ABSTRACT

With the growing requirements for protection generated by legislation such as the 1974 Privacy Act, the increasing complexity of computer and data communications applications, and increasing awareness regarding computer vulnerabilities, the discipline of computer security is achieving independent recognition. Current data processing literature is a rich source of information. Articles and papers regarding security, design of software protection, operational practices and auditing number in the thousands. Most of them are very narrow in scope or so general that they are of little use.

It is important to the data processing professional to be able to sort out the large body of material in order to gain perspective. This paper attempts that by relying on a carefully selected and fully annotated bibliography of 134 items, many of them of interest to the systems analyst or designer. These papers are referenced in the text, which attempts to carefully distinguish between the technical and operational elements of computer security, while providing an overall perspective.

INTRODUCTION

The computer has unleashed countless opportunities for industrial growth, new applications, labor-saving accomplishments, and improvement of the quality of decisions. Most industrial and governmental organizations could not survive without the processing capability of their computer systems, and it can be shown that society itself is dependent upon the computer. At the same time, computer technology has spawned a whole new field of crime and has generated a series of problems for both designers and users of information systems.

With the growing pervasiveness of computers, their increasing complexity and the development of sophistication regarding computer vulnerabilities, the discipline of computer security is achieving widespread recognition. Many organizations have created the position of DP security specialist or manager and college courses in computer security are being taught. There are a number of driving forces behind the interest, some of which are outlined below.

Historical

In the middle 1960's, Congress began discussing the issues of privacy and the computer. A national data bank was proposed. Congressional committees were established, and public testimony published. The general consensus was that technology had not advanced to the point where privacy could be maintained.

Concern over the inherent lack of controls in computer systems led to much discussion and some activity on the technological front. A landmark meeting of active professionals in computer security in 1972 set the stage for an understanding of the technological issues and led to intensive design efforts to achieve "secure" computer systems.

In the meanwhile, activity on the legislative and social fronts saw a culmination in the Privacy Act of 1974 (Public Law 93-579). This act applied privacy requirements to most computer systems operating within the Federal Government. It also generated a number of papers regarding implementation requirements, and attempts to determine the true cost of privacy, especially as applied to large, multi-use data banks.

The need for computer security is also affected by technological factors. As systems become more complex and sophisticated, so do the problems of data integrity. Resource-sharing systems achieve their greatest advantage when used simultaneously by many customers. This also means simultaneous processing of data with varying needs for confidentiality and pervasive needs for accuracy. The problems of management control also have increased as the flexibility and capability of systems improve.

The scope and complexity of the field becomes apparent when a survey of the literature turns up over a thousand articles dealing with physical security of computer assets, threats to the computer, protection against fraud, embezzlement, and other human fail-
ings, the need for insurance, software protection, hardware safeguards, legal considerations, risk assessment, auditing, computer system design and the principles of operating system software security.\textsuperscript{1,11,107} A multi-disciplinary approach is needed.\textsuperscript{90}

**Definitions**

Computer security is a widely discussed subject, and a generally agreed definition refers to it as protection of data against accidental or intentional disclosure, destruction or modification. Security can be viewed as a problem of “comprehensive control,” involving the development of means to insure that privacy decisions are enforced.\textsuperscript{97}

Data confidentiality is “the status accorded to data which requires the protection from unauthorized disclosure.”\textsuperscript{97} It refers to the protection of data from unauthorized disclosure, whether the basis for such protection is agreement, law, policy or prudent judgment.\textsuperscript{109}

Privacy is a legal and social concept, having roots in constitutional law and social justice requirements.\textsuperscript{6,132} It refers to the right of an individual to control the collection, storing and dissemination of data about himself.\textsuperscript{6}

Data integrity is the protection of data against accidental or intentional destruction or modification. It also is the ensuring of accuracy and completeness of data. It involves the need for all components to operate together in a consistent and reliable manner.\textsuperscript{93}

It can be seen that the object is data. We have been discussing data security as contrasted with computer security. To include the broader-based definition of the subject, and the need to think of the other assets involved such as computer hardware, facilities and people, the term ‘processing integrity’ has been coined.\textsuperscript{105} It is the property of having adequate processing capability, availability and reliability in order to provide the requisite services of data processing.

