M.I T. PROJECT MAC September 5, 1973

Computer Systems Research Division Request for Comments No. 36

ONGOING RESEARCH AND DEVELOPMENT ON INFORMATION PROTECTION

by Jerome H. Saltzer

DRAFT 2

Acknowledgement

Many individuals involved in the projects described here have spent time patiently explaining their activities to me, putting together written descriptions for me to work from, and reviewing early drafts of my (often muddled) writeups of their research. Thanks are due all of them, but responsibility for mistakes and omissions is my own.

Introduction

Topics related to protecting information stored in computer systems have recently become a very popular subject for research; there appear to be at least nineteen major ongoing research and advanced development projects and perhaps ten smaller efforts in the general area. In addition to these research projects several different manufacturers are developing protection features for their commercial products, and many different government agencies have begun actively worrying about how to secure sensitive information already being (or about to be) processed by existing computer installations. In the following paragraphs I describe all of the current projects I know about that are exploring new areas. Much of the work described here is government sponsored, and that work is largely under the Department of Defense. The topics are categorized by the organization performing the work; the organizations appear in no particular order. As an aid to fitting together the information, the report begins with a brief summary of the different kinds of activities being pursued, with forward pointers to the more explicit project descriptions.

Summary of the kinds of Activities being pursued:

The different kinds of activities related to information protection cover a wide spectrum and defy complete categorization, but it is helpful to summarize the various projects at different locations in terms of their intent. Following each summary is a parenthetical list of organizations doing something in that category. Nine categories cover most of the work reported here:

---

1. System penetration exercises. This kind of activity is directed at current systems, usually with the intent of pointing out the fallaciousness of premature claims that security has been achieved. Successful exercises have also the beneficial side effect of suggesting areas where more work is needed. (Lawrence Livermore Laboratory, Information Sciences Institute, IBM Corporation Research Division, Air Force Electronic Systems Division, System Development Corporation, and the Central Intelligence Agency.)

2. User interface studies. One of the chief problems of present protection systems is that they provide the user with an unacceptably complex environment in which to describe his information protection desires. Research in this area consists in trying out particular protection description schemes on real user communities to learn what responses occur. (IBM R.S.S. Project, Cornell University, Information Sciences Institute, M.I.T. Project MAC).

3. Proofs of correctness. Another major problem of present protection systems is the uncertainty as to whether they are correctly implemented. There are currently no acceptable methods of certifying the correctness of a typical operating system. Work in this area consists primarily in attempts to extend current, rather primitive techniques for proving assertions about programs to cover the constructs typically encountered in operating systems. (Information Sciences Institute, Stanford Research Institute, National Security Agency, University of Toronto.) N.B.: Many other organizations are working on proofs of correctness. The organizations mentioned here have particular interest in the correctness of protection mechanisms.

4. Mathematical models of protection kernels. Complementing the work on proofs of correctness is work on developing a mathematically consistent model of what it means to protect information. Such models might well suggest assertions which would then be input to proofs of correctness. (Air Force Electronic Systems Division, Mitre Corp., Stanford Research Institute, Case Western Reserve, University of Washington.)

5. Protection mechanisms. This activity consists of invention of appropriate architectural structures for protection of information inside the computer system. Problems being studied include structures for enforcing access to change protection specifications; structures which permit user-defined protected objects or protected subsystems; and capability systems. (Carnegie-Mellon University, University of Cambridge, University of California at Berkeley, Digital Equipment Corporation, University of Toronto, and M.I.T. Project MAC.)
6. Security in data communication networks. This activity is centered outside the computer system, but it involves such techniques as end-to-end encryption, which may require help from the computers using the network. (National Security Agency, IBM Corporation Research Division, and Air Force Electronic Systems Division.)
7. Data base facilities. Included here is work on integrating information protection facilities into data management systems. (Cornell University, Rand Corporation, TRW Systems, Rutgers University.)
8. Authentication mechanisms. Several groups are interested in developing more reliable methods of identifying and authenticating the user of a remote terminal. (IBM Research Division, National Security Agency, Air Force Electronic Systems Division.)
9. Department of Defense operational problems. A variety of activities are underway in support of current operational problems of various Defense Department computer-using organizations. (System Development Corporation, TRW Systems, Air Force Electronic Systems Division, and Central Intelligence Agency.)

