DOCUMENT RESUME

ED 078 879 LI 004 414

AUTHOR	Bergart, Jeffrey G.; And Others
TITLE	An Annotated and Cross-Referenced Bibliography on Computer Security and Access Control in Computer Systems.
INSTITUTION	Ohio State Univ., Columbus. Computer and Information Science Research Center.
SPONS AGENCY	Office of Naval Research, Washington, D.C.
REPORT NO	OSU-CISRC-TR-72-12
PUB DATE	Nov 72
NOTE	61p.;(85 References)
EDRS PRICE	MF-$0.65 HC-$3.29
DESCRIPTORS	Annotated Bibliographies; Bibliographies; *Computer Oriented Programs; *Computers; Computer Science; Computer Storage Devices; *Confidentiality; *Confidential Records; Electronic Data Processing; *Security

ABSTRACT

This paper represents a careful study of published works on computer security and access control in computer systems. The study includes a selective annotated bibliography of some eighty-five important published results in the field and, based on these papers, analyzes the state of the art. In annotating these works, the authors try to be objective, indicating the strong as well as the weak points. In addition, they attempt to show how one piece of work is related to or influenced by another, since research works seldom evolve without interaction. Because a number of outstanding works on computer security and access control in computer systems are classified or unpublished, this collection is not exhaustive. The annotated material is organized into four sections of which the sections on computer security and access control in computer systems are emphasized. In addition, to provide some background and broad understanding of the issues of computer security, they have included several bibliographies, some articles on the business and management overview, and several works on social and legal implications. (A related document is LI004415.) (Author/DH)

(OSU-CISRC-TR-72-12)

AN ANNOTATED AND CROSS-REFERENCED BIBLIOGRAPHY ON COMPUTER SECURITY AND ACCESS CONTROL IN COMPUTER SYSTEMS

by

Jeffrey G. Bergart, Marvin Denicoff,
and David K. Hsiao

Work performed under Contract N00014-72-C-0391,

Office of Naval Research

The Computer and Information Science Research Center
The Ohio State University
Columbus, Ohio 43210

November 1972

PREFACE

This work reported herein was, in part, supported by the Office of Naval Research under Contract N00014-72-C-0391. Reproduction of this report, in whole or in part, is permitted for any purpose of the United States Government.

This report consists of annotations of the published work on computer security and access control in computer systems. The work was performed by Jeffrey G. Bergart, The Moore School of Electrical Engineering, and the Graduate Division of The Wharton School of Business and Finance, University of Pennsylvania; Marvin Denicoff, Information Systems Program, Office of Naval Research; and David K. Hsiao, Department of Computer and Information Science and Instruction and Research Computer Center, The Ohio State University.

It is published by The Computer and Information Science Research Center of The Ohio State University which is an interdisciplinary research organization consisting of the staff, graduate students, and faculty of many University departments and laboratories.

Table of Contents

I. INTRODUCTION

This paper represents a careful study of published works on computer security and access control in computer systems. The study includes a selective annotated bibliography of some eighty-five important published results in the field and, based on these papers, analyzes the state of the art. In annotating these works, we try to be objective, indicating their strong as well as their weak points. In addition, we attempt to show how one piece of work is related to or influenced by another, since research works seldom evolve without interaction.

Because a number of outstanding works on computer security and access control in computer systems are classified or unpublished, this collection is by no means exhaustive. Furthermore, since the authors are themselves involved with work in this field, it is not without their personal views.

The annotated material is organized into four sections of which the sections on computer security and access control in computer systems are emphasized. In addition, to provide some background and broad understanding of the issue of computer security, we have included several bibliographies, some articles on the business and management overview, and several works on social and legal implications.

The subject of privacy protection and access control in computer systems is concerned with effective means to protect the anonymity of private information on the one hand, and to regulate the access to shareable information on the other hand. Effective means for privacy protection and access control can be considered on three levels: memory level, process level, and logical level.

At the memory level, protection mechanisms are those which regulate access to memory in terms of units of memory. The main point is that protection is of the containers, i.e., the memory units, not the contents. As a consequence, everything inside the container is subject to the same access control as the enclosure itself. Furthermore, the contents are safe only as long as they are kept in the same containers.

Typically, physical memory protection schemes employ memory bounds registers or storage protection "keys" which keep the users from venturing into memory areas. Other, more sophisticated, schemes are possible. The idea of having an m x m matrix of control bits to keep track of access rights

to m memory areas has been advanced by [Lampson 1967]. For example, an entry A_{ij} would determine the access rights to the i-th area from the j-th area. The A_{ij} may correspond to various access rights such as read-only, read/write, execute-only and privileged mode.

In general, one user's access rights to an area may differ considerably from another user's access rights to the same area. In a multi-programming and shared data base environment, the system must therefore provide, in real-time, different matrices for different users. The use of virtual memory may, therefore, enhance the implementation of the matrix scheme. Here, page and segment tables are consulted by the hardware at instruction decoding time. Each user has his own tables and therefore cannot get into a page of memory which does not have an entry in those tables. As a result, sophisticated schemes such as Lampson's matrix are more easily implemented with virtual memory. Yet, even in virtual memory, we note that the protected areas are again units of memory.

The second level of protection and control is called process protection and access control. A process is simply a set of (one or more) programs and their associated data. Thus, unlike memory protection, the notion of process protection and control is concerned with access to and protection of programs. To this end, we must develop mechanisms which can determine when and under what conditions programs can pass control from one to another. In other words, the mechanisms must be able to monitor the execution of programs in terms of their calls and returns.

Graham [Graham 1968] first proposed a concentric ring mechanism which allows one program to give control to another without violating any of the access control rights of either program, thereby safeguarding each program's working tables, data, intermediate results, etc. Graham's concentric rings can be implemented whether or not one has a virtual memory machine. Therefore, one should not indulge in a misconception that virtual memory protection and process protection are one and the same.

Conceptually, concentric rings may not be the only way to support a general process protection and access control requirements. It can be argued that the concentric ring mechanism forces the user to arrange his processes hierarchically, where processes at the lower part of the hierarchy (i.e., outer rings) have less privileged access rights. However, a cyclic process protection and control structure, for example, may be difficult to

realize in a hierarchy-based system. An interesting task is to investigate structures other than concentric rings and to determine their usefulness as process protection and control mechanisms.

The third level of protection and control is logical. We feel that, in a large data base environment, the user will first organize his data into some logical structure. He will then refer to his structured data in terms of logical entities such as arrays, strings, fields, records and files. The important point is that these entities are logical units of information which may have little resemblance to their physical storage images. By allowing the user to associate access control requirements and privacy protection measures with the logical units, the protection and control mechanism can facilitate direct control and protection of the information regardless of the whereabouts of that information. Furthermore, the mechanism does not require the user to be familiar with the physical storage structure of the computer system.

Hoffman's work was significant in the logical control area. He recognizied that the process of access control is divided into a linear collection of related procedures [Hoffman 1970a]. He felt that to obtain access control there must be a list of step-by-step actions which are necessary for complete protection. At each of these points, Hoffman allows the user to incorporate his own mechanisms (called Formularies) for protection. In this way, Hoffman suggested that the user will pay for only that amount of protection he desires. The more protection deemed necessary, the larger and more complicated will be the formularies; this in turn will cost more in core space and execution time.

In order to have any meaningful logical protection and control, the user must in some way be able to describe his data. We note that Hoffman's formulary approach requires that the user describe his data by complicated procedures and supply unique identifiers for his data.

The authors believe that logical access control and privacy protection mechanisms must have the facility for the user to describe his data structure, assign access rights and protection requirements to that data, and incorporate procedures for further authentication of other users of his data. Notable mechanisms which have this facility can be found in [Hsiao 1968; Manola 1971; Conway 1972; and Owens 1972]. Logical and process protection and control mechanisms are included in Section 2.3. For memory protection schemes the

reader should refer to Section 2.4.

Where do we go from here? One possibility is, for each level of protection, to try to determine which types of implementations are the best. Then we also must examine the basic problem of putting these levels of mechanisms together. Is the best total system available a hook-up of the best scheme from each level? Are there interrelationships between the levels of mechanisms which would make the merging of the best system at each level a less than superior total system? There is also the question of whether to start with memory and process protection hardware and associated software, and then build a logical control mechanism; or to use a top-down approach whereby we first define our data structure, choose a logical control scheme to handle it, and then find the machine which best suits our system.

Before we can provide the right answers to these questions, we should perhaps try to understand the work which has already been accomplished. A useful way to place these works into proper perspective would be to develop abstract models which can classify the significant aspects of these works. Furthermore, one hopes that these abstract models would show new ways to generalize the existing mechanisms and facilitate new designs and implementations. Significant works in modeling can be found in Section 2.2 of which Graham and Denning's attempt [Graham 1972] to model memory and process protection mechanisms, and Manola's effort [Manola 1972] to m the logical and process protection mechanisms are worth noting.

II. PRIVACY PROTECTION AND ACCESS CONTROL IN COMPUTER SYSTEMS

(1) General Discussion And Survey

Armer 68

Armer. P. Privacy Aspects of the Cashless and Checkless Society. Testimony before the Senate Subcommittee on Administrative Practice and Procedure. The RAND Corporation, Santa Monica, Calif. (April 1968) (P-3822, 19 pp.).

