrect authentication of a user may result in unauthorized access to the data or processing resources of another individual. At worst, it can result in the total loss of system security if the identity being used has universal access privileges. Risks of incorrect authentication based on physical characteristic measurements vary with the method and the equipment. Results of such experiments can be found in the open literature.

(3) People Verification by a Program

This area is generally the same as for operating systems except that the program itself requires verification of the person using it. The program can request an additional authenticator (a password or a solution to a partially specified problem) for secondary authentication. No further analysis was made of this problem.

b. Hardware

Unique identification of computer hardware is a communication requirement. Correct addressing and routing are necessary to communicate between various parts of a computer system or among such systems in a computer network. Controlled accessibility typically has been implemented by separating facilities and by physical protection given to terminals, data files, and computers. This section deals with methods of identifying and authenticating hardware devices by other components of a computer system.

(1) Terminal Verification by a Computer

(a) How: In a system with "hardwired", dedicated terminals, identification of a terminal is equivalent to identification of the data line. Authentication can be done with a "tamper alarm" cable or other physical protection. The problem becomes more difficult in a "dial in" network or a switchable digital communication system. The terminal must send a network-unique identifier and be able to authenticate itself via a computer-known authentication pattern, parity checking, signal characteristics or cryptographic communication. "Call back" from the computer to the terminal may also be implemented, letting the responder "call back" to the calling party.

(b) When: Can be done continually in a dedicated link or within every connection, every message, or every character. Random "call backs" may also be initiated.

(c) Where: Must be done at the data communication processor of the computer.

(d) Cost: Identification is necessary for correct operation Authentication is expensive in that it causes reduced terminal flexibility in hardwired systems. In a switchable

system, both the terminals and the data ports must be augmented with added hardware for authentication, e.g., encoders/decoders.

(e) Risk: Message misrouting can occur without continual authentication. Data access controlled only by terminal segregation can result in data being sent to the wrong location. Diversion, substitution, deletion, or injection of messages on communication lines may occur without authentication procedures.

(2) Terminal Verification by the Operating System

(a) How: Operating systems generally identify terminals by their data port entry to the computer (data-line scanner number, commutator position, interrupt address, data bus address, etc.).

(b) When: Each message (character, line, record) handled by the operating system on behalf of a terminal must have the identifier of the terminal associated with it (implicitly by dedication of an I/O handler; explicitly by a message identifier in a time-sharing system). Authentication must occur at initial connect time (log-in). It may also occur before each confidential output, upon a request for security related service or at random.

(c) Where: Both identification and authentication can be done within the operating system, probably in a specially designed and protected module.

(d) Cost: Identification (identification tables, I/O handlers, etc.) is necessary for correct operation and the cost is already assumed. Storage space (main memory and secondary storage) is needed for authentication modules and tables, computation time is needed for verification procedures, and protection is needed for the module during both storage and execution.

(e) Risk: If the computer hardware is authenticating a terminal and the hardware and operating system authentication methods are integrated, the risk is minimized. If not, data can be directed by the operating system to the wrong data port and hence to the wrong terminal.

(3) Computer Verification by a Terminal

This identification/authentication requirement is similar to its reciprocal problem. The terminal needs to be able to identify the computer to which it is connected for controlled accessibility. This results in a requirement for an intelligent terminal or an intelligent terminal interface. It must authenticate the computer with a known authentication pattern (requiring storage at the terminal), protected "hardwired" connection or a secure communications protocol. The risks and costs are similar to those of the reciprocal problem.

(4) Computer Verification by a Program

Distributed computing in a computer network has become an important topic. In such a system, several processors in the network are capable of performing every process. In a system where controlled accessibility is not a factor, each processor is equivalent to every other. However, if the processors have different protection environments, a process must be able to identify the processor upon which it is executing. A program leased for execution on one processor only should be able to ensure that it is running on that processor for the economic interest of the lessor.

(a) How: A computer serial number in a read-only register; automatic measurement of a unique computer characteristic, etc. can be used to identify a processor.

(b) When: Identification and authentication should both occur during process initiation. They need to be performed only once unless the process can be transferred during execution (while in run state).

(c) Where: Identification and authentication should occur within the control processor.

(d) Cost: Only a unique readable number is needed for identification. Authentication may require special programmed checks of the computer, causing a reduction in flexibility and transferability.

(e) Risk: Computer authentication by a user program is of generally low risk. A program probably can be modified to by-pass internal checking mechanisms unless the

program randomly generates and executes the checking mechanism.

(5) Computer Verification by Another

This problem is similar to computer-terminal identification. However, because of the higher capacity for data transfer, there is a higher risk in case of incorrect authentication.

(6) Computer Verification by Operating System

The problem of identification in this instance is related to system reliability requiring automatic reconfiguration in case of a hardware failure. Most current operating systems are generated for a particular computer system configuration from a set of parameters describing the configuration. The system is generated by a special system generation program which is usually run "off-line" in a dedicated mode. The resulting operating system may have some special features for automatic reconfiguration (reduction in available memory, peripheral equipment failures, etc.), but most operating systems are static.

(a) How: Identification is accomplished by system configuration, operable equipment detection, or computer serial number. Authentication is done by programs that measure system characteristics or by testing protection features.

(b) When: Identification needs to be done during system initialization, after each restart, and after every error and automatic recovery. Authentication should occur at these times and after penetration attempts have been detected.

(c) Where: Identification and authentication should take place in various operating system modules, both in "once only" initialization modules and in the operating system kernel.

(d) Cost: Identification is needed for reliable system operation. Authentication costs will vary depending upon the implementation method which may include unchangeable component identifiers and continual system monitoring of all hardware protection features.

(e) Risk: The primary risk is an undetected failure of protection hardware permitting operation of the unsecure computer system.

c. Software

The software area was broken into identification and authentication of both the operating system and specific programs by other system components. The operating system is the key mediator of access by processes within a computer system. Therefore, users and their processes must have a way of verifying that they are, in fact, in communication with the operating system. Similarly, an operating system in a computer network must verify that it is in communication with the specified remote operating system. However, once authenticated, an operating system is the dominant controlling mechanism over user processes. These processes thus depend on the operating system's access control mechanisms for their protection.