As will be seen, not all of the work of the various organizations fits perfectly into these categories. Also, some categories such as "Data base facilities" are almost certainly incomplete, since almost every organization developing a data management system is also looking at protection specification mechanisms.

Carnegie Mellon University: HYDRA

As part of the ARPA-sponsored project to develop a multiprocessor computer from a mini-computer base, Professor William Wulf is leading the development of an operating system kernel named HYDRA. This system kernel defines a capability-like architecture which can identify and enforce usage constraints on a large variety of data types (extendable by the user of the kernel). Such a view provides a simple and consistent description of what is sometimes called a "protected subsystem" in other architectures. There are, of course, formidable design and implementation problems that are being explored by Wulf and his colleagues: the protection and stacking of the addressing environment has been worked out in detail; the integration to a user-level interface has just begun.

Although the work was begun in support of the multimini-processor project, the objective of exploring this protection architecture is a full-fledged goal in itself, and has already been the topic of a Ph.D. thesis, by Anita Jones. The current intent is to carry through a complete inplementation of this protection scheme in both hardware and software.

University of Cambridge: The Cambridge Capability System

Dr. Roger Needham of the Computer Laboratory of the University of Cambridge (England) is leading a hardware/software development project to create a new computer system based on a mildly restricted implementation of the "capability" view of protection. In the Cambridge Capability System there are two kinds of segments: those which hold data and those which hold capabilities. (A completely unrestricted architecture would allow capabilities to be placed anywhere.) Further, as many as four capability segments may be active at once in the sense of being available for indirect addressing. This architecture is quite experimental and raises a host of questions about how to develop a complete system around it; understanding and proposing answers to those questions seems to be the main research objective of the group. Complete implementation of both hardware and software are intended.

Lawrence Livermore Laboratory: RISOS Project

Under the leadership of Robert Abbott and sponsorship of ARPA, the RISOS Project (Research In Secured Operating Systems), at Lawrence Livermore Laboratory, in Livermore, California, is trying to develop systematic methodologies to be applied in testing the security of computer operating systems. A key element in the work is the application of computers in both the execution of a test and in the analysis of source code while preparing for a test. A PDP-11 computer is being used during the performance of security tests, while a CDC 7600 is used to assist in analyzing source codes of different operating systems prior to the start of tests.

The PDP-11 will contain a catalog of techniques which have permitted successful systems penetration in a variety of systems. This catalog is hoped to be useful in: developing a metric of a system's security features; helping to spotlight common weaknesses so that researchers and developers of secure systems will learn which areas need more work; and in providing for a while at least, a counter-measure for those present day systems which are retrofitted with security features.

The overall effort is intended to form the basis of procedures which will be used in the certification of the security of an operating system.

In an unrelated project, the Laboratory has developed a computer terminal access system for its CDC 6600-7600 complex which is claimed to be secure.

Information Sciences Institute: Software Assurance Project

Another ARPA-sponsored project is the University of Southern California Information Sciences Institute software assurance project. So far, only a small team is at work there, concentrating primarily on the extension of Ralph London's work on automatically proving assertions about a computer program. London hopes to be able to expand the range of program constructs he can handle to include those of parallel processing coordination, and to handle larger programs. Overall, the objective is to extend these techniques to the point that the central "protection" core of an operating system could be subjected to proof of correctness, as a method of certification.