A conflict exists between personal privacy and society's right to know. Measures of diminishing privacy are: 1. Percent of transactions recorded, 2. Amount of detail, 3. Degree of centralization, and 4. The speed of transmission and retrieval. Computers have reduced privacy by 1. Reducing costs of data storage and retrieval, 2. Centralizing data, and 3. Allowing anonymity by supporting remote terminals.

The author is generally against a checkless, cashless society. He often refers to Westin's Privacy and Freedom [Westin 70]. An example of information retrieval via Boolean expression is given which can compromise an individual's privacy.

Bushkin 70

Bushkin, A.A. "A Technical Context for Multi-level Security in a Multiplexed Computer System." Seminar on Privacy: Legal and Technical Protection in the Computer Age, October, 1970, 12 pp.

The author describes the basic requirements for a secure system. Hardware requirements include a known response for all possible operation codes with all possible tags or modifiers whether legal or not, program readable hardware configuration status switches, and other more standard conditions. Software requirements include "Need-to-know" lists which are associated with each file. However, sub-file protection may be too expensive to implement and there is the danger of deducing TOP SECRET information from reading only SECRET reports. By using pure-procedures, one cuts down on "contamination" due to improper mixing of data of varying sensitivity levels. Lastly, Bushkin lists ten design guidelines for a monitor system.

Conway 72a

Conway, R. W.; Maxwell, W. L.; and Morgan, H. L. "On the Implementation of Security Measures in Information Systems." Comm. ACM, 15, 4 (April 1972).

The terms privacy and security are compared. A table is given with the outcome of each possible combination of privacy decision and security action.

		Privacy Decision	
Action of Security System	Access Obtained	Access Permitted Proper Access	Access Denied Successful Invasion
	Access Prevented	Improper Rebuff	Successful Defense

Access control is carried out by a matrix of decision-rule elements for each user-data item pair. Data dependent and independent decision rules are distinguished so that one may perform much of the checking only once at translation time rather than repeatedly at execution time. This important distinction is lacking in Hoffman's survey [Hoffman 69] and Petersen and Turn's paper [Petersen 67].

The "matrix" concept, however, is costly unless one can: 1. Reduce the matrix size by defining "virtual users". i.e., to aggregate identical security authorization or access rights, 2. Keep the entries in the matrix as simple as possible, i. e., to try for yes-no decisions, and 3. Carefully analyze when and how the matrix should interrogated, i.e., to separate data dependent from data independent decisions.

A functional model is described using F_t, S_t, F_r, S_r (for translation-time and run-time Fetch and Store functions). Hoffman's Formulary System [Hoffman 70a] is said to be wasteful since it always has calls to F_r and S_r even for data independent requests. MULTICS wastes time in much the same manner but its F_r and S_r are implemented in hardware; therefore the author

is less critical of that system.

To implement their system a library routine is needed to store, manage and protect the security matrix. Also, the I/O service routines would have to be modified to contain the F_r and S_r functions. F_t and S_t can be implemented either by modifying the standard compiler or by interposing a preprocessor in front of it. Some problems are: 1. Sometimes the programmer does not access the data by name (e.g., How do you protect against array subscripts going outside the declared bounds), 2. How does one protect against improper use of pointers in PL/1, and 3. Similarly, one must guard against passing of a data address as a parameter to a subroutine in which that data is not allowed.

Garrison 70

Garrison, W. A.; and Ramamoorthy, C. F. Privacy and Security in Data Banks. National Tech. Info. Service AD 718 406, 1970, 120 pp.

This is a survey of some of the systems or mechanisms which provide access control and privacy protection. Attempts are made to summarize them.

Considerations for a secure data bank are concentrated on the following: 1. Information classification in terms of transmission, manipulation and storage, 2. Validation of information, 3. File update and manipulation functions, 4. Access control and protection of information, and 5. Surveillance and threat monitoring. For information handling, various encrypting schemes are discussed, compared and summarized. On file functions and access control, discussions include read/write restrictions, boundary restrictions and processing restrictions. Two schemes using memory bounds as well as Graham's ring mechanism for processing control [Graham 68] are discussed. It was pointed out that Graham's method cannot be used in associative memories.

The authors talk about virtual addressing as a means of protection. This scheme does not allow the programmer to protect selected areas of memory, and requires much overhead to keep track of the constantly reshuffled programs.

The current status of several systems with access control capabilities

is discussed:

I. The Cambridge University File Protection System. When a file is created, its owner declares which of five prime activities each of four user classes will be allowed to use with the file. Thus, there exists a 4 x 5 matrix of 1 bit elements for each file. This system is advantageous in that it allows a precise and understandable mechanism for setting up access profiles for all users [Barron 67]. It is limited in that it is only effective at the file level.

II. The Berkeley Computer Corp. Model I System. The three essential concepts are: a. Objects are given unique unalterable names called capabilities and one must possess a capability in order to access its object, b. Capabilities are grouped into domains and capabilities change when control passes from one domain to another, c. Within each domain are special capabilities called access keys. These keys authorize the domain to grant capabilities within itself. This approach works better in an environment where the address space of one domain is a subset of another, e.g., Graham's [Graham 68] ring-like structures. For a price, protection can be at any level (down to the bit). When complex file structures overlap various domains, additional data has to be kept about each domain call and checks have to be made at every domain crossing. Thus, the scheme becomes complex and may complicate its effectiveness of the access control [Dennis 66 ; Lampson 69].

III. The Rush Time-Sharing System [Babcock 67].

IV. ADEPT-50 Time-Sharing System. This system uses software for protection. Four security objects are used (user, terminal, file and job). Each object is given a security profile triplet (Authority, Franchise or need-to-know, and Category (e.g., crypto)). This system enables a file owner to establish a security profile for the users of his file on the one hand, and can remember the security history of past files on the other hand. The designer notes its disadvantages as the amount of critical coding, dispersal of programs and data in memory which degrades confidence. Furthermore, the system needs to implement more security classifications and monitoring for later audits [Weissman 69].

Garrison and Ramamoorthy favor the capability list approach. It allows distribution of control and cost throughout the files whereas the Multics ring structure can quickly become expensive. Of course, any system which attaches capability lists to each file faces the problem of managing the control information. Thus, in such systems one needs to periodically purge inactive capability lists.

Directed grapns are mentioned as a possible means of looking at file structures. Connectivity and reachability matrices can help discover the nature of these file structures. But such work is not advisable unless the files are static and are not subject to frequent reorganization.

Hellman 70

Hellman, J. J. Privacy and Information Systems. The RAND Corporation, Santa Monica, Calif. (May 1970) (P-4298, 76 pp.).

One point made is the need to "Minimize Temptation to 'Break' the System". Thus, Hellman develops the equations

1. $C_V >> V_{IV}$

2. $V_{IO} >> C_p$

where C_V = cost of violating the system

C_p = cost of protecting the system

V_{IV} = value of information to the violator

V_{IO} = value of information to the owner

If either a prevention or an apprehension facility were 100% effective [i.e., $\frac{C_V}{V_{IV}} \rightarrow \infty$] then either one would be sufficient to protect the information. However, since this is not the case, a combination of the two is needed. Unfortunately, privacy mechanisms in computer systems are non-analytic. Only exhaustive enumeration allows us to design, implement and test these systems.

Hoffman 69

Hoffman, L. J. "Computers and Privacy: A Survey", Computing Surveys, 1, 2 (June 1969), 85-103.

This is an excellent survey of what has been done in the area of access control and privacy protection in computer systems prior to 1969. Most of the papers center on technological advances and limitations. It is noted that access control is necessary below the file level, and that Hsiao's [Hsiao 68] system is the first working one which does this.

The author emphasizes the concept of the authority item as advanced by Hsiao. However, in the implementation of the concept, he believes that Hsiao's system is too expensive in that there would be too many entries in authority items when most files in the system are shared. The excess is due to the current implementation where authorized rather than unauthorized file names are used in the authority items. Hsiao's concept does not preclude other implementation approaches. For example, in Manola's EDMF [Manola 71] the entries on an authority item may contain either authorized or unauthorized file names.

The author discusses various authentication mechanisms, one of which he later develops into "formularies" [Hoffman 70].

A useful annotated bibliography of sixty-nine entries is given.

Hoffman 70b

Hoffman, L. J.; and Miller, W. F. "Getting a Personal Dossier from a Statistical Data Bank." Datamation (May 1970), 74-75.

This short paper shows how one can easily obtain individual-specific information from a seemingly "aggregate-only" Data Bank. By proper selection of conjunctive terms in one's Boolean inquiries to the Data Bank and with a little a priori information, the authors show that extensive information about an individual can be obtained.

Weissman, C. "Programming Protection: What do you want to pay?", SDC Magazine, 10, 7 & 8 (combined), (July, August 1967), 30-31.

Protection is a trade-off between the cost C_p to build and maintain the privacy system and the cost C_b involved in "beating" the privacy system. If the cost relationship is $C_p << C_b$, one can say that the system has adequate protection. For even higher security (e.g., military top-secret), one can consider the replacement cost C_r for compromised information and then insist that $C_p << C_r << C_b$ holds. But this is too expensive for most privacy needs. The author suggests that an insurance policy against the costs of compromise would be more economical for private industry than the additional costs involved in satisfying the latter equation.