(1) Operating System Verification by the User

(a) What: The user must know, when he initiates his first process (log-in), that he is really in communication with the operating system, instead of an interloper or spoofing program. This requires not only an identifier, e.g., version number, but also an authentication of this identity. All processes of the operating system that affect a user's security should be authenticated by the user or his agent (a process to perform this function).

(b) How: To authenticate itself the operating system must have some service or mechanism that is denied to a user or a user's process, such as:

- A user input that is guaranteed to force control of the computer into a known part of the operating system (Control C on the DEC SYSTEM 10).
- An operating system output (i.e., an asterisk in column 1) that cannot be simulated by a user process.
- An authenticator pattern, unique for each user of the operating system, which is sent to the user.

(c) When: Whenever a new interface between a user, or his process, is established with the operating system (log-in,

create new process, request for service of a secondary process or processor), identification and authentication should occur.

(d) Where: If the user is the identifier, the operating system must send a response to the terminal for visual verification. If a user's process is doing the recognition, that process must be in a computer system (but not necessarily the one being identified) and a response must be sent to the user.

(e) Cost: Any of the approaches to authenticating an operating system (b above) is inexpensive to program and operate. Each requires only a few instructions in communications code, or an additional password table. Any restriction of input or output characters (column 1 reserved, special character reserved, not allowing user-subsystem capture of control functions) may be a significant cost because such a restriction does impact programming generality. However, this cost is probably acceptable in an environment which requires security.

(f) Risk: The primary risk of a user not being able to identify an operating system is that a spoofing program, simulating the log-on process) can obtain another user's identifier and authenticator (for later use by the spoofer), can obtain other information from the user, or can simply monitor the user's activity.

(2) Operating System Verification by Another Operating System

(a) What: Identification of operating systems by other operating systems is a critical issue in networks of cooperating computers. An operating system in a network must know that it is in communication with a specified computer and a specified operating system (not a masquerading user program). If the operating system to be identified is subject to penetration or physical capture, no "network-wide" measures can be effective. In this case, the penetrator, or his agent, is actually the operating system.

(b) How: A computer-to-computer solution will partially solve this problem. Cryptographic methods can ensure communication protection and authentication between computers via end-to-end encryption and key distribution

schemes. This will prevent an unauthorized computer from imposing itself in the communication path and masquerading as each successive participant in the dialog, either actively or passively.

In a distributed network with no central authority, mere identification of what service is available is a difficult problem, especially if the network configuration is constantly changing. In a network whose computers have sound internal access control mechanisms, authentication can take place by means similar to those which are used for people and operating systems -- keys, handshaking, code words, etc. For two cooperating operating systems, a variable handshaking technique is simplest and sufficient.

(c) When: In a computer network, communication protection and authentication must be continually used. Authentication between operating systems in such an environment need occur only on communication synchronization and when errors occur at either end, with random checks for system integrity.

(d) Where: Authentication measures can be distributed (computers $A_i$ and $A_j$ each know the other's authenticators for all possible (i, j)), or centralized (computers $A_i$ and $A_j$ each apply to a central facility for joint authentication).

(e) Cost: Distributed authentication is more economical in a small stable network where each computer is known. In a large dynamic network, the central authentication facility (perhaps duplicated for reliability) may be more economical since changes are needed only at the central site and the one computer involved.

(f) Risk: An operating system that can simulate one with a level of access authority can request and obtain all the information needed by that authority. A computerized attack against another computer has a very high risk factor.

(3) Program Verification by the Operating System

The operating system must be able to identify user programs accurately in order to perform its task of activating them for

the user. The file directory search and retrieval routines normally perform this function, including assigning unique program names (generally a concatenated set of modifiers) and the maintenance of date-time information. The operating system must also be able to identify and authenticate programs and processes which are a part of the operating system and differentiate them from user's programs. A fundamental attack on today's operating systems is to make the operating system execute a user program as if it were a supervisor program.

d. Data

Recognition that data has not been replaced, modified, or deleted is of vital importance to proper operation of a computing system. This problem has been previously addressed from a reliability standpoint rather than a security standpoint. However, modification of tables or changing parameters of the operating system have been basic techniques used to penetrate security mechanisms. This section will address the problem of how to identify and authenticate data.

(1) Data Verification by an Operating System

(a) What: The operating system must be able to recognize its own data resources, especially those which impact security. These include authorization and authentication files, sensitivity files, catalogs, modules, driving tables (such as status, service request, and priority).

(b) How: Data must be identified by name and location. It is authenticated by redundancy, checksums, error detection techniques, or encryption.

(c) When: Data verification should occur whenever initialization, a request for service, reloading, status change, domain crossing, soft or hard system failure, or a system restart takes place.

(d) Where: Data verification should occur in all areas that can affect the access control mechanism and stored data integrity.

(e) Cost: Basic identification of its components is necessary for any operating system to work. Some authentication is necessary for reliability. Continual authentication will be

a. Certification methods for hardware and software systems. This area includes proof of correctness and fault tolerant hardware.

b. Structured design and implementation methods.

c. Optimized system architecture for both efficiency and security.

d. Improved human-engineered terminals which are easy to use, inexpensive, connectable to any computer, emanation-free, communications securable, and easily transportable.

e. Security enhancements to languages, control methods, data structures, and retrieval systems.

f. Digital communication networks which are inexpensive and secure.

7.1 Measurements Working Group
Front Row: Robert Courtney, Peter Browne (Chairman), Gary Carlson, Hilda Faust, Rein Turn.
Back Row: Roger Schell, Jeffrey Buzen, Richard Canning (Recorder).

expensive in overhead of operation and in design and implementation, but will result in increased reliability.

(f) Risk: The risk involved in improper authentication of internal system's data by the operating system is maximum, i.e., when improperly done, the operating system may be penetrated by a malicious user and thus yield all information that is in the system.

(2) Data Verification by a Program

(a) What: An individual program must identify and validate its data, which includes subroutines, overlay modules, driving tables, input data, and parameters for proper execution. Protection of a program's data and subprograms is especially important in command and control programs, as well as in information storage and retrieval systems.

(b) How: Identification of data is typically by name (reference, association), location (memory address, file position), or content (associative processing). Data can be authenticated by specification (upper and lower bounds, magnitude), parity, checksum, redundancy, organization, and encryption.

(c) When: Identification of data must be performed during program execution. Data must be authenticated by a program if it affects the protection domain of that program.