Information Sciences Institute (Continued)

A second, independent effort at ISI is a system-penetration expertise developed by Richard Bisbey. This expertise was developed before the Lawrence Livermore Laboratory began its project; Bisbey is still performing some of the same functions that LLL is expected to assume when it gets underway. This expertise is being used to develop policies, tools, and techniques for testing and evaluating secure systems.

Also at ISI, James Carlstedt is attempting to formalize the expression of user protection requirements and the translation of such expressions into a general protection description and assertion language.

Case Western Reserve:

There are two projects at Case that are related to information protection. The first of them, under the leadership of Professors E.L. Glaser and C.W. Rose, the LOGOS project (sponsored partly by ARPA) is only indirectly related; its objective is to structure the design and make the implementation of hardware and software systems more or less automatic, thereby reducing the number of logical and implementation errors which make certification of correctness so hard to achieve. The second project, directed by Professor Kenneth G. Walter, is more directly on the subject of information protection: to develop a model of the central protection kernel of an operating system. This work is being done under a newly developing Air Force program on computer security.

Stanford Research Institute: A Demonstrably Secure Kernel

A small team at SRI, led by Peter Neumann, is designing the security-dependent kernel of an operating system. The initial aim is to verify the correctness of the design with respect to security, by as formal an approach as possible. This involves heavy use of structured design, a formal specification language, and structured verification techniques. Considerations of implementation are relevant, but the emphasis is initially on the design.

With respect to verifying the correctness of (implemented) programs, related work is being done by Bernard Elspas, Karl Levitt and Richard Walinger.

Stanford Research Institute (Continued)

At present a prototype system exists, whose performance is now being improved by at least an order of magnitude. Although not specific to security, this type of system could be helpful -- in addition to the above techniques for proving design correctness -- in eventually verifying an implemented system. Each of these projects is government sponsored.

Also at SRI, under a subcontract of the LLL RISOS Project, Donn Parker is developing a file of case studies of computer-related criminal and anti-social acts. This historical record is intended to be of value to workers in the protection field by providing information both on typical system vulnerabilities, and also about typical situations and personalities involved in misuse of computers.

National Security Agency: Computer Security Research Division

The National Security Agency, which already has responsibility for developing methods of securing government communication facilities, is beginning to develop an interest in the problem of securing information in computer systems. To this end, a research division on computer security, under the leadership of Hilda Faust, has been formed. Activities currently receiving attention include: design of a certifiably secure operating system, investigation of methods for proving program correctness, and development of communications security techniques applicable to computer networks. The division is also interested in methods of identifying and authenticating remote terminal users.

University of California at Berkeley: PRIME Project

An ARPA-funded project to develop an ultra-reliable protection system is underway at the University of California at Berkeley. As part of this project, Professor Robert Fabry is developing a software operating system with the property that all protection decisions are performed twice with different algorithms on independent hardware, and cross-checked. Such a strategy will presumably greatly increase confidence that the operating system is correctly implemented, and will also catch most of its own errors, thus making certification easier. It would also maintain protection integrity in the face of hardware failure.

University of California at Berkeley (Continued)

Fabry also is continuing to develop a better understanding of the organization of capability architecture, in which both he and the University of California at Berkeley have had a long-standing interest.

Cornell University:

At Cornell University, Professors R.W. Conway and W.L. Maxwell have been concerned with the appiication of privacy controls to data base systems. They have developed a model of the problem which separately identifies controls applicable at compile-time from controls applicable at run-time, and which includes the idea of controls which are data-dependent. (E.g., access is granted to examine all salaries whose value is less than $10,000.) This model has been implemented in a data base system which is now in production use, and used as a case study for instruction.

University of Toronto:

At the University of Toronto work on the design of secure systems was carried on under the auspices of project SUE. Currently there is an attempt to prove properties of programs including the effectiveness of protection mechanisms. In addition, an investigation is underway of existing systems with respect to security requirements and provisions. The work is under the leadership of Professors K. Sevcik and D. Tsichritzis.