II. PRIVACY PROTECTION AND ACCESS CONTROL IN COMPUTER SYSTEMS

(2) Abstract Model And System Proposal

Bingham 65

Bingham, H. Security Techniques for EDP of Multilevel Classified Information. National Technical Information Service. (AD 476 557, October 1965) 195 pp.

The results of a Burroughs study to develop hardware and software protection techniques for their computers are presented.

Hardware protection techniques suggested include the use of flag bits for additional parity checking, instruction execution in execute-only mode, memory loading by memory bounds, jump or trap code, and security labeling of data. Additional techniques call for the detection of single addressing error and the ability to assign remote terminal numbers which have maximum code distance from each other.

Software protection techniques suggested include the use of special control tables, redundant programming, monitoring job execution and I/O operations, and logging of system activities.

An analysis of the cost of hardware protection, in terms of equivalent flip flops, and of software protection, in terms of additional instructions and executions, is given. The author argues that, for access control and privacy protection of a data base, checking the control code of a file against the user's control profile is preferred to checking the file-user list included in the file for the user. Hoffman points out in [Hoffman 70a] that the concept of user control profile is similar to the concept of the user-oriented authority item in [Hsiao 68].

Although it is somewhat out-of-date, this paper is highly recommended for reading.

Browne 71

Browne, P. and Steinauer, D. "A Model for Access Control." 1971 ACM-SIGFIDET Workshop on Data Description, Access and Control, 241-262.

The authors argue that neither the partition of data by compartmentalization [Friedman 70] nor the hierarchical classifications via MULTICS ring [Graham 68] offers a satisfactory solution to the access control problem. Their scheme is to generalize both approaches resulting in an abstract model.

In the model some programs may only be accessible through other programs - an access control problem, they maintain, which is difficult to enforce in ring [Graham 68 , Schroeder 71], or domain [Lampson 69] mechanisms.

Carroll 70a

Carroll, J. M. "Privacy and the Computer." Proceedings of the Conference on Interdisciplinary Research in Computer Science, Univ. of Manitoba, June 8-10, 1970, 27-74.

This paper represents a unique attempt at quantifying privacy.

A number of questionnaires (federal, provincial, local governments, insurance, finance companies, etc.) were evaluated as to the information content of various files. A privacy environment model was then proposed. The notions of absolute indeces for disclosure D, privacy values v_i, relative disclosure $d = D/D_{max}$ and relative privacy $p = 1-d$ were defined and used to produce "ground state" values.

Next, modes of privacy invasion (direct and indirect intrusion, violation of confidence, exchange of information, inadvertent disclosure and small sample disclosures were discussed and simulated by each of nine modifications to the file structure (create or destroy k files; add or delete k questions; merge or split k files; copy k files; exchange the contents of k pairs of files; and differentiate file access). For example, adding questions to a file is a form of direct privacy intrusion. The results are shown graphically for each modification and value of k.

The most interesting result is that "The idea that splitting up existing data banks into numerous low-density files can enhance privacy is a snare and delusion ... unless each of these low-density files is subject to regulation every bit as stringent as that imposed upon the original data bank". This statement is based on a debatable assumption in their model that the probability of disclosure of the i-th question of the j-th file is inversely proportional to the density of the file.

Daley 65

Daley, R C.; and Neumann, P.G. "A General-Purpose File System for Secondary Storage." Proc. AFIPS 1965 FJCC, 27, 213-229.

A general-purpose file system needs safeguards against: 1. Masquerading, 2. Accidents or maliciousness by authorized and unauthorized people, 3. Self-inflicted accidents, 4. Hardward and software failures, 5. Tampering with system safeguards themselves, and 6. Burdensome safeguards. A system is proposed to meet these requirements. The files are tagged with address, status, and access control information. As one goes down the file directory branches, there are access control lists at each node which specify one of 5 modes allowed (trap, write, read, execute and append). Features of this system include: 1. The inherent hierarchical structure of the file system, 2. Access control may be associated with a directory branch, 3. The backup and recovery procedures, and 4. Some hardware and software safeguards. (Summary grid of features vs. needs on p. 220.)

Dennis 66

Dennis, J. B.; and Van Horn, E. C. "Programming Semantics for Multi-programmed Computations." Comm.ACM, 9, 3, (March 1966), 143-155.

A few meta-instructions are defined for multi-programming systems. Several of them relate to the protection of information within "spheres" [Graham 68] specified by a "list of capabilities." Each capability points to a computing object, and indicates the actions that the computation may perform with respect to that object. Types of capabilities include segment restrictions, access indicators (e.g., execute only, write only, etc.), ownership, etc.

This is a rather detailed paper on the semantics of the "spheres of protection" scheme. Hoffman [Hoffman 69] feels that the capability lists may be too large, and that instead, programs should be used which can set up the lists dynamically when needed. Further, Hoffman suggests that capabilities be related to a smaller unit than a segment although segments may vary in size.

Friedman 70

Friedman, T. "The Authorization Problem In Shared Files." IBM Systems Journal, 9, 4 (1970), 248-280.

The author discusses the general nature of the authorization problem. Authorization is considered to be a mapping function of users' access rights to protected data. For implementing the authorization function on computer systems, the author suggests five guidelines: isolation of the authorization mechanism, access limitation, adjacent tagging, single-tag rule, and compartmentalization.

We note that the adjacent tagging of a protected field makes it necessary for the system to retrieve not just the tag, but also the field in question before the system knows if the field can be accessed by the user since the tag is stored adjacent to its field. Thus, checking and updating the tags also involve the movement of the tagged data which tend to compromise the data. The issue is whether the access control information should be stored alongside of the data. Hoffman [Hoffman 70a], Hsiao [Hsiao 68], and Manola [Manola 71] believe that control information about the data should be separated from the data itself.

The author points out that both adjacent tag and single-tag rule may be very sensitive to the file structure and record organization. The issue here is whether the structural information about the data should be separated from the raw data. If so, then control information can be associated with the structural information of data. Restructuring of data requires the processing of structural information and its associated control information; however, there is no need of reprocessing the raw data. (See[Hsiao 71] and [Manola 71]).

The author calls for a partitioning of the data into discrete compartments such that each protected item is assigned to one and only one compartment. Compartmentalization is independent of the rigid hierarchical structure of military classifications. Rather, it seeks to allow groups of data to be released to cliques of users on a need-to-know basis. This technique is acknowledged to be similar to Hsiao's [Hsiao 68], but the author incorrectly assumes that Hsiao's technique does not treat sub-file records.

The author proceeds to give a hypothetical model with a matrix of profiles listing data group access privileges for each user in its primary directory. The main drawback to this model is that protection information is stored with the data.

Graham 68

Graham, R. M. "Protection in an Information Processing Utility." Comm. ACM, 11, 5 (May 1968), 365-369.

Protection assures integrity of common user data bases and aids in debugging by limiting the propagation of errors. Mode switches are all-or-nothing solutions to protection. The author calls for various access privileges on the logical segment level, thus permitting different access rights by different users to the same physical segment. Further, he wants to isolate one process from another. An abstract model of his system of concentric rings of protection is proposed. This is implemented in the MULTICS [Glaser 67].

Our observations are given as follows: First, procedure arguments passed to any subroutine in an inner ring must be validated (i.e., access restrictions on all addresses must be checked). This assumes that the validation routine can distinguish between addresses and data. Secondly, checks at each gate (i.e., the crossing from an outer ring to an inner one) may be redundant. Thirdly, since a procedure in an outer ring may not have access to parameters in an inner ring, the parameters are duplicated and passed from the inner ring to the outer ring. This cost is high. Further, since segments are good for large data aggregates, the use of the ring mechanism on segments may be wasteful to protect smaller areas. And lastly, the concentric ring mechanism can facilitate protection where procedure's access control requirements are structured hierarchically. For cases where requirements are, for example, cyclic, there is difficulty in using this mechanism.

Graham 72

Graham, G. S.; and Denning, P. "Protection-Principles and Practice." Proc. AFIPS 1972 SJCC, 40, 417-429.

An abstract model of a protection system is developed which allows "cooperation of mutually suspicious subsystems." This model attempts to generalize the notions developed by Lampson [Lampson 69], Dennis [Dennis 66] and others. The authors state that an important property of their model is that every attempted access by a subject to an object is validated. However, according to Conway [Conway 72], some degree of preprocessing of access requests would cut down on this overhead.

Eight rules are presented for system commands which need to modify the "access matrix." The interesting notions of "copy flag", "limited-use attributes", "transfer-only copy flag", and "indirect attributes" are especially worth noting.

In this model, the owner of an object can revoke the access rights of others to that object, as is done in Lampson's model [Lampson 69]. This is in contrast to Vanderbilt's model [Vanderbilt 69] in which a "contract" exists between the owner and those whose access has been granted. Revocation of others' access rights constitutes a breach of the contract.

Hsiao 69

Hsiao, D. K. "Access Control in an On-Line File System." File Organization: Selected Papers from FILE 68 - An I.A.G. Conference. Swets and Zeitlinger N.V., Amsterdam, 1969, 246-257.