(d) Where: Identification of data is performed at every access interface when a data item is referenced or moved. Data structures and access tables are used by programs to identify data. Authentication procedures can be built into a program's basic logic.

(e) Cost: Data identification and authentication by a program increases design and programming cost because of increased storage space and slower data access.

(f) Risk: The risks of incorrect data verification include incorrect program execution (incorrect billing, overpayment) and denial of service (command and control).

## 3. SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

a. Summary. The working group was able to outline the solution entries of the expanded problem matrix. The solutions, although not detailed, included many new approaches not previously encountered by the group. The structured approach of identification problem analysis showed the solutions will depend on solutions to related problems, i.e., operating systems authenticating operating systems depended, at least in part, on computer-to-computer authentication. It was noted that each area of controlled accessibility depended on other areas for protection. Access control mechanisms depend on identification techniques and identification program modules depend on the access control mechanisms for protection against malicious modification. Thus each portion of an overall solution to the computer security problem must be integrated correctly into a satisfactory operational system and then operated and maintained in that condition.

b. Conclusions. The main product of the working group was to structure the problem areas of identification and authentication in a controlled access computer system. However, only partial solutions or suggestions could be given. Many problem areas which needed more definition, more refined solutions, and unified implementations were not discussed. Optimum coding schemes (using information theory), error detection and correction, handshaking procedures, cryptographic techniques, message routing, and communication switching, (all impacting identification/authentication implementations), were not covered. This workshop served only as an initial effort in identifying and satisfying identification requirements.

The optimum (or even just an acceptable) method of software implementation of access control is a major task. Trade-offs between ease of implementation, efficiency, and security must be evaluated from the viewpoint of the cost, risk, and utility.

c. Recommendations. If the members of the data processing community are to obtain the maximum benefits from efforts in creating secure computer systems, full coordination and exchange of information must be accomplished within government and private industry. Further workshops and conferences are needed to exchange information in the rapidly evolving fields of computer hardware, computer software, and computer communications.

## 4. REMAINING PROBLEMS

Many problems remain to be solved. Some of them are:

## 7.2 GOALS OF THE MEASUREMENTS WORKING GROUP, Peter S. Browne

One of the most pervasive issues in the design of secure systems is how to measure security effectiveness. How does one quantify risks, what data should be collected, what are the trade-offs, and how can one evaluate protection? The fundamental principles of security measurement techniques have not yet been well stated. The goal of this group is to search out and elucidate these fundamentals.

In order to do this, we are arbitrarily dividing this topic into four major sections. The end result of the deliberation of these may be that these are invalid boundaries, but they provide a starting point for discussions and interaction.

1. Risk Assessment. This is one of the areas in which the technology is perhaps the most advanced. There are a number of methods currently in use that assess and quantify risks that face any computer installation. Various systematic classifications have been made; perhaps the starting point is Bob Courtney's approach that says data can be destroyed, disclosed or modified, either accidentally or intentionally. Risks of empirical studies and actual experience should result in actuarial tables that quantify these risks. From there it is a simple step to determine the cost/benefit trade-off as needed for a proper security system design. Perhaps the working group should formalize the terminology and methods, pointing the way towards further research.

2. Cost Effectiveness. Cost can be measured not only in dollars, but in machine overhead and people. Time is also a factor to be considered. It is well recognized that as a system gains capability and power, it loses capability for protection. Safeguards become more complex and costly. Also, in order to determine proper cost effectiveness the overhead of the security should be measured. It is a logical next-step to consider the overhead of the mechanisms that measure the overhead (and so on). What other measures besides CPU overhead, memory use, clock-time and user convenience/inconvenience can be derived? All of these impact or cause effectiveness, and should be discussed.

3. Secure-worthiness. This is perhaps the most intriguing area for research and accomplishment. Security is never a one hundred percent proposition. The dimensions are multiple and simultaneous. Do we wish to derive measures of "break in" probability? What are the work load factors required to prevent penetration by a presumed or known threat? What is the value of a given piece of protection? Because the effect of protection is cumulative and correlative, the question cannot be answered in a simple manner. This has great implication for present activities working toward certifying systems. Our working group should attempt to derive some meaningful method to understand and quantify the protection status of any system. Perhaps the approach used by manufacturers of vaults and safes to provide "fire ratings" is a starting point for discussion.

4. Measures of System Penetration. Periodic or continual auditing for security can be very useful as a deterrent. This topic is covered by another working group. The knowledge that normal measures of efficiency or effectiveness exceed a certain threshold value could be useful in determining that someone was penetrating the system and altering or withdrawing data. Techniques to detect, measure, and set alarms automatically from within a data base when abnormal activity indicates something is "wrong" would be very, very useful. The concept of threat monitoring is at least five years old, but it appears it has not received widespread use in the real world. We know of one or two uses of the concept in real-time systems, but it appears the results are, at best, indeterminate. The workshop needs to explore further the measures required to detect and monitor.

Statistics to measure effectively the above four topics have either not been developed or are not well known. The Conway/Morgan matrix which shows a difference between proper access, and proper rebuff, successful invasion and successful defense is a useful starting point (see April 1972 Communications of the ACM).

The challenge to this working group is to develop the fundamentals of protection measurement. The need for statistics on cost benefit tradeoff, risk assessment, and the "security" merit of any given system should be addressed.

## 7.3 MEASUREMENTS WORKING GROUP REPORT, Peter S. Browne, Rein Turn, and Jeffrey Buzen

The activities of the Working Group on security measurements focused on the following questions:

1. Why measurements?
2. What can be measured?
3. How are measurements made?
4. What are the fundamental principles of security measurement?
5. What are the needs for future effort in this area?

### 1. WHY MEASUREMENTS?

There is hardly any need to argue that quantitative measurements of the relevant design parameters are a basic prerequisite in the design and evaluation of any system. Such measurements are used as a basis for design tradeoffs and for optimization of a system's performance.

In the "hard" systems engineering dealing with physical devices and processes, such measurements are natural to the devices and processes and can be performed without undue difficulty. In the "soft" systems involving the society, people and their interactions, relevant measurements are much more difficult to identify and make.

Controlled accessibility in computerized information systems appears to straddle both the "hard" and the "soft" subsystems; it involves computer hardware devices and software packages, as well as people, procedures and regulations. It is not surprising, therefore, that although there is a general agreement about the desirability of measurements in this area, to date only qualitative terms have been used.