IBM Corporation: Research Division

The IBM Research Division at Yorktown Heights has recently created a group under the leadership of Dr. Joel Birnbaum to explore protection problems. Three projects are currently underway. The first is a long-standing effort to develop a simple cryptographic system suitable for securing the communication line between a terminal user and his computer. A prototype system, called LUCIFER, has been developed, based on a hardware enciphering box at the terminal which accepts a 128-bit key on a magnetically striped card. At the computer end, the main processor performs enciphering and deciphering. The second project is exploration of the possibilities of using the dynamics of a hand-written signature as an authentication mechanism. A simple scheme for observing

IBM Corporation (Continued)

the dynamics of a handwritten signature has been invented, and the problem being explored is the reproducibility of the dynamics of the original signer as compared with those of a potential forger. The third project, under Dr. Laszlo Belady, is an analysis of the CP-67 system from a security point of view to learn what kinds of security holes may still turn up in a system which is basically designed to keep users totally separated from each other. This third project is intended to form the nucleus of a larger, more general attack on information protection problems.

IBM Corporation: R.S.S. Project

The IBM System Development Division has installed a special version of OS/360 MVT, known as the Resource Security System, at four sites. The system has two major modifications when compared with the standard OS/360: all known ways of "crashing" the system have been repaired, and a security compartment/category/classification system resembling the U.S. government defense security system has been added. The purpose of the study is to test the modifications in a live user environment to see what reactions, if any, are invoked. Specific questions under study are: What performance cost is encountered? How is the user not concerned with security affected? Is the security control system provided in R.S.S. adequately convenient and flexible? The test sites are the M.I.T. Information Processing Center, TRW Systems, The State of Illinois, and an IBM internal site in Gaithersburg, Maryland.

System Development Corporation: System Security Department

The System Development Corporation is engaged in a broad program of research and development in computer security, headed by Clark Weissman. Three separate efforts are exploring security problems in current, soon-to-be-available, and future computer systems.

The first effort, under Bruce Peters, is directed at the securing of existing, especially defense department, systems. This effort includes both penetration studies, and identifying security requirements of particular installations. One of the key systems under study is the World-Wide Military Command and Control System (WWMCCS) and its data communication network.

System Development Corporation (Continued)

The second effort, directed by William Shorberger, is intended to make possible specification of security requirements when procuring a new computer system. It includes developing operational policies for computer systems which correspond to already existing security policies of military and commercial organizations, and translation of these policies into system specifications.

The third direction, under Gerald Cole, is development of appropriate system architectures for future systems to use, and for practical retrofits to improve security on current systems. The group is also exploring the use of structured programming as an aid to producing provably correct operating system software.

Air Force Electronic Systems Division: Security project

The United States Air Force Electronic Systems Division at Hanscom Field, Massachusetts, has begun a program, under the leadership of Major Roger Schell, to provide security in Air Force computing systems. This program is planned to be quite wide-ranging, although it is just now gathering momentum. Among the projects now underway are: development of mathematical models of the security kernel of an operating system; development of simple cryptographic facilities for securing computer input/output lines; constructing a demonstration prototype of a magnetic strip "credit card" authentication system; and establishment of security requirements and system changes needed by a Honeywell Multics system to be installed at an Air Force Pentagon site. A technology study, performed by a panel of outside consultants, chaired by Professor E. L. Glaser, has recommended a seven-year, multi-million dollar activity to provide security for Air Force computing systems; the Electronic Systems Division is proposing to carry out the activities recommended in the technology study.

MITRE Corporation:

The MITRE Corporation, under Dr. Steven Lipner, is working closely with the Air Force Electronic Systems Division, and in addition is pursuing several related projects. These are: design and implementation of a provably secure kernel for a DEC PDP 11/45 computer, formal modeling of security aspects of computer systems (Multics in particular), two micro-programmed emulations of

MITRE Corporation (Continued)

the Honeywell 6180 as part of security architecure studies, application of virtual machine techniques within a security kernel, application of a certifiably secure kernel to Multics, and development of a prototype secure data management system for the PDP 11/45.