**PLANNING FOR COMPUTER SECURITY**

**Threats and vulnerabilities**

The result of a security breach is what usually draws attention to a threat, a vulnerability or a particular countermeasure. The short history of computer security is spotted with numerous “horrible examples,” fads such as the interest in magnets as a threat, the implementations of security measures that are anything but cost-effective.\textsuperscript{10,101,131} A rational approach to the subject implies some sort of quantification of risks, and an analysis of the costs and benefits of countermeasures. Although some articles and papers have called for this approach,\textsuperscript{23,30} only recently has there been a serious attempt to model the risk-cost interface.\textsuperscript{20,40,79,87}

One of the key steps in devising protection is the classification of various threats. There are two sources of threats, people and natural hazards.\textsuperscript{25} It is possible, though not easy, to quantify the threat of fire, earthquake, flood and storm.\textsuperscript{19} On the other hand, those events that arise from human acts such as mistakes, disgruntlement, fraud and sabotage are not always possible to quantify, namely because of the complexity of motivations, environmental considerations and the effect of in-place countermeasures imposed.\textsuperscript{100} The first step is to organize and classify the threats in a systematic manner.\textsuperscript{97} Threats are usually part of the environment. On the other hand, the vulnerabilities of a particular computer system to those threats are dependent on a large number of factors relating to location, people, capabilities of the system, building structure, nature of the processing and operating practices.\textsuperscript{123} Most security surveys and evaluations are designed to review these installation dependent vulnerabilities and postulate countermeasures accordingly.\textsuperscript{91,109}

Adequate cost-effective protection against data security threats is uncommon. Usually the implementation of computer security is given low priority. It has suffered from inadequate attention and analysis, with too many existing measures lacking flexibility, consistency, completeness and redundancy. These attributes are all necessary in order to achieve protection that works when it is supposed to. One-hundred percent security or reliability is never possible. What is needed is a set of security measures that take into account the failures, errors, omissions and vulnerabilities of any given environment.\textsuperscript{23,104}

**Risk analysis**

Risk analysis is the term applied to the systematic quantification of threats, loss exposures and countermeasure benefits.\textsuperscript{26} The ingredients of a risk analysis are the postulation of threats and their probability, the calculation of loss exposures, including degraded productivity, usually on an annualized basis. It is important not to ignore the very low probability, high loss events that occur so infrequently that the annual loss potential appears negligible. A high loss exposure, regardless of the probability, should be evaluated carefully. In any event, the apparent simplicity is misleading. It is not easy to quantify all the potential losses, to postulate all the threats or to estimate their probability. It is also a complex and time-consuming task, which accounts for the relatively few completed risk analyses to date.

**OPERATIONAL COMPUTER SECURITY**

Computer systems are generally not designed with security as a primary objective.\textsuperscript{99} Generally, the large main-frame manufacturers claim that users have been
slow to request security. Current research effort by independent sources and manufacturers alike indicate that the next generation of computers will achieve adequate, measurable and certifiable protection in hardware and software.111

Much protection for computer systems can be implemented outside of the computer hardware and system software. Managers of computer installations have always been concerned with the problems of system integrity, processing availability and security. For them, physical security, backup and administrative controls are highly relevant.

**Physical security**

Physical security has been subjected to study and implementation long before the arrival of computers. Implementation of physical access controls to computer facilities represents a generally agreed first step in achieving threat protection. The reason is that many threats, especially of a human nature, can be reduced by limiting access.26,111 To deal with the threat of fire, utility unreliability and environmental disturbances, numerous control and monitoring systems have been devised. All should be considered in the context of the overall DP security plan, even though responsibility for their implementation may be elsewhere in the organization.

**Backup and recovery**

Recovery planning to ease the pain if a disaster were to strike is important.28 The objective is to assess the capability of the organization to respond immediately, and ensure that supplies, data files, programs, documentation and equipment are available off-site. The contingency planning must be of sufficient detail so that in case of disaster, all the elements can be pulled together in order to resume operations in as short a time as possible.117

**Administrative controls**

The administrative burden of proceduralizing and formalizing a security program is generally underestimated. It takes great clerical resources to ensure adequate maintenance of a selective access program, whether it be selective authorization to data files or physical areas. Other administrative aspects include the development and implementation of security policies, guidelines, standards and procedures. Again, these functions may be centralized or decentralized, but stand a greater chance of success if the latter.29