All participants of this and other working groups agreed that a methodology is needed to design, implement, and maintain access control systems: the access control mechanisms, the detection/response subsystem, the testing and auditing function, and the management controls. It has been suggested that this methodology be called "data security engineering".

More specifically, data security engineering would provide systematic procedures for classifying access control systems; models of these systems; basic principles involved in their design, operation and interaction with other systems and operating environment; methodology for threat and vulnerability assessment; guidelines for system design, implementation, testing and evaluation; but, above all, definitions of measurements of effectiveness, cost, reliability and integrity, risk and exposure, and value of protected information. Also integral to data security engineering are techniques of making measurements, a calculus for computing measurements for composite systems, methodology of trade-off analysis, and the like.

Given a data security engineering discipline as outlined above, the design, implementation, and continued operation of access control systems would be based on a rational basis and selection of suitable access control alternatives for a given information system could be done with greatly increased confidence.

While the development of the data security engineering could be regarded as a long-term objective as well as a sufficient answer to the question "Why measurements?", there are also specific benefits which could be immediately useful without the general framework of a data security engineering discipline.

The existence of quantitative measurements would permit the following:

- Determination of relative effectiveness of access control mechanisms, subsystems, and systems.
- Performance of cost-effectiveness, cost-benefit, or cost-risk analyses.
- Assessment of the relevant vulnerabilities, threats, exposure and risks.

- Optimization of the access control system design for a given threat domain and external constraints.

- Assessment of the effects on access control effectiveness and cost of proposed system modifications.

- Design of effective detection and response subsystems.

- Specification of the access control system design requirements and criteria.

- Support and development of effective internal auditing procedures, and management procedures.

## 2. WHAT CAN BE MEASURED?

The measurements that can be made relative to controlled accessibility (i.e., excluding those considerations of physical security which deal with fire, flood, physical destruction, and the like) appear to fall into the following classifications:

- Measurements of Effectiveness of the access control mechanisms, and subsystems (i.e., the "amount of protection" against unauthorized dissemination, modification or destruction; accidental or deliberate).

- Measurements of Activity of the access control mechanisms and detection/response subsystem.

- Measurements of Structural Attributes of the access control mechanisms (such as simplicity, generality, etc.).

- Measurements of Value of protected resources to the owners of the resources, custodians, potential intruders.

- Measurements of Threat Domain: likelihoods of threats, exposure of the system, vulnerabilities, risks.

- Measurements of Personal Integrity as applied to the information system personnel and users, as they relate to controlling access, subversion, etc.

- Measurements of Costs of implementing and operating the access control mechanisms.

This list of measurement classes is not necessarily complete and exhaustive, nor is it clear that meaningful quantifiable measurements can be defined and/or performed in each class.

a. MEASUREMENTS OF EFFECTIVENESS

Effectiveness of access control mechanisms is the "degree of protection" that they provide against accidental or deliberate, but unauthorized, dissemination or modification of protected resources (e.g., programs, data or processing time).

(1) Integrity. Measurements in this category should indicate the quality of access control mechanisms in discrete values. The measurement vector of integrity can be viewed as an assessment of the effectiveness of the controls when working under various circumstances (e.g., when the associated computer hardware is not malfunctioning).

Essential components of this measurement vector are:

- Logical Completeness of the hardware and software that implements the control mechanism. This involves the verification that the access control mechanism is capable of correctly handling all possible situations -- it does everything it is supposed to do and does nothing it is not supposed to do.

- Logical Correctness of the hardware and software implementation of the access control mechanisms. The question has to do with whether or not the access control mechanism is performing the correct control operations (i.e., is the initial design correct?).

It must be pointed out that measures of logical completeness and correctness are subject to change at any time that any modification is made to hardware or software involved in access control mechanisms.

(2) Reliability. Malfunctioning hardware can lead to failure of access control mechanisms. In general, various reliability measurements are derived for the entire information system's hardware, but it is necessary for the purposes of evaluating the effectiveness of access control mechanisms to evaluate the reliability of hardware directly involved.

The measurements can be in the units normally used in reliability assessment such as probability of correct operation and mean time between failures (MTBF).

Software malfunctioning can also lead to failure of access control mechanisms. However, any errors in software are instances of logical incorrectness or incompleteness, and must be measured accordingly.

Operating system personnel unreliability will be addressed in the section on personnel measures.

(3) Intrusion Work Factor. The intrusion work factor for access control mechanisms deals with the ease of deliberately circumventing, nullifying or deceiving its operation and hence may be regarded as the level of protection it provides against unauthorized access.

Intrusion through technological means (rather than through subversion of personnel requires the following actions by an intruder:

- Obtaining sufficient information about the target system, its access control mechanisms, level of security, integrity, etc.
- Formulating an acceptable penetration plan.
- Gaining access to the target system either indirectly through a terminal, communication link, computer, etc. or directly via physical access.
- Penetrating the data bank and escaping detection for sufficiently long time to complete the action.

The access control mechanisms, as a rule, function as "locks' which can be opened by the right "key". More complicated mechanisms also require performing special operations on a key supplied by the mechanism. The objective is to increase the uncertainty of the intruder regarding the correct key (or set of keys) and, thereby, to increase the intrusion cost.

Given a particular access control mechanism and an intruder's intention to penetrate by a technological attack, the options open to him are the following:

- Determine the correct keys through systematic analysis.
- Attempt to disable the lock (access control mechanism).
- Gain control of the lock.
- Determine the keys through wiretapping or eavesdropping.

Corresponding to each activity there is effort that must be expended by the intruder. The amount of work done -- the intruder's work factor -- depends on his expertise and availability of resources and information.

The following classes of intruder's activities can be identified:

- Systematic Analyses. These are the activities to determine a particular key. Included are:
  - Combinatorial trial-error searches (e.g., for passwords)
  - Cryptanalysis
- Exploitation of Design Incompleteness and Errors. This activity is aimed at discovering ways of circumventing or capturing control of the access control mechanism. There are two parts:
  - Heuristic search for flaws
  - Utilization of existing flaws
- Penetration of Physical Barriers.
- Accumulating Dispersed Information. Compiling lists or collections of data from items that are kept in non-aggregated form in the system.