RAND Corporation: Privacy in Data Banks

The RAND Corporation is performing a study, funded by NSF and led by Dr. Rein Turn and Dr. Mario Juncosa, on aspects of maintaining privacy of personal information stored in data banks. Two directions are being pursued. The first direction is the application of mathematical analysis to privacy problems. Methods from information theory are being used to analyze irreversible privacy transformations, and entropy theory is being used to measure the amount of protection afforded by statistical aggregation in a data bank. Methods of game theory are being applied to models of the interaction between a data bank protector and an intruder. Finally analysis of protection in centralized versus decentralized data bank systems is being performed, along with preliminary studies of the psychology of privacy problems.

The second direction is less theoretical, and includes developing a model which displays the privacy aspects of a data bank, and the threats it must face, developing models of protection systems, and developing measures of effectiveness of protective mechanisms, including privacy transformations which encrypt sensitive information.

In a related project, Dennis Hollingworth has been exploring methods of adding entrapment strategies to computer systems.

Rutgers University:

Rutgers University has an ARPA contract to do research on secure operating systems, concerned with the conceptual and technical problems involved in the specification, design, and validation of protection mechanisms in operating systems. The long-range goal is to automate the design and verification of protection mechanisms in operating systems.

Rutgers University (Continued)

This project, under Professors William Easton and Chino Srivanasan is just getting started. One particular area to be explored is protection of individual records stored in highly indexed information retrieval systems, in which the indexes may be sufficient to reconstruct individual records.

TRW Systems:

TRW Systems, in Redondo Beach, California, has developed several activities related to information protection, primarily with respect to government classified information. Dr. Eldred C. Nelson is associated with these activities. In addition to participating as a study site in the IBM R.S.S. project, three other kinds of activities are underway:

1. A relatively secure operating system for batch jobs on the CDC 6600 has been developed
2. Under a contract with Rome Air Development Center, TRW is developing a computer security handbook for Air Force systems. It would help administrative personnel establish their real security requirements, and provide detailed specifications, for example, of threat monitoring techniques.
3. TRW has developed data management systems with separate control of access to files, records, fields, and even specific field values, and depending on the operation requested. Study is proceeding on the interface between the data management system and the underlying operating system: the object is to develop more carefully a model of the data management system's support needs.

M.I.T. Project MAC

The Computer Systems Research Division of M.I.T. Project MAC, under Professor Jerome Saltzer, has a variety of projects underway related to information protection. These fall into three categories. The oldest area is research on design and implementation of new protection mechanisms. The techniques being explored include protection implications of an addressing architecture with an address space so large that addresses need never be reused; methods of permitting mutually suspicious programs to be used in a

M.I.T. Project MAC (Continued)

single computation; and methods of imitating, in the computer, the restricted hierarchical control of information access found in most social organizations. The second area is development of better, simpler user interfaces to information protection facilities. Particular problems here include simplifying the interface encountered by the user with a routine information protection need; establishing reliable default settings for access controls on newly created objects, so that only exceptions require explicit consideration; and arranging so that a user can easily determine whether or not his access control specifications match his protection intents. The third, and largest, activity is developing a version of the central core of the Multics supervisor which is sufficiently simple and small in size that it could reasonably be audited for security troubles. The heart of this third activity consists of sorting presently protected supervisor functions into three categories: those not requiring any protection, those requiring protection but not implementing information protection (e.g., processor scheduling), and those which implement information protection. A key constraint on this work is that the functional capabilities of the present Multics not be compromised in any important way. This project is just beginning, is expected to require about three years, and is intended to produce a working prototype.