Security in recent years has been a major concern of computer operations groups. It is here that the organization can channel resources most effectively to deal with the lack of security in operating systems or in application system design. It is a necessary but not sufficient condition for providing true computer security.21 One of the best guides for information about secure operating practices is the System Review Manual on Security, published by AFIPS.112 Other guidance can be found in the more exhaustive of the many checklists and guidebooks on computer security.114,117,119,121,122

**Audit**

Audit has been defined as “an independent and objective examination of the information system and its use (including organizational responsibilities) into:

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

... the adequacy and effectiveness of system controls versus dishonesty, inefficiency and security vulnerabilities.”24

Independent and objective are the key words. Whether or not an auditor’s objective is the detection of fraud in computer systems, his role is certainly one of reviewing the adequacy of system security. Many CPA firms have finally recognized their unique role in security assurance.133,116 Some critics say their attention is still inadequate and not yet relevant.119 Suffice to say that computer systems need auditing, both internal and external. It is not possible to even consider auditing “around the computer” because of the risks involved. Given the nature of computer related threats and vulnerabilities, the traditional independence and inquisitiveness of the audit profession and the requirement for independent assessment of controls, it is logical that much computer security activity will be a part of the auditor’s domain.23

**TECHNICAL ELEMENTS**

Even though the first line of defense is to rely on secure operational practices and physical security, the elements of system design have always intrigued computer security professionals. Obviously things can go wrong with hardware and software. Data integrity, encryption and security surveillance must be considered in any complete computer security program. Understanding of these elements usually requires a person well-versed in systems programming and application system design. That the skills required in this area are completely different (and perhaps incompatible) with the skills required for handling operational security problems has not been well identified in the literature. In addition, no present commercially available operating system is immune from penetration, and so the prevalent attitude is that it is futile to
attempt to provide protection against the determined technical penetrator. However, much research and vendor effort is being devoted to the appropriate technical safeguards in operating systems.11

**Identification**

Positive identification of people, devices, programs, systems and processes is clearly a requirement for adequate security. Holding a person accountable for his actions is one of the first principles in good design. This requires certain knowledge that he is who he says he is. There are three approaches to personal identification, (1) identification based on passwords (2) on credit card technology and (3) on personal characteristics of the requestor. Passwords are the most common method, but they suffer from some serious inadequacies.6 They should be random in nature and of sufficient length to avoid compromise.5 The use of credit cards, usually with a magnetically encoded stripe, is achieving great popularity, especially in regard to Electronic Funds Transfer Systems. This approach makes sense if the cards are controlled, used in conjunction with a unique personal identifier (PIN number) and if the system is made aware of lost cards so that casual retrieval of a card will not be an open invitation to access. Identification based on personal characteristics, such as voiceprint or fingerprints is still not a commercially popular methodology, but offers future promise.48 Identification not only relates to personnel access, but also to other system entities. Security objects can be people, terminals groups of people (cliques), programs, terminals, data communications devices or segments of virtual memory.49 Then one can specify restrictions based on a number of parameters such as the characteristics of the requestor (name, terminal, program, etc.) content of data (all salaries over $30,000), context of data (association of college grades, number of parking tickets and credit rating) or one can use procedures (formularies) based on the nature of the situation.47

**Authorization**

Once a system resource or person is identified, the problem of access of the identified subject becomes an important concern. Authorization refers to the establishment of allowable interactions among system elements.15,29 The traditional concept of authorization in system design presupposes that any system entity automatically is authorized access to any other system entity unless specifically prohibited. The secure concept of system design takes the opposite view. The concept of "least privilege" holds; namely that any system entity is prohibited access to another system entity unless specifically authorized. For example, there is no need for a peripheral allocator to be able to control or even have access to user data bases or other elements of the operating system. It should have knowledge of only those resources necessary for allocation of devices to jobs.11

The concept of an access matrix espoused by Conway, et al10 appears to be the easiest way to implement access control, but the implementation is not clean.59 There are a number of choices that one can make in defining the rules of access. For example, what level or degree of privilege should be permitted? Are we talking about control of access to files, records, elements within records or specific hardware or software elements of the computer system?72

