MTP-142

computer security research & development requirements

S. Lipner

THE MITRE CORPORATION

February 1973

MTP 142

MTP 142

COMPUTER SECURITY RESEARCH AND DEVELOPMENT REQUIREMENTS

by

Steven B. Lipner

February, 1973

THE MITRE CORPORATION
BOX 208
BEDFORD, MASSACHUSETTS

This document has been approved for public release.

Contract No. 19628-73-C-0001
Project 572E

ABSTRACT

This paper is concerned with Air Force requirements for secure computer systems, and planned technical approaches for satisfying those requirements. A secure computer system is defined as one that simultaneously processes multiple levels of classified data and supports users with varying clearances. User requirements for secure computer systems are identified, and a cohesive plan to satisfy these requirements, including main computer and supporting communications equipment, is outlined. The technical approach to developing a provably secure, general-purpose main computer is described.

ACKNOWLEDGEMENT

The approaches identified in this paper reflect the suggestions of numerous individuals active in the field of computer security. Of particular note are the contributions of those people who served with the author on the Computer Security Technology Planning Study Panel of the Air Force Electronic Systems Division: James Anderson, Melvin Conway, Daniel Edwards, Hilda Faust, Edward Glaser, Eldred Nelson, Bruce Peters, Charles Rose, and Clark Weisman.

In addition to the panel members, Major Roger Schell and Lieutenant Gerald Popek of ESD's Directorate of Information Systems Technology have suggested technical approaches to building a "security kernel." To their suggestions are added those of David Bell, Edmund Burke, and Leonard LaPadula of The MITRE Corporation.

TABLE OF CONTENTS

INTRODUCTION

This paper presents the slides and text of a briefing on Computer Security Research and Development that was presented September 26, 1972, to the Office of Naval Research Conference on ADP Secure Data Sharing. The conference brought together researchers, users, and manufacturers of computer systems to discuss secure data processing problems and the possibilities for their solution.

The briefing covers the background, problems and requirements, and needed developments for secure data processing. Five development objectives are defined, and a technical approach for meeting the most crucial of these is identified. In addition, related efforts in the field are cited, and a projected schedule for implementing a secure computing capability is presented. The sections on needed developments and technical approach have taken some direction from the recommendations of the ESD Computer Security Technology Planning Study Panel.

THE MITRE

COMPUTER SECURITY
R & D REQUIREMENTS

BACKGROUND

PROJ.
VG. D72-V-547

- STUDIES OF USAF PROBLEMS
- MITRE RESEARCH/STUDY EFFORTS
- ESD PANEL ON COMPUTER SECURITY TECHNOLOGY

BACKGROUND

The Air Force Electronic Systems Division (ESD) and The MITRE Corporation have been involved in computer security efforts for the past several years. Edward Bensley of MITRE was a member of the Defense Science Board Task Force on Computer Security (the Ware panel). More recently, MITRE/ESD teams have performed studies and made recommendations on the computer security aspects of a variety of Air Force systems including the Military Airlift Command Integrated Management Systems (MACIMS) and the Air Force Data Service Center's large multicomputer facility. Team members also participated in computer security tests and studies outside the Air Force, including the Defense Intelligence Agency's On-line System (DIAOLS) test and the Joint Technical Support Agency's ongoing World Wide Military Command & Control System (WWMCCS) security evaluation.

Experience with current commercial computer hardware and software systems has shown that systems must be designed for security if they are to provide a useful degree of protection for the information they store. Thus, MITRE has undertaken (under Air Force sponsorship) a research and experimentation program in the design of a secure, special-purpose (communications processor) computer system, as well as mathematical modeling of a secure, general-purpose, hardware/software system.

In a further effort to identify promising approaches to solving computer security problems, ESD has funded the Computer Security Technology Planning Study Panel. This panel is chaired by Professor E. L. Glaser of

Case Western Reserve University, and operates under a contract from ESD to James P. Anderson and Company. A number of the recommended developments and approaches in subsequent sections of this briefing are drawn in part from the Panel's draft report. The discussion of user requirements builds on the author's experience as chairman of the Panel's Requirements Working Group.