The author briefly describes the working access control mechanism for the Moore School's Problem Solving Facility (PSF). The mechanism's characteristics are: 1. It accepts logical expressions of index words and file names for the specification of protected records, 2. It allows its access control information to be separated from the users' data, 3. It enables the capabilities of using a file to be associated with a user rather than the file, 4. It is built into the system's executive information storage and retrieval subsystem (rather than being incorporated into the file commands themselves which would make it more vulnerable to attack), 5. It provides control mechanism over on-line multi-user access to shared data, 6. It enables a file owner to authenticate users of his file with his log-in program, and 7. It allows protection on a sub-file level.

The use of this system for medical application can be found in [Gelblat 71; Nakanishi 72]. The extension of the access control level to fields and bits is done also by [Gelblat 71].

Hsiao 71

Hsiao, D. K. "A Generalized Record Organization." IEEE Trans., C-20, 12 (December 1971), 1490-1495.

The author discussed the idea of a "record template" whereby the attributes and values of fields are separated. The implication for data security

is that access control information can be separated from the data. In particular, we note that some of the field control information may be placed in the record template along with field names. Therefore, it is possible to determine the validity of a request without bringing that data requested into main memory. A system using this technique is described in [Manola 71].

Manola 72

Manola, F. A Model for Logical Access Control, NRL Memorandum Report, Information Systems Group, Naval Research Laboratory, 1972.

This model attempts to generalize the concepts of capability and object by Dennis and Van Horn [Dennis 66], and the notion of authority item by Hsiao [Hsiao 68]. There is considerable similarity between the author's work and the work of G. S. Graham and P. Denning [Graham 72]. However, the difference lies in the author's attempt to associate the access to data with the structure of data to be accessed since shared data is assumed to be structured.

Vanderbilt 69

Vanderbilt, D. Controlled Information Sharing in a Computer Utility. National Technical Information Service (AD 699 503, October, 1969) or Project MAC (MAC-TR-67), 172 pp.

The author develops an abstract model for structuring and controlling shared information, based on related work by Dennis and Van Horn [Dennis 66].

II. PRIVACY PROTECTION AND ACCESS CONTROL IN COMPUTER SYSTEMS

(3) Working Mechanism And Existing System

Babcock 67

Babcock, J. D. "A Brief Description of Privacy Measures in the RUSH Time-Sharing System." Proc. AFIPS 1967 SJCC, 30, 301-302.

This is a description of the Remote Users of Shared Hardware System. A non-printed password is used at the terminal. The monitored log features include the disconnection of the terminal after two unsuccessful tries. Four character key is used for read-only; two more characters may be appended for write permission. We note that LOAD/SAVE commands are not allowed within a program loop. However, it is possible that the last letters of a password may be linquistically predictable from the first four. Users are limited to man-machine language processors. Remote Job Entry is controlled by prescanning all job control language statements and file calls. No protection from wire tap is considered. It was noted that the interpretive mode of operation aids protection, and remote terminals make it easier to have physical security of the computer center.

Barron 67

Barron, D.; Fraser, A.; Hartley, D.; Landy, B.; and Needham, R. "File Handling at Cambridge University." Proc. AFIPS 1967 SJCC, 30, 163-167.

The authors present the file handling facility of the Cambridge University Titan computer. The owner of a file is allowed to designate "part owners" of that file and their privileges. The file "status" determines those allowable ranges of activities permitted.

Carrc 71b

Carroll, J. M.; Martin, R.; McHardy, L.; and Moravec, H. "Multi-Dimensional Security Programme for a Generalized Information Retrieval System." University of Western Ontario, 1971, 25pp. Also, Proc. AFIPS 1971 FJCC, 39,571-7.

An existing System with 3-levels of protection. They are based on: 1. the subset of ten available processing functions the user can exercise, 2. the items on which these functions can operate, and 3. the records that are locked against the user. The protection code is stored in the password area as bits. All records must have the same number of items in a prescribed order. The Host System is a PDP-10/50, therefore, the entire Information Retrieval System could be compromised by the Host System. Also, no protection from wire tapping. An interesting method of modular and residue arithmetic used to assign partially overlapping data bases is presented.

Conway 72b

Conway, R.; Maxwell, W.; and Morgan, H. "Selective Security Capabilities in ASAP - A File Management System." AFIPS, 1972 SJCC, 40, 1181-1185.

ASAP is a file maintenance and information retrieval system. It uses a directory of authorized users to decide who can get what information and what processes they can execute. The subset of data accessible to a certain user may be described in ASAP by a Boolean expression of keywords as in [Hsiao 68] or by dividing the data into nine independent security classes. When accessing data for a user, the system checks the directory to see whether he is allowed to see that class of data. There is no hierarchical order to these security classes.

Access controls are enforced only at the source language level. Each entry in the symbol table contains a security mask. When the field is referenced its security class is compared with the user's. The authors believe that security checking at compile-time is cheaper than at real-time. However, run-time access control for multi-user on-line environment is not discussed. An encrypting provision for master files is available and is supposed to cost about 500 microsec. on a 370/155 to encrypt a 500-byte record.

Gelblat 71

Gelblat, M.; and Hsiao, D. K. "Privacy Measures and Data Accessibility in a Medical System." A paper presented at the Fourth Annual Meeting of the Society for Epidemiologic Research, May 21, 1971.

This is a description of an automated Cardiovascular Research Data Bank System built on the PSF (the Moore School's Problem Solving Facility).

Privacy controls in form of authority items are attached to the users of the system rather than to the files. Protection of medical information can be facilitated down to individual records and fields. The result is that many different users may have different levels of access to different portions of a file. Further, PSF allows the file owner to write special user programs to screen or authenticate users who wish to use the file owner's data [Hsiao 68].

Glaser 67

Glaser, E. L. "A Brief Description of Privacy Measures in the MULTICS Operating System." Proc. AFIPS 1967 SJCC, 30, 303-304.

MULTICS features: 1. References to file by symbolic name, 2. Each file has an access-control list defining authorized users and how they may gain access to the file. Two main design features are: 1. Compartmentalization of the supervisor to insure minimum damage or loss due to a failure, 2. Auditability, so that one can determine that the proper system is running. Also, an audit trail is kept during the use of the high-privilege "observation" function when the manager can snoop into the activities of a user. It is a very brief paper on MULTICS.

Hirsch 71

Hirsch, J. I. Access Control and Retrieval Optimization Functions of the Supervisor for an Extended Data Management Facility. Moore School Tech. Report 71-21, University of Pennsylvania, April 1971.

The author discusses the Authority Item which is EDMF's control over data security. The authority item is in response to RCA's TSOS DMS which has an "all or none" algorithm for allowing file access. In EDMF the user may be denied access to some parts of the file and yet still be given information from the others. EDMF can protect data on the file, record or field level.

Further, EDMF access control is user-oriented. The access control information is associated with each user as opposed to being found in the header of each file. Thus, the access status information is in a system file instead of scattered about in less secure user files; it is also more easily updated.

A Service Status Block contains information about every file processed by a user during his run. This eliminates some duplicate retrievals of authority item information. A file Status Block is used to overcome the problem associated with multiple users sharing a file in real-time.

For a more up-to-date access control mechanism in EDMF, the reader may refer to [Manola 71].

Hoffman 70a

Hoffman, L. J. The Formulary Model for Access Control and Privacy in Computer Systems. Stanford Linear Accelerator Center, Stanford University (SLAC-117, May 1970, 88 pp.

Hoffman discusses memory wastage problems related to access control information. He notes that Bingham [Bingham 65] suggested using "User Control Profiles" to associate access control with a user rather than with a file, thus reducing duplication of file level access control information. He also noted that Hsiao's system [Hsiao 68] using "authority items" associated with users has the advantage of keeping raw data and access control information separated, and controls access beneath the file level. He further pointed out that Weissman's model [Weissman 69] does not deal with access control below the file level.

In this model, access control is based on a set of procedures called formularies. Data access is controlled by programs instead of by bits or tables. The emphasis on procedures instead of tables is motivated by the author's belief that the decision to allow or disallow access can be made more easily in real time, at data access time, with procedures. The author's approach allows control of data to any level (even to the bit) and separates the functions of data addressing and access control.

To control access to shared data for multiple users, a mechanism known as the LOCKLIST is proposed. The author acknowledges that the mechanism is similar to Hsiao's Blocking/Unblocking mechanism [Hsiao 68].

The use of procedures for access control is not without precedent. For

example, Hsiao's system [Hsiao68] has a mechanism for the file owner to incorporate for a file a LOGIN procedure which can authenticate users of the file each time it is to be opened. However, the generalization of procedure oriented control to exclude any use of tables may be unwarranted. For example, to control access to data, one must describe data. Data description information is mostly non-procedural. To require a user to describe all his controlled field specifications, record organization and file structures in procedures may introduce a cost which far exceeds the cost-conscientious formularies.

Hoffman 71

Hoffman, L. J. "The Formulary Model for Flexible Privacy and Access Controls." Proc. AFIPS 1971 FJCC, 39, 587-601.

This represents a condensed version of Hoffman's Ph.D Dissertation [Hoffman 70a].

Hsiao 68

Hsiao, D. K. A File System for a Problem Solving Facility. Moore School Tech. Report #68-33, University of Pennsylvania, May 1968, 175 pp. Also available from NTIS as report AD671826.