Much of the early work in authorization technology is the result of research activities.23,26,31 The academic environment has fostered some good studies53,56 which have led to some actual efforts at implementation. Work at MITRE and the US Air Force on security kernels (provably small security reference monitors)84 at Stanford Research Institute on proofs of program correctness,31 at System Development Corporation for the DOD community,126 at MIT Under Project MAC112 and at computer system manufacturers,12,34 has led to actual demonstration of computer and communications systems with security as a prime design requirement. An excellent but dated paper by Saltzer summarizes current (as of early 1975) research and development efforts.111

**Integrity**

Obviously, things can go wrong with hardware and software. Data can be (and frequently is) inconsistent or unreliable. Data integrity interfaces with computer security at almost every point. In fact, many observers see the two concepts as being nearly synonymous.103 A high integrity operating system can by its nature provide security against unauthorized use of system resources. System integrity is the condition of proper and predictable operation of the total system, including hardware, software and human elements. It includes the physical and operational security mechanisms in place.

Part of the integrity solution lies in providing an operating system that does not treat every operation as "benevolent," but in fact assumes that users are going to attempt to get into supervisor state, and are going to overreach the limits of the software design. Other corrective elements can be found in attempts to enhance the reliability and availability of applications.105

**System audit trails**

System surveillance, measurement and auditing are critical elements in providing the technical base for adequate security and integrity. The effectiveness and operability of the entire system, especially the protec-
tion mechanisms, must be continually scrutinized and measured. Management must be assured that the protection is in place and effective. Management must also be able to detect and respond to events that constitute system security threats. Many of the same mechanisms used for performance measurement also can be used for monitoring of the protection mechanisms and the integrity of the entire system. A properly functioning audit mechanism should allow the specification of certain system events (such as OPEN, LOGON, etc.) to trigger an audit trail. The interfacing of system measurement and surveillance activity with the auditor is the subject of much activity and research.119

CONCLUSION

As of early 1976, systems are in use which provide a high degree of computer security and integrity, and may provide the basis for systems accreditation. The MULTICS project at MIT has led to commercial marketing of the system by Honeywell and a multi-level security enhancement by MITRE and the USAF.112 The General Electric Mark III® Service has long been known for its good security. Other operating systems have been designed with security as an objective,12,52,60,91,100,112 and the efforts of IBM and Honeywell have been previously mentioned. Current research directions are outlined in the paper by Saltzer111 and should see commercial reality sometime in the next few years. Awareness of the risks is being fostered by numerous seminars and conferences. Large organizations, both commercial and government, are funding the position of systems security officer or computer security manager. An association, the Computer Security Institute, has been formed to provide information to, and give voice to the growing number of specialists in the field.

Current state of the art would seem to allow quite flexible and cost-effective security measures. But in practice, protection is generally not elaborate, flexible or impenetrable.32 As a result, most safeguards are imposed “after the fact”, through a mixture of managerial controls and physical security. This type of control is largely ineffective, due to inconsistencies, lack of proper redundancy or incompleteness. It appears that this will be the case, even after computer systems come provided with flexible and effective protection mechanisms.

In 1969, Lance Hoffman said that much research is needed to design security controls and to evaluate computer access control methods.33 Nothing has changed to alter this. When designers and implementors agree on the needs, and the computer and software providers supply the secure methods to use their products, it is still up to the user to provide the proper environment, the procedures and the management climate to implement the principles of “least privilege,” compartmentalization, redundancy in controls and personnel awareness that are the necessary first step in provision of security, privacy protection and system integrity. Only then, shall we realize the goals of simple, economic, functionally capable and modular protection mechanisms.114

In conclusion, it is important to realize that we are talking about a complex technology, with many interfaces.114 Because of the great need, the next few years should see a continued broadening of interest, the forcing of computer security protection because of privacy legislation, awareness of the economic consequences of security deficiencies, increased risk management efforts by computer system implementors and increasing government regulation of the data processing industry.

COMPUTER SECURITY BIBLIOGRAPHY

3. Allen, Brandt, “Embezzler’s Guide to the Computer,” Harvard Business Review, July-August, 1975. The author talks directly to the would-be embezzler and cautions him not to be concerned about getting caught. The real big embezzlement schemes are still working and the perpetrators are not being caught. Shows how to defraud through manipulation of payroll, accounts payables, inventory, shipping documents and accounts receivable records that are maintained in computers.
4. AICPA, Audits of Service-Center Produced Records, American Institute of Certified Public Accountants, Auditing Standards Division, New York, 1974. This is a guide for Certified Public Accountants for their use in examining and reporting on the financial statements of clients whose records are produced by a computer service center or time-sharing firm. It is the basis for third-party audit reviews of such firms, and is oriented toward security and controls.