Cryptanalysis and heuristic search for flaws are complicated activities and it is difficult to establish the expected number of trials needed to achieve success. The effort involved in one iteration depends on the nature of the cryptographic algorithm or the operating system being examined. It is generally possible, however, to estimate the work factor in terms of number of logical operations and, consequently, in terms of time and cost.

Penetration of physical barriers can be measured in a way already used by the protective safe and vault industry: time for penetration.

b. MEASUREMENTS OF ACTIVITY

For penetration, detection or security monitoring, it is necessary to measure certain activities of the access control mechanism. This includes counting various actions that are taken such as:

- Number of accesses of an object by a subject.
- Number of attempted but failed accesses of an object by a subject.
- Number of functions of a particular type performed by an authorized subject.

- Number of data elements transferred, modified, or erased by a subject.

The exact activity measured depends on the detection, auditing and threat monitoring capabilities which are implemented. The measurements may be used to check the ongoing activity against sets of threshold values that have been determined to represent "normal" activity. Studies of intrusion efforts may also provide sets of threshold values which represent the "signatures" of various types of intrusion attempts and hence can be used to detect such attempts.

c. MEASUREMENTS OF STRUCTURAL ATTRIBUTES

The ability to test a given access control mechanism for logical completeness and error-free implementation is highly dependent on the following attributes:

- Simplicity. The size and structure (in terms of the number of control paths, parallelism, conditional branches, loops, and the like) is the major determinant of the feasibility of a logical completeness proof. Simplicity enhances the ability to understand the operation of the mechanism and reduces the likelihood of errors in its implementation.

- Generality. The ability of an access control mechanism to handle a variety of situations. There is a trade-off between simplicity and generality: specialized controls are simple but more of them are required to handle all circumstances.

The above attributes also affect the ease of implementation of a control mechanism. Other aspects of this have to do with the design of the mechanism in a way that is compatible with the rest of the system and its implementation.

d. MEASUREMENTS OF VALUE

The resources of a computer system include the processing capability of the system, i.e., "computer time", system- and user-owned programs, and data files. These resources have distinct, but usually different, levels of value to the owners, to the custodians (if different from owners), and to potential intruders. Further, these values are time-variant (change with circumstances and time).

Value may be expressed in dollars. The specific values depend on direct replacement costs (if resources are destroyed), costs of lost use, costs of lost exclusive possession (if copies made by competitors), and costs of collateral damages. The value to rational intruders (economically minded, profit-oriented) is the potential profits through use or sales, or avoidance of costs (as in illicit use of the computer). Values to irrational users, those who not profit-motivated, are generally impossible to ascertain.

The value of personal information stored in a computer system is especially difficult to assess. Such information has different subjective values to different owners and, likewise, different market value to the intruders. Some fact of a personal nature may irrationally be valued highly by one person, while others don't care at all.

e. MEASUREMENTS OF THREAT DOMAIN

Measurements in this category deal with assessment of the likelihood of the various types of threats against the computer system and the vulnerability of the system to these threats. To do this, it is useful to classify systems in a way relating to various classes of threats. One such classification is:

- Centralized/Decentralized. In a centralized facility, all resources to be protected are at the same location. In a decentralized system, resources are at several separate locations which are connected by a communications network.

- Off-line/On-line. An on-line system permits direct real-time interaction of a user with the resources through a terminal.

- Closed/Open. In a closed system (sometimes called a transaction-based system) users have to utilize an interaction language supplied by the system; they cannot submit any programs themselves. In an open system, users can submit programs.

- Dedicated/Shared. A dedicated system is one used exclusively for a specific application or by a single user for any time period.

In general, the systems described by the word preceding the slash are more vulnerable to threats than those described by the word following the slash.

In measuring the threat domain of a system, one should consider the following:

- The classification of the system.

- The value of its resources to potential intruders.

- The optimum location, structure, services, and the user environment if there were no potential threats.

- The political and emotional climate of personnel in the locality of the planned facility.

- History of threats, successful or attempted, against similar systems.

- The potential threats, their sources, and methods of accomplishment that have been identified.

Based on the above, it may be possible to determine the following for the given information systems and list of threats:

- Intrinsic Exposure of the system, expressed in dollars, that the owners of resources would suffer if the resources were used, modified, or disseminated in unauthorized ways.

- Threat Probabilities of potential intruders or accidents.

- Risk ((threat probability) x (exposure)).

f. MEASUREMENTS OF PERSONAL INTEGRITY

Measuring personal integrity in a quantitative way is extremely difficult. It is possible, however, to establish lists of personnel selection and administrative procedures which have proven effective. Each person then must be evaluated qualitatively against this list.

Risk assessments may also be made from a deterrent point of view, i.e., what is the likelihood of getting caught and penalized? In this case, risk = (probability of detection) x (penalty).

g. MEASUREMENTS OF COSTS

Security costs include not only initial and recurrent monetary expenditures for hardware, software, environmental controls, etc., but also loss of system availability for productive work (i.e., increase of the overhead required for access controls).

There is, however, a great deal of experience available in estimating costs of various processing tasks in computer systems, and all this expertise as well as techniques of measurement, should be directly applicable also to the estimation of costs of access control mechanisms.

## 3. HOW ARE MEASUREMENTS MADE?

The measurements discussed in previous sections are useful only if it is possible to assign values to them. Depending on the system characteristics being measured, the measurement process involves analysis, observations, simulations, tests and actual physical measurements.

Available for the measurement process are various tools from the areas of operations research, applied mathematics, management sciences, and computer sciences. Among these are:

- Mathematical models of structures and processes
- Matrix and graph models
- Theorem proving techniques
- Statistics and probability theory
- Simulation and gaming models and programs
- Operational testing techniques
- Internal auditing techniques

For each class of measurements it is necessary to determine where they are made (relative to the structure and elements of the access control mechanism and the entire information system), when they are made, and by which means. Many of the measurements can be made off-line with the system under study (e.g., measurements of effectiveness and work-factor measurements). Others are made when the system is operational, e.g., detection/response subsystem performance.

### a. MEASUREMENT OF COMPLETENESS

Evaluating the logical completeness of operating systems requires application of program proving techniques. The success of these techniques depends on the structural characteristics of the programs to be tested (simplicity, generality, etc.). One example of program proving showed that a 200-line program could be proved by one man in 2-3 months. Automated procedures are being developed, but are still in elementary stages. If the programs of an access control mechanism could be partitioned into sufficiently small modules, program proving techniques could be applied. A complicating "fact of life" of computer systems is that many changes are applied to the operating systems of contemporary computers. Each change (or set of changes) would require repeating the completeness and correctness proofs.