Hsiao describes in detail (including flowcharts) the workings of the file system of PSF (the Moore School Problem Solving Facility) and its access control mechanism. The authority-item approach allows security on the sub-file level; stores access control information in a user-oriented control block (not with the data); and allows the user to write his own real time authentication routine for a file.

As a result of Hsiao's system, data records do not have to be reprocessed if a change in a user's access restriction or a record's protection status occurs. In addition, the user will be unaware of any records which are protected from him. Hoffman [Hoffman 69;70] notes that this is the first working system with protection on the sub-file level.

Hsiao 69 (See [Hsiao 69] in previous section)——

Lampson 69

Lampson, B. W. "Dynamic Protection Structures." Proc. AFIPS 1969 FJCC, 35, 27-38.

This paper deals with the access control mechanism implemented in a Berkeley Computer Corp. Model I Time-Sharing System.

Fundamental to his approach are three concepts: 1. Objects (data or procedures) are named by capabilities [Dennis 66] which are protected by the system. User programs cannot change or create objects arbitrarily. Thus, possession of a capability is proof of one's right to access the object it names, 2. Domains are used to group capabilities. A process executing in a domain can exercise that domain's capabilities. When the process passes to another domain the capabilities of the process will change accordingly, and 3. Capabilities are usually obtained from their domains by presenting suitable authorization in the form of an access key.

The author goes into a detailed discussion of implementing the above system and claims that the net result is a system whereby two domains can "work together to any degree of intimacy, from complete trust to bitter mutual suspicion. It allows a domain to exercise firm control over everything created by it or its subsidiaries."

Manola 71

Manola, F. "An Extended Data Management Facility for a General-Purpose Time Sharing System." Master's Thesis. University of Pennsylvania (May 1971). Also available as NTIS report AD724 801

The author describes an advanced experimental data management system presently operated on the RCA SPECTRA 70/46G time-shared computer system at the Moore School of Electrical Engineering, University of Pennsylvania. The system, known as the Extended Data Management Facility (EDMF) covers a significant spectrum of data management system technology including file structure, record organization, access control, user interface and data management language. The access control mechanism provides both a priori and posteriori analysis of retrieval, and insures protection of data at field, record and file level. An implementation of the concept of the authority items [Hsiao 68]

allows the user to designate either allowable or deniable portions of his data base. In other words, information concerning the authorized as well as unauthorized access to shared data base can be handled by the access control mechanism via user's authority items - a feature which is believed to be advocated by Hoffman [Hoffman 69].

Nakanishi 72

Nakanishi, K; & Hsiao ,D.K "A Cardiac Catheterization Information System - An Application of an Advanced Data Management Facility." Proc. Computer 72, Islands of Applications - Tokyo Conference, IEEE Computer Society and Department of Commerce, Tokyo, Japan, (June 1972).

The paper presents a description of an operational medical information system developed for the doctors and medical researchers at the Cardiac Catheterization Laboratory of the University of Pennsylvania, and includes a discussion of an advanced data management system, know as EDMF [Manola 71], on which the Cardiac Catheterization Information System is built.

The use of the access control features of the EDMF for medical applications is briefly discussed.

Owens 71a

Owens, R. C., Jr. Primary Access Control in Large-Scale Time-Shared Decision Systems. Project MAC TR-89 (July 1971), 91 pp.

The access control problem of the MacAIMS (Project MAC Advanced Interactive Management System) is discussed in light of the following:

1. The 'physical' level at which to apply control (files, record, field...).
2. The fineness of distinction applied to the term "access" (yes or no; or more refined categories like write, read, execute...).
3. The meaning of the term "user identification" (names, passwords, extended handshake, etc.).
4. The degree of sophistication employed in assigning restrictions to new data files (assume no restrictions, all the way to an automatic classification mechanism based on the classification of the inputs).

Owens favors Hoffman's formulary approach [Hoffman 70a]; however, the author is not sure whether the user is sophisticated enough to write his own formularies.

The MULTICS system is described and evaluated in terms of data management purposes. Owens believes that the MULTICS does not have adequate access control mechanisms which allow the user to describe his data in terms of Boolean and arithmetic expressions of keywords or names, on the one hand; and which permit the system to control access to data based on these expressions, on the other hand [Hsiao 68]. He also notes that Weissman's ADEPT-50 scheme [Weissman 69] of automatic classification of new files is a nice feature which MULTICS lacks, but is too restrictive for non-military use. Thus, the MacAIMS project tries to fill in the holes of MULTICS.

From the data base to the user, MacAIMS provides four levels of access: 1. N - for no access (the default condition), 2. M - manipulate; user is allowed to perform set theoretic operations on the data but may or may not be allowed to see the results of those manipulations depending upon other restrictions on the data, 3. S - only statistical information given, and 4. P - any information desired will be printed upon request. From the user to the data base, the standard MULTICS controls are provided: no access, append, write, and change access. Further, MacAIMS separates the concepts of the "owner" of the information, the "originator" of the information, and the person(s) who may change the access control restrictions. A detailed description of the mechanics of MacAIMS is given.

It is an interesting paper on what is being done to upgrade MULTICS for data management.

Owens 71b

Owens, R. "Evaluation of Access Authorization Characteristics of Derived Data Sets." 1971 ACM-SIGFIDET Workshop on Data Description, Access and Control, 263-278.

The author points out that the MULTICS access control mechanisms are closely tied with the physical structure (e.g., segments) of the data base. In contrast, he feels that:

> "The process of access control is the mediator which regulates the flow of information between the logical storage medium (the file), and the requesting entity (the user). The mediation process is a comparison of the characteristics of the sensitive data with the characteristics of the requesting entity and the logical (not the physical) nature of the requested interaction and the results of that interaction, followed by a granting or denial of that request."

The author describes a hierarchy of access capabilities whereby the lower ones must be a proper subset of the next higher level. We note that this approach may not be practical. The notion of separate capability hierarchies for the two directions of information flow is a useful one. Also, the author distinguishes between the ownership of a file and the originator of the data in that file; the latter having more capabilities with respect to that file than the former.

The author disagrees with Weissman's automatic classification scheme for new data files.

Ramirez 68

Ramirez, J. A. Problems in Protection of Information in a Multiuser On-Line System. Moore School Master's Thesis, University of Pennsylvania (May 1968).

The author goes into the actual in-depth implementation of the authority item in the Moore School's PSF (Problem Solving Facility) as described in [Hsiao 68]. Also discussed are the methods used to prevent conflicts arising when more than one user are sharing the same data simultaneously.

Weissman 69

Weissman, C. "Security Controls in the ADEPT-50 Time-Sharing System." Proc. AFIPS 1969 FJCC, 35, 119-133.

This paper describes a set theoretic model which characterizes the access control mechanism incorporated in the ADEPT-50 system of S.D.C. Objects such as users, terminals, programs, files are treated as sets and the mechanism uses set theoretic operations such as membership, intersection, and union to determine access privileges. Objects are given a "security profile" which is a triplet of "Authority", "Category", and "Franchise" property sets. These triplets correspond respectively to the military's classification, compartments and need-to-know.

Features of ADEPT include: 1. Automatic file classification based upon the cumulative security history of referenced files (using the "High-water work" approach), 2. A "security umbrella" of the ADEPT job, 3. Once-only passwords,

4. The ability of the owner of a file to specify and control the file's privacy including the make-up of the need-to-know list, 5. Modification of the 360/50 employed to include fetch protection, and 6. An automatic AUDIT routine.

Extensive work has been done to close any "trap doors" which one usually finds in the I/O section of the operating system. To control classified residue, ADEPT zeros out memory pages and drum pages before allocating them. With disc, however, ADEPT uses "dirty" memory. Therefore, the File Control Section has to make sure that tracks allocated to new files cannot be read until they are first written.

The author maintains that approximately 5% of the design, code and debugging effort was for the security features and 10% of the 50,000 instructions in ADEPT are for security control. Operating overhead is estimated at 1 to 2% of total CPU time.

The major limitations with the ADEPT system are that: 1. Protection is only available at the file level, 2. The security profiles are not easy to compose, and are difficult to update since they are characterized by three property sets, and 3. The use of this system in a non-military environment may be inflexible because compartmentalization of data and the need-to-know privilege are centered around the military applications.

II. PRIVACY PROTECTION AND ACCESS CONTROL IN COMPUTER SYSTEMS

(4) Hardware Protection

Evans 67

Evans, D. C.; and LeClerc, J. Y. "Address Mapping and the Control of Access in an Interactive Computer." Proc. AFIPS 1967 SJCC, 30, 23-30.

This paper describes a hardware mapping mechanism at the segment level by which procedures are bound to their parameters at execution time without modification or relocation. The authors believe that access to a segment does not solely depend on that segment but also on the parameters being passed and the parameters being received.

Lampson 67

Lampson, B. W. Scheduling and Protection in an Interactive Multi-Processor System. Ph.D. Dissertation, University of Calif. at Berkeley (March 1967), 82 pp.