10. Bergart, J. F. and Marvin Denicoff and David K. Hsiao, "Legal and Security Issues Posed by the Privacy Act of 1974," Proceedings: Fourth Data Communications Conference, Quebec City, Canada, October 1975, IEEE, New York. Encryption can be an effective process for protecting data during transmission. The degree of protection depends on the encryption algorithm, the implementation of the algorithm, and the associated administrative procedures. Additional security requirements of user identification, access authorization and auditing may be satisfied by combining encryption technology with a network access control machine (computer). This paper presents the proposed Federal encryption standard and the security requirements satisfied by proper use of the algorithm. It also discusses implementation.

11. Bigelow, Robert P., "The Privacy Act of 1974," The Encyclopedia of Information Systems, Vol. 1, 1965. A classic study that predates much of the efforts around spheres of control. It discusses a unified view of data base recovery mechanisms, the removal of access controls from the host computer, and the placing of a mini-computer-based access control system at the peripheral interfaces. This is a logical extension of the hypervisor, or virtual machine monitor. It is one solution to problems of security in fourth generation computer architecture.

12. Bisbey, Richard L. and Gerald J. Popek, "Encapsulation: An Approach to Operating System Security," Proceedings, 1972 ACM Conference, San Diego, California, also, AD-771-758, October 1973, ARPA. Encapsulation is the removal of access controls from the host computer, and the placing of a mini-computer-based access control system at the peripheral interfaces. This is a logical extension of the hypervisor, or virtual machine monitor. It is one solution to problems of security in fourth generation computer architecture.

13. Bingham, H. W., Security Techniques for EDP of Multi-Level Classified Information, RAD-TC-66-415, December 1, 1966. A classic study that predates much of the efforts in authorization technology. This was a study of military intelligence security control techniques for the Burroughs D8255. Hardware and software techniques currently under study are explained in great detail.


16. Brunsden, Dennis K. and Susan K. Reed (editors), Controlled Accessibility Workshop Report, US Department of Commerce, National Bureau of Standards, NBS Technical Note 827, May 1974. Presents the results of a three day workshop in San Diego, sponsored by NBS and ACM. About 75 computer security professionals were invited, and discussed at length the technical and managerial issues of protection in computer systems. The results are significant, because much developmental work since then can be traced to the workshop.

17. Branstad, Dennis K., "Encryption Protection in Computer Data Communications," Proceedings: Fourth Data Communications Conference, Quebec City, Canada, October 1975, IEEE, New York. Encryption can be an effective process for protecting data during transmission. The degree of protection depends on the encryption algorithm, the implementation of the algorithm, and the associated administrative procedures. Additional security requirements of user identification, access authorization and auditing may be satisfied by combining encryption technology with a network access control machine (computer). This paper presents the proposed Federal encryption standard and the security requirements satisfied by proper use of the algorithm. It also discusses implementation.


19. Browne, Peter S., "Computer Security—A Survey," Data Base, Quarterly Publication of ACM Special Interest Group on Business Data Processing, Fall 1972. An annotated bibliography of over 100 items presents the 'state of the art' as of 1972. It makes reference to some little publicized material, and shows the importance of then classified Department of Defense activity in the field.

20. Browne, Peter S. and Dennis D. Steinauer, A Model for Access Control, 1971 ACM/SIGFIDET Workshop on Data Description, Access and Control, San Diego, Nov. 11-12, 1971. Authorization is discussed from the standpoint of requirements for access to given objects. A conceptual model, based on the work of Weissman is developed.


data processing, are each a concise yet complete exposition of current thinking on each topic.

   Motion, November 1973. Scrambling devices, file access 
   validation and subversion tests are all part of a security 
   environment. The author discusses his measurement efforts 
   at the Defense Intelligence Agency regarding the overhead 
   of these mechanisms.

33. Clements, Don and Lance J. Hoffman, Computer Assisted 
   System Designs, Electronics Research Laboratory, College 
   of Engineering, Univ. of California, Berkeley, CA, ERL- 
   M408, November 1974. Describes a computer software 
   package that partially automates the selection of security 
   techniques applicable to a particular system design.