Miscellaneous other Activities:

A variety of other activities, on related topics but generally smaller in extent, are underway at other places. These are listed here for completeness:

- The Oberpfaffenhofen Computer Center in Wessling (near Munich) is devising an access control language to be used in a "national data bank" for the German Government.
- Within the ARPA network, interest has developed in one-way encrypting transformations to protect passwords to be passed through an otherwise insecure environment. Suggestions for such transformations have come from G. Purdy, of the University of Illinois, Dr. Arthur Evans of the M.I.T Lincoln Laboratory, and Major Roger Schell of AF/ESD.

- The Association for Computing Machinery convened a workshop in January, 1973, to discuss protection of information in computer systems and to write papers summarizing the state of the art. (The workshop proceedings have not yet been published.)
- The Central Intelligence Agency reported at the June, 1973, National Computer Conference that it has developed a team of specialists to test the security of its own computer installations.
- The Canadian software house of Sharp Associates, Ltd., has developed an APL-based file system which it claims to be secure. The system goes under the name of APL plus.
- The Dartmouth Time-Sharing System has recently been described as providing substantial protection from user-induced system failures.
- Gregory Andrews of the University of Washington, is attempting to develop a model protection system about which provable statements may be made. The system seems to have properties of both domain and capability models, and is to be demonstrated by implementation on an X.D.S. Sigma 5 computer system.
- James Anderson, a private consultant to several government agencies on computer system security, has been examining defenses against attempts to render a system unusable. He has also acted as a leader in helping define the government's requirements for secure systems.
- National Cash Register, San Diego, recently developed a secure transaction processing system based on a capability organization. For the moment, however, this work is not being pursued.
- At the Digital Equipment Corporation, Michael Spier has developed a domain model of protection and has implemented a working prototype on a PDP 11/45 computer system.

Summary of Locations and Level of Effort

Summarized below are the locations working on information protection, and a rough estimate of the current level of effort at each location, measured in professional man-years of work per year of real time. The estimates are mostly my own, based on personal observation or hearsay, and are

therefore subject to considerable noise. They are nevertheless useful in assessing the breadth and depth of the work to be done at each site.

	Site of work	estimated man-years/year
1.	Carnegie Mellon University	3
2.	University of Cambridge	7
3.	Lawrence Radiation Laboratory	7
4.	Information Sciences Institute	4
5.	Stanford Research Institute	4
6.	Case Western Reserve	3
7.	National Security Agency	5
8.	University of California at Berkeley	3
9.	Cornell University	3
10.	University of Toronto	3
11.	IBM/R.S.S. project	?
12.	IBM/Research Division	6
13.	System Development Corporation	~10(?)
14.	MITRE Corporation	13
15.	Air Force Electronic Systems Division	5
16.	RAND Corporation	6
17.	Rutgers University	3
18.	TRW Systems	?
19.	M.I.T. Project MAC	8

The following sites are estimated to be operating at a rate of about one man-year per year or less:

20. Oberpfaffenhofen Computer Center
21. University of Washington
22. ARPAnet password work
23. ACM Workshop
24. Central Intelligence Agency
25. Sharp Associates/APL
26. Dartmouth Time-Sharing System
27. James Anderson
28. National Cash Register
29. Digital Equipment Corporation

Bibliography

It is difficult to construct a useful bibliography of work in progress, since written material is often limited to project proposals and progress reports, neither of which are widely available. For the reader interested in pursuing the literature on information protection, the following two references contain extensive annotated bibliographies of previously published work:

1. Bergart, J.G., M. Denicoff, and D. K. Hsiao, "An Annotated and Cross-Referenced Bibliography on Computer Security and Access Control in Computer Systems," Ohio State University, Computer and Information Science Research Center Report OSU-CISRC-TR-72-12.

2. Hoffman, L.J., "Computers and Privacy: A Survey," Computing Surveys 1, 2, June, 1969, pp. 97-103.

In addition, the Lawrence Livermore Laboratory RISOS Project has constructed a KWIC-index style bibliography of the literature in this area.