Relevant sections are Chapter 4 on hardware protection and Chapter 5 on memory addressing schemes. Four types of protection are described (protection of the system from the users, users from system, users from themselves, and the system from itself). A further distinction is made between memory protection (accessing, changing or transferring control to certain words in memory) and control protection (executing instructions which are privileged). One suggestion for control protection is not to determine master-mode permission by job but rather by the memory locations from which the job is executed. This would extend the memory protection mechanism to determine not just read-only, but privileged areas as well. Addressing schemes from least to most sophisticated:

1. Physical memory protection is carried out by bound registers defining single contiguous regions or by block-orientated schemes where the address space is divided into fixed-size blocks, each with its own protection bits.
2. Paged memory protection (paging allows the physical location of the various pages referenced by a program to be altered during execution without disturbing the program) is the same as the block-oriented schemes where the blocks are physical pages. Control information is collected on the page tables which can facilitate access control since addressing to part of a physical page must be decoded by hard-

ware via its page table.

3. Segmented memory protection. (Segmentation provides another dimension of managing large address spaces by grouping pages together in units called segments.) Along with the protection features of paging, segmentation reduces the number of unnecessary duplications of the protection bits in the page tables.
4. Partitioned memory protection. (The entire memory is partitioned to m x n segments.) The protection information is specified not by a vector of bits, but by a matrix of m x n entries. An entry A_{ij} determines if segment i is allowed to access segment j, and if so, what kind of access (read only, execute, etc.). We note that A_{ii} determines access rights of segment i to itself.

Molho 69

Molho, L. M. Hardware Reliability Study. System Development Corp., Internal Working Paper, N-(L)-24276/126/00, December 1969, 70 pp.

This is an in-depth study of the hardware aspects of the storage protection and Problem/Supervisor state control systems of the IBM 360/50. By "brute force" the author was able to trace the internal workings of the microprograms of the CPU and discover various "weak points" in the IBM hardware. For example, PSW bit #15 (the Supervisor state switch) is never checked once it is stored in its polarity hold circuit. No redundant storage element is compared to it and no parity check is performed on the half byte in which it resides.

At each junction the author asked "If this element fails, will hardware required for secure computing go dead without giving an alarm?" Dozens of such places were found (listed in his Table 3), three of which were in the PSW bit 15 Supervisor state logic. His discoveries do not include other possible failures such as a shorted input which will cause invalid output states only part of the time or a logic element which exhibits excessive signal delay, and therefore, appears to have an invalid output state for some time after any input transition. Fortunately, many other hardware failures, which would lead to an overall system crash if occurred, are detectable.

The author feels that security problems are really in the control logic

rather than in the multi-bit data paths which most manufacturers load with redundancy and error-detecting/correcting hardware. He also believes that software tests can eliminate hardware failure as a security problem. Such tests, he states, would eliminate 85% of present single-failure hazards in SDC's ADEPT-50 T.S.S. running on the 360/50 CPU [Weissman 69]. If these tests are placed in the microprogram and executed every timer-update time (60/second), the overhead for this protection would be only .015 percent.

Several other points of interest are:

1. "Interdependence is quite useful in a fail-secure system, as it allows failures to be detected by faulty system operation - a seemingly inelegant error detection mechanism, yet one which requires neither software nor hardware overhead."
2. "A further poin[t] . . somewhat controversial: that an overabundance of 'inhibit'-type asynchronous logic is a good indicator of sloppy design or bad design coordination."
3. "To sum up, the fact that a system crashes . . . rather than 'failing soft' . . . may be a blessing in disguise."

This paper is highly recommended for those who want to implement protection mechanisms down at the microhardware level.

Molho 70

Molho, L. M. "Hardware Aspects of Secure Computing." Proc. AFIPS 1970 SJCC, 36, 135-141.

The author summarizes his study of the memory protection and problem/supervisor state control systems of the IBM 360/50. A total of 99 single-failure hazards are found in the storage protection hardware which would not be detectable by a system crash or other noticeable system misbehavior. Software testing of hardware as implemented in the SDC ADEPT-50 T.S.S. [Weissman 69] eliminates over 85% of the above hazards. The author stresses the three following notions:

"Fail-safe" ≡ It does not blow up when it fails.

"Fail-soft" ≡ Degrading of performance when a failure occurs instead of becoming completely useless.

"Fail-secure" ≡ Ability to protect the integrity of information in case of failure.

When hardware fails in a "fail-secure" system, something between the extremes of system crash and silent automatic correction should occur.

Much of the material in this paper is based on an earlier study by the same author [Molho 69].

Schroeder 71

Schroeder, M. D.; and Saltzer, J. H. "A Hardware Architecture for Implementing Protection Rings." Third ACM Symposium on Operating Systems Principles, Palo Alto, Calif. (October 1971), 55 pp. Also available in Comm. ACM 15, 3 (March 1972), 157-170.

MULTICS is a general-purpose, multi-user, interactive computer system developed at Project MAC of M.I.T. It is run on a modified Honeywell 645. The authors describe the hardware implementation of the MULTICS protection rings concentric as conceptualized in [Graham 68]. In hardware, cross-ring calls and subsequent returns can be accomplished without "traps"; and automatic hardware validation of references across ring boundaries can be performed. The Honeywell 645 has access control flags on the segment level. MULTICS uses these flags in its implementation, and therefore, a segment is the smallest unit of information that can be separately protected.

III. COMPUTER SECURITY

(1) General Discussion And Overview

Baran 65

Baran, P. "Communications, Computers, and People." Proc. AFIPS 1965 FJCC, 27, Pt. II, 45-49.

To find solutions to the security problem, one must 1. Assume that everyone is "diabolically clever", 2. Note that systems will get increasingly more complex and that only computer design people will understand them, 3. Concentrate on good design instead of "software patchups" and retro-fits, 4. Devise laws which can raise the price of stealing information, and 5. Use standard equipments on all machines for safeguards (but this will probably not occur until after a disaster). Specific recommendations include: 1. Use of cryptographic techniques for transmitting and storing data, 2. Random audit of file handling programs, 3. Sensible and precise ground rules for inter-system interrogation and access and 4. Provision for the detection of abnormal information requests and recording of the sources of requests.

Bates 70

Bates, [illegible] "Security of Computer-Based Information Systems," Datamation 16,5 (May 1970), 60-65.

The author discusses the security failures in computer hardware and software, and graphs a "system security framework". He suggests that the system monitor be placed in read-only memory. Furthermore, the monitor performs all I/O operations, erases memory segments after each "roll outs" and periodically tests memory protect and privileged instructions to ensure proper functioning.

Beardsley 72

Beardsley, C. W. "Is Your Computer Insecure?" IEEE Spectrum (January 1972), 67-78.

The author spends a good deal of time exposing the security myths being circulated by certain consulting firms. Sloppy storage is said to cause more damage to tapes than vandalism. The "functional password" in [Carroll 70] and the "extended handshake" of the ADEPT-50 [Weissman 69] and Hoffman's formulary model [Hoffman 70a] are summarized. The I.D. card with a magnetic stripe is thought to be the method of future identification. Methods such as measuring physical characteristics of the user are rejected as being too costly and too rigid to reflect daily human conditions (e.g., colds), and too easily fooled.

The author suggests that one should never depend on a computer program to generate random numbers (for a crypto system) since everyone knows the algorithms. He then gives a cost-effectiveness chart showing Vigenere and 2 Vernam schemes. Finally the author believes that the technology is available to protect and audit computer systems, but human frailties still exist. In short, "you can build locks, but who gets the keys?"

Carroll 71a

Carroll, J. M.; and McLellan, P. M. "The Data Security Environment of Canadian Resource-Sharing Systems." INFOR,9, 1 (March 1971), 58-67.

Examples are given on how one can break into a PDP 10/50 system. Countermeasures are discussed along with their effectiveness. Theft of hard copy or card decks was found to be the biggest threat to security, and confidentiality of passwords was "tenuous". Their survey of computer manufacturers showed that: 1. Passwords are the most common method for access control, 2. There is little customer demand for hardware or software cryptographic transformations of data, 3. The manufacturers stress integrity management and log keeping monitoring procedures, and 4. Communications links are seen as a major security weakness.

Their conclusions are that the security of resource-sharing systems is not good; adequate measures are within the state-of-the-art but are costly, especially the need for specialist personnel; and most security provisions would tend to reduce operating efficiency and flexibility.

Courtney 71

Courtney, R. H., Jr. "40 Commonly Found Deficiencies in the Security of Data Processing Activities." I. B. M., June 30, 1971, 14 pp.

This is an annotated list of the 40 most commonly found deficiences in security by the head of I. B. M.'s Data Security and Privacy Systems Development Division. It consists mainly of common sense ideas which try to play down the sensationalism of some members of the security consulting industry.

R. Courtney is also quoted in Industrial Security (13, 6, December 1969, 18-37.) as saying that there is little difference between accidentally or intentionally destroyed data. Therefore, he defines data security as safeguarding data from any unauthorized modification, destruction or disclosure. Courtney dislikes passwords and describes the extended handshake as "people ... being asked questions which the computer already knows the answer to, and they know the answer to ... You are, in effect, talking to yourself at $100.00/hr. or more." Instead, he favors the magnetically encoded credit card leaving off any identifying printed information except perhaps a unique number known only to the security office. Further, a waist-high card-operated gate would surround the terminal so that a user could not forget his card in the terminal without having to jump the gate.

Farmer 70

Farmer, J.; Spring, C.; and Strumwasser, M. J. "Cheating the Vote-Count Systems." Datamation, May 1970, 76-80.

Detecting unauthorized software modifications.