34. Computer Security Research Group, Computer Security 
   Handbook, Computer Security Research Group, Douglas B. 
   Hoyt, Chairman, Macmillan and Company, Inc., New York, 
   October 1973. Provides detailed information on manage- 
   ment's role in the accountability and reporting, hardware/ 
   software controls, computer risk insurance, auditing com- 
   puterized systems and outside contract services. The Com- 
   puter Research Group was sponsored by the Atlantic and 
   New Jersey Chapters of Association for Systems Manage- 
   ment. Authors are Arthur Hutt, Belden Menkus, Eugene 
   Redmond, Seymour Bosworth, Ralph Jones, Herbert Dick- 
   son, Robert Daley, Dick Brandon, Joseph Wasserman, 
   Theodore Christianson, Guy Migliaccio and Stephen Falh.

35. Conn, Richard W. and Richard H. Yamanoto, A Model 
   Highlighting the Security of Operating Systems, RISOS 
   Project, Lawrence Livermore Laboratory, Proceedings, 
   ACM 1974 Conference, San Diego, CA. Penetration of 
   computer systems has led several authors to identify 
   generic weaknesses in operating systems, but have not led 
   to formal methods of analysis. An approach showing 
   promise in identifying trouble spots, as well as charac- 
   terizing existing operating systems in a more general 
   sense, lies in forming graph models in which nodes are 
   program modules or data structures, and arcs are access 
   or shared resource synchronization paths. A given system 
   should be capable of reduction to a graph of this sort by 
   appropriate analysis of its load modules.

   Measures In Information Systems,” Communications of the 
   ACM, Vol. 15, No. 4, April 1972. Excellent presentation 
   of those concepts that are germane to authorization and 
   efficiency. All authorization does not have to be accom- 
   plished at run-time. To the extent that privacy is data 
   independent, the access function is inexpensive to imple- 
   ment.

37. Conway, R. W., W. L. Maxwell, and H. L. Morgan, “Selec- 
   tive Security Capabilities in ASAP—A File Management 
   System,” 1972 Spring Joint Computer Conference, p. 1151, 
   May 1972. Shows implementation of principles described 
   in the previous article.

38. Cotton, Ira W. and Paul Meissner, “Approaches to Con- 
   trolling Personal Access to Computer Terminals,” Pro- 
   ceedings of the 1975 Symposium, Computer Networks, 
   Trends and Applications, National Bureau of Standards 
   Institute for Computer Science and Technology. Considers 
   a number of approaches to protection against unauthorized 
   access to computers. Surveys the current state of the art 
   of personal identification. Explains how devices can be 
   compared, and introduces criteria that can be used in 
   personal identification system evaluation and/or compari- 
   son.

39. Courtney, Robert H. Jr., Forty Commonly Found Deficien- 
   cies in the Security of Data Processing Activities, IBM, 
   June 1971. A common sense primer to management, out- 
   lining frequently overlooked security deficiencies.

40. Courtney Robert H., Jr., Security Risk Assessment in 
   Electronic Data Processing Systems. National Bureau of 
   Standards, Task Group 15, October 1975. An approach 
   toward determination of risk to data processing is postu- 
   lated. It shows how to quantify the potential benefits 
   afforded by given security protection for comparison with 
   costs.

41. Davies, C. T., Jr., A Recovery/Integrity Architecture for 
   a Data System, IBM, Systems Development Division, May 
   1972. Discusses concepts of integrity as related to operat- 
   ing system and data base architecture.

42. Dean, Albert L., Jr., “Data Privacy and Integrity Require- 
   ments for On-Line Data Management Systems,” 1971 
   ACM-SIGFIDET Workshop on Data Description, Access 
   and Control, Nov. 1971, San Diego, CA. Identifies security 
   requirements for an on-line data base management sys- 
   tem. Concepts were implemented in work by the author 
   for the US government.

43. Denning, Peter J. (Chairman), An Undergraduate Course 
   on Operating Systems Principles (Module 6-Protection), 
   Interim Report of the COSINE Committee of the National 
   Academy of Engineering (Commission on Education), June 
   1971. Embodies the principles of protection as discussed 
   in the paper by Graham and Denning.