THE MITRE

COMPUTER SECURITY R & D REQUIREMENTS

OPERATIONAL NEEDS

PROJ.
VG. D72-V-548

- MULTILEVEL OPERATION
- OPEN OPERATION
- ON-LINE OPERATION
- TRANSACTION PROCESSING
- PROGRAM DEVELOPMENT
- NETWORKS

PROBLEMS AND REQUIREMENTS

Operational Needs

Working-level staff members from a variety of Air Force commands served on the Requirements Working Group of the ESD computer security panel. The operational needs listed on the slide are drawn from observations of the working group members, and confirmed by ESD/MITRE experience with planned and existing Air Force systems.

A multilevel operation is one in which users having varying levels of clearance and need-to-know can access a computer that stores data of several classifications and categories. As larger, more powerful computer systems are installed, they tend to replace separate systems dedicated to single security levels. For example, one new WWMCCS computer may be required to support both comptroller functions classified up to Secret, and operational functions classified to Top Secret. It is often impractical to clear all system users for the highest level of data, or to separate the processing of different levels by time of day. Thus the computer system is required to prevent users from accessing data for which they are not cleared.

Open operation is the most challenging type of multilevel operation. In this case, some users, user work areas, or communications are uncleared. The open environment provides a would-be penetrator with a logical point from which to begin his attack on a system.

Most new computer systems being installed by the Air Force have at least some aspect of on-line operation, with numerous users accessing the

computer directly from communications terminals. An open on-line system (there are several planned) allows a penetrator to attack the computer's security controls from a remote location (by telephone) so that even if he is detected, he runs little physical risk of being apprehended.

Transaction processing systems provide some users with restricted functional capabilities, such as allowing them to retrieve or update only certain fields in a data base. Such systems restrict users' abilities to probe for security weaknesses and thus seem "easier" to secure than more general ones. However, even transaction processing systems can provide points of attack, as noted in the discussion of the next slide.

Program development is the most vulnerable area for an attack on a computer system's security. The programmer has a powerful tool — the computer itself — with which to probe for potential weaknesses. While the prudent penetrator perfects his attack on a "friendly" computer, identical to his target, an error by the penetrator may be indistinguishable from a coding bug, and may go unnoticed by system security personnel. Although the bulk of the users of a transaction processing system are not allowed to write programs, the system must still support changing applications and maintenance, both of which require some amount of continuing program development.

Numerous organizations are now planning the development of computer networks to support the rapid interchange of data among related computer systems. Even if every computer in a network is secure, problems of user identification and distributed responsibility arise. If any member of the net can be penetrated, as is likely with today's computer systems, the entire network community may be in jeopardy.

THE MITRE CORPORATION

COMPUTER SECURITY
R & D REQUIREMENTS

SECURITY CHALLENGES

PROJ.
VG. D72-V-609

- MALICIOUS THREAT
  - CENTRAL TARGET
  - REMOTE ATTACK
- SECURITY PERIMETER
- PENETRATION OF SYSTEMS
  - GCOS EXPERIENCE
  - OS/360 EXPERIENCE
  - NOT A PRESCRIPTION

Security Challenges

In designing security controls for a military computer system, an environment of "malicious threat" must be assumed. In such an environment, a would-be penetrator is professionally supported, has considerable resources to expend, and is willing to undertake a relatively long-term effort. Such a penetrator is motivated by the concentration of highly accurate classified data in the computer system, and encouraged (if the system is an open one) by the possibility of a remote attack. With almost every system now in use, it must be assumed that the penetrator has his own computer on which to prepare an attack. While the target computer's operating system may be a modified version of the one available to the penetrator, in most cases security modifications are superficial and an attack transfers easily from a standard environment to a "secure" one.