After simulating a vote counting fraud, the authors concluded that:
1. The Op. System is vulnerable to modification and would permit changes without access to the user vote-count system, 2. A vote bias routine could be written

without altering the length of the nonbiased program, 3. A valid "logic and accuracy" test would have a prohibitive cost, 4. Most fraud techniques require only one person, and 5. None of the techniques would be detected by a casual observer, even if he had extensive EDP experience.

A computer fraud routine must: 1. Pass any "logic and accuracy" tests, 2. Be automatically initiated or require minimal intervention while in use (e.g., setting a switch in the console to kick-in the bias routine), 3. Not be identifiable in core dumps or load maps (e.g., use TXT cards when modifying the object deck since REP cards will show up on linkage editor map), and 4. If detected, be attributable to several individuals.

The paper's solutions (i.e., countermeasures) are the same general ones found in the literature and give little assurance to the reader of being successful.

Garrison 70 (See [Garrison 70] in previous section)

Hansen 71

Hansen, M. H. "Insuring Confidentiality of Individual Records in Data Storage and Retrieval for Statistical Purposes." AFIPS 1971 FJCC, 579-585.

Hansen, a statistician, looks at data retrieval of census information. He suggests several techniques to insure against disclosures of confidential information. For example, with aggregate data, one knows that none of the components exceeded the aggregate. Also, on a 50-question questionnaire with 10 questions each having 2, 3, 5, 10 and 20 alternatives, a cross-tabulation yields approximately 10^{38} cells thereby making it highly likely that each person answering the questions would be uniquely determinable. (See Hoffman and Miller's "Getting a personal dossier..." article in Datamation, May 1970 [Hoffman 70b]).

IBM 70

Considerations of Data Security in a Computer Environment. I.B.M., G520-2169-0 (Repr. 7/70), 36 pp.

I.B.M.'s assessment of the security problem.

Discusses: 1. How to determine the nature and extent of the protection required, 2. Audit functions, and 3. Key factors influencing design of the security system. Also covered are terminal identification techniques, Data File Protection, and Data Definition for subfile level protection. An in-depth look at monitoring activity and audit logs is also included.

Peters 67

Peters, B. "Security Considerations in a Multi-Programmed Computer System." Proc. AFIPS 1967 SJCC, 30, 283-286.

"Security cannot be attained in the absolute sense. Every security system seeks to attain a probability of loss which is commensurate with the value returned by the operation being secured... Further, any loss which might occur must be detected." p. 283

The author, an employee of N.S.A. discusses the basic requirements necessary to obtain a highly secure system which uses software protection mechanisms. These are: 1. An 'approved' monitor system which may provide multi-programmed or processor modes and which can provide sufficient logical separation of peripheral devices, 2. Adequate memory protection and privileged instructions, 3. Appropriate physical security to prevent local over-riding of the monitor, 4. Cleared personnel, 5. A log book of activity, 6. Users subject to common discipline and authority, 7. A monitor which provides all I/O without exception, 8. A special program which periodically tests for memory bound failures, 9. Security which is not turned off for program debugging, and 10. Security flags such that "classified" will not become "unclassified" if a single bit is dropped.

Petersen 67

Petersen, H. E.; and Turn, R. "System Implications of Information Privacy." Proc. AFIPS 1967 SJCC, 30, 291-300. Also available as RAND Corporation Report P-3504 (April 1967), 40 pp.

Numerous threats and countermeasures are discussed and summarized in a table. This paper was the first to set down a terminology for various types of infiltration (e.g., "masquerading","between lines entry").

Interesting countermeasures include the requirement that the processor must also be authenticated by the user (not just the other way around); terminal identification; random and one-time passwords; and "privacy instructions" whereby the query languages could do further authentication of the users. We note that some of these countermeasures have been realized by Hsiao [Hsiao 68] as "LOGIN procedures" and by Hoffman [Hoffman 70a] as "formularies".

This paper is comprehensive and informative. It may be considered as a required reading in computer security and privacy.

Turn 70

Turn, R.; and Petersen, H. E. Security of Computerized Information Systems. The RAND Corporation P-4405, July 1970, 8 pp. Also presented at the 1970 Carnahan Conference on Electronic Countermeasures, Lexington, Kentucky, April 16-18, 1970.

The authors note that electronically - perpetrated crime is very simple, involving little physical risk and small probability of detection. Possible techniques of a thief include: deception, wire tapping, circumvention, tampering and physical penetration. Possible countermeasures include: improved operating system, real-time monitoring, positive identification (e.g., one-time passwords, but not necessarily devices such as fingerprint readers which are still susceptible to wire-tapping), protected communications lines and physical premises, and cryptographic techniques ("It is clear that unless the Vernam system is implemented, a large key space is only a necessary but by no means a sufficient prerequisite for obtaining increased security.")

The authors caution the reader that crypto-techniques are still very vulnerable when used on computer languages. This is because these languages have: 1. Limited vocabulary, 2. Rigid format and grammatical structure, 3. Predictable statistics, e.g., character frequencies, and 4. Fixed character set. Further, special circuitry may be necessary to transmit control words used to control a communications network: One does not want to encrypt these words since it would give the wire-tapper information about the encoding mechanism and would

make it impossible for the communications hardware to "pick up" these words. Also, one has to be sure that a word is not encrypted into a special control sequence or it will "fire off" an incorrect control action.

Ware 67a

Ware, W. H. "Security and Privacy: Similarities and Differences." Proc. AFIPS 1967 SJCC, 30, 287-290. Also available as RAND Report P-3544.

The author uses "security" when speaking of computer systems which handle classified defense data and "privacy" for all other data which is to be protected.

The author compares the military security problems with those of the business community. The essential differences are: 1. Legal protection is better for military secrets, 2. The worth of military data is greater, 3. The enemy and the protector have more resources to steal/protect military data, 4. Communications networks are dedicated and protected at all costs for military data, and 5. Users of a "computer-private" network are not subject to the same rigid security training as their military counterparts.

Ware 67b

Ware, W. H. "Security and Privacy in Computer Systems." Proc. AFIPS 1967 SJCC, 30, 279-282.

This short paper is an introduction to the AFIPS 1967 SJCC session on Privacy. The author gives a diagram of a typical resource-sharing computer system and then proceeds to point out the security weak points in such a system. The computing center itself is vulnerable in control of access to files, hardware radiation, hardware and/or software failures, and deliberate acts of penetration of accidental mistakes. The communications links and the remote terminals have similar vulnerabilities.

Ware 70

Ware, W. H. (Editor). Security Controls for Computer Systems. RAND Corporation: Santa Monica, Calif., 1970, R-609, CLASSIFIED ("CONFIDENTIAL").

[We have tried to get this article de-classified. However, a review of the article has appeared in Computing Reviews, March 1972, pp. 101-102. The fol-

lowing is a comment on the review.]

"....One of the most complete documents ever published on computer security." The report also includes a checklist on how to test the secure-worthiness of an installation.

Weissman 70a

Weissman, C. "Trade-off Considerations in Security System Design." Seminar on Privacy: Legal and Technical Protection in the Computer Age (October 1970), 13 pp.

Protection Strategies, as related to the work done on the ADEPT-50 [Weissman 69], include: 1) Isolate 2) Confound (e.g., camouflage and disguise by use of cryptography) 3) Deter (have a high risk/gain ratio) 4) Wager (insure against loss of information) and 5) Delegate (shift protection responsibility and liability to a second party). Further, there is a trade-off between the degree of protection and the cost associated with that protection in terms of dollars and loss of capabilities.

Several tables are included. The first shows system services in order of increasing capability; the next is of control safeguards in order of increasing sophistication; the last is a list of system threats in order of increasing activism derived from papers at AFIPS 1967 SJCC [Ware 67a, Ware 67b, Petersen 67].

The author suggests that where access control for machine language programs is not supported, it is much cheaper and easier to build protection mechanisms (see [Conway 72]). ADEPT allows machine language programs; therefore, it has taken more time and effort.

The author concludes that "certification today is a mystic's occupation! There are no guidelines, rules, policies, agencies, tests, models, or active lobbyists encouraging the development of information system certification. The serious designer must 'solo' from the beginning or hire a professional consultant who makes a living 'breaking' systems."

III. COMPUTER SECURITY

(2) Cryptographic Consideration

Baron 64

Baran, P.. On Distributed Communications: IX. Security, Secrecy and Tamper-Free Considerations. The RAND Corporation, Santa Monica, Calif. (August 1964) (RM-3765-PR, 39 pp.).

This paper is an introduction to basic cryptographic concepts as applied to a data communications network. These concepts and techniques are as follows: 1. Suppress silent periods, 2. Transmit successive message blocks over ever changing paths, 3. Combine end-to-end and link-by-link schemes, 4. Split key bases into parts and deliver separately and 5. Encourage heavy use of unclassified data and then process all data as if they were top secret. The author proposes a universal high-secrecy system made up of a hierarchy of less-secure subsystems where all communication is to be classified. This will hopefully raise the cost of espied information to an excessive level.

Carroll 70b

Carroll, J. M.; and McLellan, P. M. "Fast 'Infinite-Key' Privacy Transformation for Resource-Sharing Systems." Proc. AFIPS 1970 FJCC, 37, 223-230.