### b. WORKFACTOR MEASUREMENTS

Workfactors of systematic analyses can be estimated by actually performing the analysis -- determining the mathematical procedures and the number of

operations per iteration required for an algorithm attack. The expected number of iterations can be estimated on the basis of a threat analysis. Workfactor calculation is rather straightforward for a brute force testing of passwords.

A heuristic search for flaws in the hardware and software of the access control mechanism is, likewise, an iterative process. The expected number of iterations, however, is also dependent on the flaws present, as well as the expertise and resources of the intruder. A trial heuristic search may provide some insight in the estimating of a true workfactor but can be expected to be highly subjective.

The effort involved in completing a penetration once a suspected error has been found involves a workfactor measured in time. Again, evaluating this for potential intruders may require experimentation and/or simulation.

c. PROBABILISTIC MEASUREMENTS

The probabilistic measurements outlined in previous sections deal mainly with the reliability of hardware, and with estimating the likelihood of threats. If historical data is available regarding a threat and its realization in similar systems and under similar circumstances, then it can be used to establish empirical probabilities. In other situations, the potential profit that might be gained from successful intrusions could be used as a relative indication of the "temptation" facing potential intruders. Combined with other measurements, some indication of the likelihood of threats could be derived.

d. VALUE MEASUREMENTS

Certain resources have intrinsic value by virtue of what they are or what they represent. For example, computer time is valuable; a computerized bank account has direct value if it is the basis for allowing cash withdrawals. The value of these resources is determined rather directly.

Other resources may have direct value only to the parties involved. Deliberate or accidental erasure of data or a program represents a replacement cost to its custodian.

Resources have secondary value when they can be used to gain profit or benefit. Value of resources to an intruder depends on the market for those resources.

The value of information is often dependent on how widely it is known as well as its timely dissemination. Information is defined as that which helps to resolve uncertainties -- the moment an uncertainty becomes a certainty, the value of the information is lost.

## 4. WHAT ARE THE FUNDAMENTAL PRINCIPLES?

The discussions of the group pointed to a number of basic assumptions which appear to hold true for all cases. They are:

- There cannot be a single-figure metric for security.
- Analysis of the vulnerability of a computer system must be systematic and complete.
- Increasing the uncertainty of an intruder in a system will increase his workfactor of penetration.
- Increasing the difficulty of penetrating a system by one method will cause an intruder to shift his emphasis to another method.
- If security is not designed into a system, a security measurement cannot be complete.

In addition, several caveats surfaced concerning the formulation, making or use of measurements:

- It is likely that not all aspects of access control and data security are equally quantifiable. It is important not to overlook those that are not (e.g., the number of locks on the front door is not a measure of the security of the entire house, or even the front door itself -- only of the security against attempts to come through the door in a normal way).
- It is important to establish clearly the context and the scope within which measurements are made and used (e.g., there may be a tendency to concentrate on external intrusion as the principal data security problem, but as far as the management is concerned, incompetent operators and users, fire, flood, etc., may cause just as much damage and be much more likely threats).
- Measurements tend to have time-dependent values. In the area of the effectiveness of access controls, for example, the effectiveness may decrease over time as vigilance decreases, but may also increase as education programs are instituted.
- An intruder may not be entirely rational in the sense of desiring economic gain. Intrusion may be motivated by the

"genius complex", or to cause embarrassment, or for "purely evil" reasons. Trade-off analyses based on economic considerations should be made with this factor in mind.

- Care must be taken in using statistical and empirically derived probabilistic measures because the sample is likely to be extremely small. In fact, a threat of a particular type may materialize and be attempted only once.

## 5. NEED FOR FURTHER EFFORT

Since little work has been done to date in the measurement area, there is a wide scope for further research. Basically, the problems are:

- To develop methods of measuring the effectiveness of hardware/software against deliberate attack.
- To gather statistical data relating to attempted and detected attacks.
- To develop the methodology of a security measurement metric.
- To define precisely the measurements which determine the overall security of a system.
- To establish procedures for applying the security metric.

## APPENDIX

## NAMES AND ADDRESSES OF PARTICIPANTS

Robert P. Abbott
Lawrence Livermore Laboratory
Box 808
Livermore, California 94550
415 447-1100 Ext. 7421

Alfred L. Basinger
IBM Data Processing Div. Hq.
1133 Westchester Avenue
White Plains, New York 10604
914 696-1889

Harvey W. Bingham
Burroughs Corporation
Defense, Space and Special
Systems Group
Paoli, Pennsylvania 19301
215 648-7370

Joel Birnbaum
IBM Corporation
Thomas J. Watson Research Ctr.
P.O. Box 218
Yorktown Heights, New York 10049
914 945-3000

Dennis K. Branstad
Institute for Computer Sciences
and Technology
National Bureau of Standards
Washington, D.C. 20234
301 921-3485

William F. Brown
Computer Center
Ball State University
Muncie, Indiana 47306
317 285-4470

Peter S. Browne
General Electric Company
Information Services Business Division
7735 Old Georgetown Road
Bethesda, Maryland 20014
301 654-9360

G. Edward Bryan
Xerox Corporation
701 S. Aviation Boulevard
El Segundo, California 90245
213 679-4511 Ext. 1440

Donal J. Burns
Central Intelligence Agency
Washington, D.C. 20505
703 351-3404

James H. Burrows
Headquarters, U.S. Air Force
Directorate of Data Automation
Washington, D.C. 20330
202 OX5-9939

Jeffrey Buzen
Honeywell Information Systems
300 Concord Road
Billerica, Massachusetts 01821
617 667-3111 Ext. 2684

Howard H. Campaigne
Slippery Rock State College
Slippery Rock, Pennsylvania 16057
412 794-7307

Richard G. Canning
Canning Publications, Inc.
925 Anza Avenue
Vista, California 92083
714 724-5902

Gary Carlson
Computer Services
Brigham Young University
Provo, Utah 84601
801 374-1211

Walter M. Carlson
IBM Corporation
Old Orchard Road
Armong, New York 10504
914 765-4240

Michael A. Casteel
National Cash Register
16550 W. Bernardo Drive
San Diego, California 92127
714 487-1230 Ext. 2781