44. Department of Defense, ADP Security Manual: Techni- 
   ques and Procedures for Implementing, Deactivating, 
   Testing and Evaluating Secure Resource-Sharing ADP 
   Systems; also see Industrial Security Manual for Safe- 
   guarding Classified Information, DOD 5200.28M, January 
   1973 and DOD 5220.22M, April 1970, order from Super- 
   intendent of Documents, US Government Printing Office, 
   Washington, DC 20402. These two manuals provide very 
   helpful guidance for non-DOD government and commercial 
   organisations in defining and implementing physical and 
   data processing security programs. Even though the con- 
   cepts of the DOD classification of information hierarchy 
   are pervasive, the methods, ideas and procedures are 
   valuable in any environment.

45. Chadwick, H. A., “Burning Down the Data Center,” Data 
   Motion, Vol. 21, #10, October 1975, pp. 60-64. A well 
   written article that discusses DP insurance from the point 
   of view of the data processing expert. Complex insurance 
   related terms and concepts are clearly explained. Guidance 
   is given as to what insurance coverage is needed, why 
   various forms should be considered and who can provide 
   insurance services to DP installers.

46. Enger, I. Sador, Guy T. Merriman and Ann L. Bussey, 
   Automatic Security Classification Study, RADC TR 67-472, 
   October 1967. Report of an investigation of the feasibility 
   of using computers to assign the government security clas- 
   sification to textual material. The “correctness” was only 
   54% but the techniques used did show promise for further 
   research.

47. Federal Fire Council, Recommended Practices No. 1—Fire 
   Clearinghouse for Federal Scientific and Technical infor- 
   mation. Discusses practices in dealing with the threat of 
   fire. Is the most thorough and concrete guidance to date.

48. Feistel, H., Cryptographic Coding for Data Bank Privacy, 
   IBM Research Report, RC-2827, March 1970, also in Scien- 
   tific American as “Cryptology and Computer Privacy,” May 
   1975. Discusses concepts of cryptography that eventually 
   led to the development of an IBM pilot project and the 
   Federal encryption standard.

49. Fenwick, William A., “Marketing EDP Services: Review- 
   ing the Legal Considerations,” Computers and Automation, 
   November 1971. A nissembler. The author is really talking 
   about security measures to protect the confidentiality of 
   data.

50. FIPS PUB-39 Glossary of Terminology for Computer Sys- 
   tems Security) Federal Information Processing Standards

From the collection of the Computer History Museum (www.computerhistory.org)
Task Group 15: Computer Systems Security, National Bureau of Standards, US Department of Commerce, Washington, DC, September, 1975. A glossary of 70 terms relating solely to the concepts of privacy and computer security. The terms were extracted from many sources and reused through the joint efforts of FIPS Task Group 15, which was established in 1975 to develop standards and guidelines in computer systems security. Emphasis is on technical terms that relate to computer security architecture and communications security.


54. Givensky, M. B., "Cryptography, the Computer, and Data Privacy," Computers and Automation, April 1972. Also see Data Privacy: Cryptology and the Computer at IBM Research, IBM Research Reports, Vol. 7, #4, 1971. An interesting study on what researchers are doing to devise 'unbreakable' codes and how many classical approaches to encryption are easily compromised. The paper discusses "Lucifer," a hardware encryption device.


60. GUIDE SHARE, Data Base Management System Requirements, Joint GUIDE-SHARE Data Base Requirements Group, November 11, 1970. An important document that outlines idealized requirements for data base management.


that itself is the authorization mechanism for other system components.


89. Menkus, Belden, “Computer Security Needs a Common Sense Approach,” Administrative Management, March 1973. Discusses two aspects of comprehensive physical security. The first step is to build security into the facility by making it inconspicuous, installing access controls, and providing basic environmental support. The second step is to ensure integrity of processing through controls over input and file access, and ensuring good facility operating procedures.

90. MITRE Corporation, The Privacy Mandate—Planning for Action, National Bureau of Standards and MITRE Corp. Washington DC, August 1976. A summary of a workshop sponsored by the publishing organizations to develop recommendations for action in implementing privacy legislation. Four working panels covered the issues of individual privacy rights, institutional responsibilities, technological implications and the economics of privacy. Viewpoints of many interested organizations are also included. Unfortunately, the proceedings do not capture the depth of discussion that actually took place.


useful for the data processing risk manager. Discusses and quantifies risks due to floods, wind, fire, earthquakes, landslides, volcanoes, freezes and droughts.