First, the authors briefly summarize Peterson and Turn's paper (Peterson 67). They then present findings of a survey of Canadian systems which shows that communications links are a major security weakness. Cryptographic transformations of data are discussed (short key and infinite key) and a mathematical approach is taken to show the effectiveness of the infinite key (e.g., its randomness and overhead costs). Five reasons are given for using an authenticated password to synchronize the cipher key. It is pointed out that the infinite key method can be adapted for eigher high or low security operations thus giving the user the option to balance degree of protection with load on the arithmetic unit due to that protection.

Kahn 67

Kahn, D. The Codebreakers. MacMillan Co., N. Y., 1967 (sixth printing 1970), 1164 pp.

This book is an encyclopedia of cryptography. The author has compiled an almost exhaustive history of crypotography from its early inception. Although the book does not deal with recent computer-aided crypto-systems, it contains a very lucid discussion of the development and theory behind such systems as the Vernam which are often proposed for use in computer applications. It also contains a clear discussion of the theory of various cryptanalytic techniques.

Shannon 49

Shannon, C. E. "Communication Theory of Secrecy Systems." Bell System Tech. Journal, 28, 4 (October 1949), 656-715.

The author gives rigorous attention to the mathematical foundations of Cryptography and Information Theory. Discussions on noise considerations, types of ciphers, and basic weak points in secrecy systems are included. Methods of measuring the effectiveness of a safe system are also discussed. A knowledge of advanced probability theory and measure theory is highly desirable in reading this paper.

Skatrud 69

Skatrud, R. O. "A Consideration of the Application of Cryptographic Techniques to Data Processing." Proc. AFIPS 1969 FJCC, 35, 111-117.

A brief history of cryptography and crypto-techniques is given. Then the author presents a digital substitution (similar to Vernam's double tape), and a digital transposition matrix method for computerizing the encrypting of information.

Skatrud 70

Skatrud, R. O. "Computer and Cryptography." In Privacy: Legal and Technical Protection in the Computer Age, University of Calif., Berkeley (October 1970), 26 pp.

The author gives a very basic run-through of the terms, history and techniques of cryptography. The techniques discussed are practical and "computer-related".

Auguste Kerckhoffs' La Cryptographic Militaire (1883) described the necessary properties of a crypto-system as:

- The security of the system must rest with the key. The key must withstand the strains of heavy traffic.
- Cryptanalysts know the security of the key. Therefore, have it evaluated before using it.
- Compromise of hardware or coding technique should not compromise security of the system.
- Cryptograms must be transmittable over communications media.
- The apparatus associated with the key should be operable or transportable by a single person.
- The key should be easily changed.
- The system must be simple, neither requiring a long list of rules nor mental strain on the operator.

Shannon [Shannon 49] imposed five criteria, two of which are different from Kerckhoffs'. They are:

- The amount of secrecy needed should decide the degree of work needed to cipher and decipher.
- Cipher errors should not spread through propagation of key causing loss of information.

Encoding information in Huffman code would satisfy the second of Shannon's criteria.

III. COMPUTER SECURITY

(3) Bibliography

Bergart 72

Bergart, J. "Computer Security, Access Control and Privacy Protection in Computer Systems." Master's Thesis. The Moore School of Electrical Engineering, University of Pennsylvania, (August 1972).

The current paper is a condensed version of the author's Master's Thesis The thesis includes several tables and diagrams which appear in reviewed works but for the sake of brevity are excluded from the paper. The thesis also includes more articles in the areas of computer security.

Harrison 67/69

Harrison, A. The Problem of Privacy in the Computer Age: An Annotated Bibliography. The RAND Corporation, Santa Monica, Calif. (December 1967; December 1969) (Volume 1, RM-5495-PR/RC, 125 pp.; Volume 2, RM-5495/1-PR/RC, 148 pp.).

The combined volumes contain a total of 629 well-annotated entries. The author provides a cross-referenced index including the following categories: Business, Congressional, News Media, Legal, Social Scientists' and Technologists' views of privacy; Cashless-Checkless Society; Computer Utilities; Data Banks; Electronic Eavesdropping; Statistical Data Center; Government Agencies; and system security.

The texts are a must for any researcher in the security/privacy field. We note, however, that the entries tend to come from the less technical literature. We hope that we have filled in these gaps and have brought the reader up to date with more recent developments.

Hoffman 69 (See [Hoffman 69] in previous section)

Witzer 71

Witzer, H. Computer Security Bibliography, 2nd Ed., AVCO Computer Services: Wilmington, Mass., January 1971, approx. 120 pp.

This bibliography is divided up into three sections: 1. Keyword index, 2. Abstracts by sequence number, and 3. Author index. The abstracts are not very extensive but the keyword index is good. Many news articles are included. It lists 257 items.

IV. BUSINESS AND MANAGEMENT OVERVIEW TO COMPUTER SECURITY

Allen 68

Allen, B. "Danger Ahead! Safeguard Your Computer." Harvard Business Review, 46 (November-December 1968), 97-101.

Security hazards include environmental disaster, mechanical failure, operator error, program errors, theft, fraud, and sabotage. Companies are more concerned with getting a program working than with security. The very complexity of computer systems gives rise to a false feeling of security. Management should apply the same methods and disciplines to its EDP operations' security that it does to any other part of the business (e.g., ledgers and journals).

Carroll 71a (See [Carroll 71a] in previous section)

Chu 71a

Chu, A. L. C. "Computer Security: The Corporate Achilles Heel." Business Automation, February 1, 1971, 32-38.

Gives examples of mistakes. Computer security is an interface of physical, personnel and procedural security, audit controls and insurance. Try to isolate the computer (e.g., double-door entry system), and use gas (vs. water) fire extinguisher system (e.g., Halon). Most computer fraud due to improper separation of programming and operation. Chu quotes W. F. Brown of Avco as saying "Security is like a seat belt. It is a nuisance and it doesn't guarantee there will be no accident. But when an accident does occur, you will find it cheaper. It may save you money, your job, or even your company."

Comber 69

Comber, E. V. "Management of Confidential Information." Proc. AFIPS 1969 FJCC, 35, 135-143.

Detailed outline form for the classification and identification of areas sensitive to intrusion. The author also mentions the predominance of human factors in computer security and gives seven elements of the relationship be-

tween man and his information system. He also examines the requirements for a useful operating system in terms of human factors.

Courtney 71 (See [Courtney 71] in previous section)

Van Tassel 72

Van Tassel, D. Computer Security Management, Prentice-Hall, Inc., N. J., 1972, 220 pp.

The author presents a well organized text on general computer security problems such as physical security, auditing, program and operator errors, fraud, disasters, insurance and cryptography. A series of questions designed to check-list the security of the reader's installation is given at the end of each chapter. An annotated bibliography is also included.

V. SOCIAL AND LEGAL IMPLICATION

Chu 71b

Chu, A. L. C. "The Need to Know ... The Right to Privacy ... . "Business Automation, June 1, 1971, 30-35.

New York State Identification and Intelligence System (NYSIIS) maintains files on over 7 million fingerprints and 2.5 million criminal case histories. The system is linked to 3,600 law enforcement agencies and to the FBI's NCIC. 72 million records are maintained by Retail Credit Corp. of Atlanta. Thus Arthur Miller's "womb-to-tomb dossier" concept may be coming true (Miller 71). The 1970 Fair Credit Reporting Acts help protect privacy, and so would Westin's "writ of habeas data" concept (Westin 70).

David 65

David, E. E., Jr.; and Fano, R. M. "Some Thoughts about the Social Implications of Accessible Computing." Proc. AFIPS 1965 FJCC, 27, Pt. I, 243-247.

"Technical means are not lacking for protecting private information from unauthorized access, while at the same time making it available for statistical surveys and other legitimate purposes." The authors also point out the movement away from "tangibility" in our lives. Their example is the transition from gold and silver as our currency to paper money to checks to perhaps a cashless society.

Miller 71

Miller, A. R. The Assault on Privacy, University of Michigan Press, 1971, 333 pp.

The author, a law professor, describes the growing threat to our privacy due to the advancement of computer technology. He warns that we may come under constant monitoring through a "womb-to-tomb" computer dossier. He is alarmed at the growth of "data-mania" which is producing a "record-prison" whereby no one can escape his record trail.

Westin 70

Westin, A. F. Privacy and Freedom, Atheneum, New York, 1970, 487 pp.

What David Kahn's monumental work is to cryptology, Westin's book is to privacy. The book is an in-depth analysis of the history of privacy. However, like Kahn's book, it was written in 1967, and therefore, is somewhat out of date on recent computer activity. Despite this, the author, a lawyer and political scientist, foresaw that laser technology would advance computer science to the point whereby one 4,800-foot reel of one-inch tape would be able to store a dossier of about 20 pages for every man, woman and child in the U.S.A.

The text is divided into four major categories: 1) The Functions of Privacy and Surveillance in Society, 2) New Tools for Invading Privacy, 3) American Society's Struggle for Controls: Five Case Studies, and 4) Policy Choices for the 1970's. This book is definitely a must for the serious student of privacy. An extensive bibliography is included. [The author has continued to write articles on privacy. In a recent work, "Civil Liberties and Computerized Data Systems", in Computers, Communications and the Public Interest, 1971, Westin jokingly suggests that we create a new protective writ called "Habeas data" to protect us in much the same way as the famous writ of habeas corpus.]