Hatcher E. Chalkley
Texas Instruments, Inc.
12501 Research Boulevard
P.O. Box 2909 MS2001
Austin, Texas 78676
512 258-5121 Ext. 448

Richard W. Conway
Department of Computer Science
Cornell University
Upson Hall
Ithaca, New York 14850
607 256-3456

Ruffin Cooper
National Security Agency
P-1
Ft. George G. Meade, Maryland
20755
301 688-7608

Robert H. Courtney, Jr.
IBM Corporation
P.O. Box 390
Department D05, Building 707
Poughkeepsie, New York 12602
914 463-8328

Isabelle Crawford
Software Management Information Div.
Room 604
State of Illinois
Springfield, Illinois 62706
217 525-3402

Robert M. Daly
Honeywell Information Systems
300 Concord Road
Billerica, Massachusetts 01821
617 667-3111 Ext. 56268

Ruth M. Davis
Institute for Computer Sciences and
Technology
National Bureau of Standards
Washington, D.C. 20234
301 921-3151

Albert S. Dean, Jr.
Logicon
1075 Camino del Rio South
San Diego, California 92110
714 291-4240

Daniel Edwards
National Security Agency
R-52
Ft. George G. Meade, Maryland 20755
301 688-8147

Philip H. Enslow, Jr.
Office of Tele Communications Policy
Executive Office of the President
1800 G Street, N.W.
Washington, D.C. 20504
202 395-5170

Robert S. Fabry
Computer System Research Project
2000 Center Street, Suite 301
Berkeley, California 94704
415 642-7220

Hilda C. Faust
National Security Agency
R-52
Ft. George G. Meade, Maryland
20755
301 688-8147

Gerald W. Findley
Institute for Computer Sciences and
Technology
National Bureau of Standards
Washington, D.C. 20234
301 921-3493

R. Stockton Gaines
Institute for Defense Analyses
100 Prospect Avenue
Princeton, New Jersey 08540
609 924-4600

Edward L. Glaser
Case Western Reserve University
Computing and Information Sciences
604 Crawford Hall
Cleveland, Ohio 44106
216 368-2808

Lance J. Hoffman
Department of EE and CS
University of California
Berkeley, California 94720
415 642-3445

Douglas L. Hogan
National Security Agency
R-45
Ft. George G. Meade, Maryland
20755
301 688-7854

David K. Hsiao
The Ohio State University
Computer and Information Science
Department, Caldwell Laboratory
2024 Neil Avenue
Columbus, Ohio 43210
614 422-3083

William M. Inglis
Defense Communications Agency
J410
1860 Wiehle Avenue
Reston, Virginia 22070
703 437-2401

Seymour Jeffery
Institute for Computer Sciences and
Technology
National Bureau of Standards
Washington, D.C. 20234
301 921-3485

John D. Joyce
Computer Science Department
General Motors Research Laboratories
12 Mile and Mound Roads
Warren, Michigan 48090
313 575-3008

E. Rex Krueger
Computing Center
University of Colorado
Boulder, Colorado 80302
303 443-2211 Ext. 8031

Richard Leibler
Institute for Defense Analyses
100 Prospect Avenue
Princeton, New Jersey 08540
609 924-4600

Steven B. Lipner
The MITRE Corporation
P.O. Box 208
Bedrord, Massachusetts 01730
617 271-3220

Ralph London
University of Southern California
Information Sciences Institute
4676 Admiralty Way
Marina Del Ray, California 90291
213 822-1511 Ext. 195

Peter G. Lykos
National Science Foundation
Office of Computing Activities
Washington, D.C. 20550
202 632-5747

Clair G. Maple
Computation Center
Iowa State University
Ames, Iowa 50010
515 294-3402

Richard G. Mills
First National City Bank
399 Park Avenue, Tube 33
New York, New York 10022
212 559-5487

M. Granger Morgan
National Science Foundation
Washington, D.C. 20550
202 632-5747

William H. Murray
IBM Corporation
1133 Westchester Avenue
Department 648
White Plans, New York 10604
914 696-2500

Eldred C. Nelson
TRW Systems Group
One Space Park
Redondo Beach, California 90278
213 536-2878

A. Michael Noll
Executive Office of the President
Office of Science and Technology
Washington, D.C. 20506
202 395-3547

Donn B. Parker
Stanford Research Institute
333 Ravenswood Avenue
Menlo Park, California 94025
415 326-6200 Ext. 2378

Bruce Peters
Systems Development Corporation
5827 Columbia Pike
Falls Church, Virginia 22041
703 820-2220

C. J. Purcell
Control Data Corporation
Computer Development Laboratories
4290 N. Fernwood Avenue
P.O. Box 2807
St. Paul, Minnesota 55112
612 631-0531 Ext. 4160

Francis J. Quirk
UNIVAC Division
Sperry Rand Corporation
8529 Zenith Road
Bloomington, Michigan 55431

Anthony Ralston
State University of New York, Buffalo
Department of Computer Science
4226 Ridge Lea Road
Amherst, New York 14226

Susan K. Reed
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234
301 921-3485

Roger R. Schell
Hq. ESD (MCIT)
L. G. Hanscom Field
Stop 36
Bedford, Massachusetts 01730
617 861-5386

Robert H. Scott
Massachusetts Institute of Technology
39-565
77 Mass Avenue
Cambridge, Massachusetts
617 253-4103

Kenneth C. Sevcik
Computer Systems Research Group
University of Toronto
Toronto 181
Ontario, Canada
416 928-6323

Walter E. Simonson
Bureau of the Census
Washington, D.C. 20233
301 763-5180

Irving I. Solomon
National Retail Merchants Association
100 West 31st Street
New York, New York 10001
212 244-8780

Selden Stewart
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234
301 921-3491

Douglas Thompson
State of Nevada
Department of Administration, CDP
Blasdel Building
Carson City, Nevada 89701
702 882-7369

James Tippett
National Security Agency
R-52
Ft. George G. Meade, Maryland 20755
301 688-8147

Rein Turn
The RAND Corporation
1700 Main Street
Santa Monica, California 90406
213 393-0411

Frederick Way, III
Case Western Reserve University
Cleveland, Ohio 44106
216 368-2800

Clark Weissman
Systems Development Corporation
2500 Colorado Boulevard
Santa Monica, California 90406
213 393-9411 Ext. 533