109. Renninger, Clark R. and Dennis K. Branstad (editors), Government Looks at Privacy and Security in Computer Systems, US Department of Commerce, National Bureau of Standards, NBS Technical Note 509, February, 1974. Potential confrontations between society and technology over problems of individual privacy and data confidentiality can be defused by understanding and action. A conference on privacy and security was held at NBS, November 19 and 20, 1975. A number of speakers provided statements of governmental needs and problems. Also suggested was a broad range of activities for satisfying the needs.

110. Renninger, Clark R. (Editor), Approaches to Privacy and Security in Computer Systems, US Department of Commerce, National Bureau of Standards, NBS Special Publicsation 404, September, 1974. This publication summarizes and contains the proceedings of a conference held at NBS on March 4-5, 1974 to continue the dialog in search of ways to protect confidential information in computer systems. Proposals were presented for meeting governmental needs for safeguarding data confidentiality. Among the proposals were the enactment of privacy legislation, improved computer system architecture and access controls, information and security management guidelines and the development of systematic, balanced approaches to system security. A number of prominent computer, legal and social professionals presented their views as to potential solutions.


112. Saltzer, Jerome H., “Protection and the Control of Information Sharing in MULTICS,” Communications of the ACM, Vol. 17, #7, July 1974. Describes the protection mechanisms in the MULTICS system. These are some of the most advanced in current implementation.

113. Saltzer, Jerome H. and Michael D. Schroeder, “The Protection of Information in Computer Systems,” Proceedings of the IEEE, IEEE Computer Society, September 1975. A thorough discussion of the technical aspects of providing protection in computer systems. This is the most complete and most valuable discussion of the concepts of protection to date.

114. Schroeder, Michael D. and Jerome H. Saltzer, “A Hardware Architecture for Implementing Protection Rings,” Proceedings, 3rd Annual ACM Symposium on Operating Systems Principles, October 1971. Schroeder and Saltzer have designed hardware for use on the MULTICS system. It has found its eventual implementation on the Honeywell 6180. It allows efficient and flexible access authorization to be implemented partially in hardware.

115. Shannon, C. E., Communications Theory of Secrecy Systems, Bell Telephone System Technical Journal, October 1949, Vol. 28, #4, pp. 656-715. The theory of cryptography has not been significantly improved since this landmark, unclassified study was published.


118. Turn, Rein, Privacy and Security in Personal Information,
The Rand Corporation, Santa Monica, CA, R-1044-NSF, March 1974. This report presents the results of a National Science Foundation research study on theoretical and technical aspects of protection of personal information in databanks. The protection requirements and design of protection is the key focus. The investigation led to the establishment of classifications of systems and the sensitivity of personal information and the development of a protector-intruder model.

119. Turn, Rein, Remarks on the Instrumentation of Databank Systems For Data Security, The Rand Corporation, Santa Monica, CA, P-5151, January, 1974. This paper discusses the information requirements of an active security subsystem as well as auditing and threat monitoring. It explores ways of instrumenting a databank system for obtaining this information.

120. Turn, Rein and Norman Z. Shapiro, Privacy and Security in Databank Systems: Measures ofEffectiveness, Costs and Protector-Intruder Interactions, The Rand Corporation, Santa Monica, CA, P-4871, July 1972, also in Proceedings, Fall Joint Computer Conference, 1972, AFIPS Press, Montvale, NJ. Introduces a model that attempts to systematize the process of measuring the "malicious" penetrator of computer systems.


127. Weiss, Harold, "Computer Security: An Overview," Datamation, Vol. 20, #1, January 1974. Even though computer crime is increasing, fire, earthquakes and storms are postulated as the greater hazard to computer systems. Few installations have taken even the simple steps toward protection.


129. Weissman, Clark, System Security Analysis/Certification Methodology and Results, System Development Corporation, Santa Monica, CA, SP-3728, October 1973. Presents an approach toward system certification.


133. Winkler, Stanley and Lee Danner, "Data Security in the Computer Communication Environment," Computer, Volume 7, No. 23, February 1974, IEEE. Describes security concerns in multi-terminal computer systems. Useful as an introduction to the problems and the nature of network security. Describes a number of possible implementations of controlled access to data.

134. Yourdan, Edward, "Reliability of Real-Time Systems," Modern Data, January-June 1972. A six-part series that thoroughly explores data integrity and reliability. Covered are the different concepts of reliability, causes of system failure, examples of failure and approaches to error recovery.