NBS-114A (REV. 7-73)

| U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET | 1. PUBLICATION OR REPORT NO. NBS TN-827 | 2. Gov't Accession No. | 3. Recipient's Accession No. |
|---|---|---|---|

4. TITLE AND SUBTITLE *Controlled Accessibility Workshop Report*
*A Report of*
*The NBS/ACM Workshop on Controlled Accessibility*
*December 10-13, 1972 Rancho Santa Fe, California*
*Dr. Howard H. Campaigne, Chairman*

5. Publication Date: May 1974

6. Performing Organization Code

7. AUTHOR(S): *Susan K. Reed and Dennis K. Branstad, Editors*

8. Performing Organ. Report No.

9. PERFORMING ORGANIZATION NAME AND ADDRESS

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20234

10. Project/Task/Work Unit No.: *640-1112*

11. Contract/Grant No.

12. Sponsoring Organization Name and Complete Address *(Street, City, State, ZIP)*

*Same as above*

13. Type of Report & Period Covered: *Final Dec 72*

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 74-600078

16. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

A report has been prepared of the NBS/ACM Workshop on Controlled Accessibility, December 1972, Rancho Santa Fe, California. The Workshop was divided into five separate working groups: access controls, audit, EDP management controls, identification, and measurements. The report contains the introductory remarks outlining the purpose and goals of the Workshop, summaries of the discussions that took place in the working groups and the conclusions that were reached. A list of participants is included.

17. KEY WORDS *(six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)*

*Access control; computer security; controlled accessibility; EDP management control; identification; measurement; security audit*

18. AVAILABILITY

[x] Unlimited

[ ] For Official Distribution. Do Not Release to NTIS

[ ] Order From Sup. of Doc., U.S. Government Printing Office Washington, D.C. 20402, SD Cat. No. C13 • 46:827

[x] Order From National Technical Information Service (NTIS) Springfield, Virginia 22151

| 19. SECURITY CLASS (THIS REPORT) | 21. NO. OF PAGES |
|---|---|
| UNCLASSIFIED | 86 |
| 20. SECURITY CLASS (THIS PAGE) | 22. Price |
| UNCLASSIFIED | $1.25 |

USCOMM-DC 29042-P74

# NBS TECHNICAL PUBLICATIONS

## PERIODICALS

**JOURNAL OF RESEARCH** reports National Bureau of Standards research and development in physics, mathematics, and chemistry. Comprehensive scientific papers give complete details of the work, including laboratory data, experimental procedures, and theoretical and mathematical analyses. Illustrated with photographs, drawings, and charts. Includes listings of other NBS papers as issued.

*Published in two sections, available separately:*

- **Physics and Chemistry (Section A)**

Papers of interest primarily to scientists working in these fields. This section covers a broad range of physical and chemical research, with major emphasis on standards of physical measurement, fundamental constants, and properties of matter. Issued six times a year. Annual subscription: Domestic, $17.00; Foreign, $21.25.

- **Mathematical Sciences (Section B)**

Studies and compilations designed mainly for the mathematician and theoretical physicist. Topics in mathematical statistics, theory of experiment design, numerical analysis, theoretical physics and chemistry, logical design and programming of computers and computer systems. Short numerical tables. Issued quarterly. Annual subscription: Domestic, $9.00; Foreign, $11.25.

### DIMENSIONS, NBS

The best single source of information concerning the Bureau's measurement, research, developmental, cooperative, and publication activities, this monthly publication is designed for the layman and also for the industry-oriented individual whose daily work involves intimate contact with science and technology —*for engineers, chemists, physicists, research managers, product-development managers, and company executives.* Annual subscription: Domestic, $6.50; Foreign, $8.25.

## NONPERIODICALS

**Applied Mathematics Series.** Mathematical tables, manuals, and studies.

**Building Science Series.** Research results, test methods, and performance criteria of building materials, components, systems, and structures.

**Handbooks.** Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

**Special Publications.** Proceedings of NBS conferences, bibliographies, annual reports, wall charts, pamphlets, etc.

**Monographs.** Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

**National Standard Reference Data Series.** NSRDS provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated.

**Product Standards.** Provide requirements for sizes, types, quality, and methods for testing various industrial products. These standards are developed cooperatively with interested Government and industry groups and provide the basis for common understanding of product characteristics for both buyers and sellers. Their use is voluntary.

**Technical Notes.** This series consists of communications and reports (covering both other-agency and NBS-sponsored work) of limited or transitory interest.

**Federal Information Processing Standards Publications.** This series is the official publication within the Federal Government for information on standards adopted and promulgated under the Public Law 89–306, and Bureau of the Budget Circular A–86 entitled, Standardization of Data Elements and Codes in Data Systems.

**Consumer Information Series.** Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

## BIBLIOGRAPHIC SUBSCRIPTION SERVICES

**The following current-awareness and literature-survey bibliographies are issued periodically by the Bureau:**

**Cryogenic Data Center Current Awareness Service** (Publications and Reports of Interest in Cryogenics). A literature survey issued weekly. Annual subscription: Domestic, $20.00; foreign, $25.00.

**Liquefied Natural Gas.** A literature survey issued quarterly. Annual subscription: $20.00.

**Superconducting Devices and Materials.** A literature survey issued quarterly. Annual subscription: $20.00. Send subscription orders and remittances for the preceding bibliographic services to the U.S. Department of Commerce, National Technical Information Service, Springfield, Va. 22151.

**Electromagnetic Metrology Current Awareness Service** (Abstracts of Selected Articles on Measurement Techniques and Standards of Electromagnetic Quantities from D-C to Millimeter-Wave Frequencies). Issued monthly. Annual subscription: $100.00 (Special rates for multi-subscriptions). Send subscription order and remittance to the Electromagnetic Metrology Information Center, Electromagnetics Division, National Bureau of Standards, Boulder, Colo. 80302.

Order NBS publications (except Bibliographic Subscription Services) from: Superintendent of Documents, Government Printing Office, Washington, D.C. 20402.

**U.S. DEPARTMENT OF COMMERCE**
**National Bureau of Standards**
Washington, D.C. 20234

OFFICIAL BUSINESS

Penalty for Private Use, $300

POSTAGE AND FEES PAID
U.S. DEPARTMENT OF COMMERCE
COM-215