In an environment of malicious threat, the extent of a system's security perimeter must be determined; i.e., the portion of the system that, if written by a hostile agent, could allow a successful attack. Programs within the perimeter must be written or reviewed line by line by cleared personnel. In many systems that use standard, current, hardware and operating systems, the security perimeter is surprisingly large. In a system that does not provide enforced barriers between programs, it is clear that the entire operating system or (in a transaction processing system) the entire transaction processing program is within the perimeter. It should be noted that even a programmer who writes the assembler or compiler used to maintain an operating system can insert sufficient code to recognize a critical operating system routine at assembly (compile) time and alter it to permit a later penetration. Therefore, the language processor should be placed within the perimeter. The alteration (or trap-door) need only recognize a penetrator's

call and execute one or two instructions for him in supervisor mode. The recognition phase may, in fact, be more difficult than the execution. The trap-door must be placed at a seldom-used entry to the operating system, and must use a long enough "key" to render its accidental invocation unlikely. Careful application of the trap-door may even allow a penetrator to turn a transaction system into a programming system by entering machine instructions (perhaps as a character string) into a buffer, and then transferring control to them.

Experience with penetrations of current commercial operating systems (and their derivatives) has confirmed the impression that such systems are not adequate for security in a malicious threat environment. This result is what one would expect, for neither the operating systems nor their underlying hardware were designed with security as a primary objective. Unfortunately, penetration does not explain what to do to secure a system. It is possible to patch all of the "holes" a friendly penetration team finds, but there is no guarantee that there aren't just as many (more obscure) holes left to find. The penetration team's problem is critical, for it must find every hole, while the actual penetrating agent, need find (or insert) only one.

THE MITRE CORPORATION

COMPUTER SECURITY
R & D REQUIREMENTS

TECHNICAL NEEDS

PROJ.
VG. D72-V-545

- GENERAL-PURPOSE SYSTEMS
  - OPEN USE
  - USER PROGRAMMED
- AIDS TO EFFECTIVE USE
  - MEDIA SANITIZATION
  - COMMUNICATIONS SECURITY

NEEDED DEVELOPMENTS

Technical Needs

The review of user requirements for computer security clearly shows a need for secure, general-purpose, multi-user computers and operating systems. If such systems are adequate for use in an open environment, requiring support for user programming, they should also be adaptable to providing security in more restricted environments, such as closed, multilevel operation (all users hold some level of clearance) or transaction processing systems. Depending on the nature of a transaction processing application, it should even be possible to place most transaction processing programs outside the security perimeter (i.e., to let them be uncertified).

A secure, general-purpose computer system must be usable and practical as well as secure. This requirement means that the system's functional capabilities must be susceptible to evolution as new applications are identified. Thus, in structuring a usable, general-purpose, secure system, there are two alternatives:

(1) Arrange for programs that are effected by evolution to be within the security perimeter, but make their recertification as secure relatively easy.

(2) Arrange for most programs that are likely to be effected by evolution to be outside the security perimeter.

At present, it appears that the second alternative is by far the more practical.

To satisfy military requirements, a secure, general-purpose computer should be supplemented by aids for effective computer use in a secure environment. One aid would provide for sanitization (or declassification) of magnetic storage media that have held classified information. Sanitization is necessary in a tactical environment to keep media from falling into unfriendly hands, and in other environments to allow storage devices to be returned to vendors in an unclassified form.

Current communications security devices are quite effective, but their installation and operation are quite costly in some computer environments. In particular, the cost of numerous communications security devices serving secure lines from a central site, and the cost of providing physical protection for communications security devices at remote terminal sites have had significant impacts on some users. Applications of new techniques may result in more economical communications security for central computer sites and remote terminals.

THE MITRE CORPORATION

COMPUTER SECURITY
R & D REQUIREMENTS

DEVELOPMENT OBJECTIVES

PROJ.
VG. D72-V-608

- CENTRAL COMPUTER HARDWARE/SOFTWARE
- DATA MANAGEMENT SOFTWARE
- FRONT-END PROCESSOR/CRYPTOMULTIPLEXER
- INTEGRATED SECURE TERMINAL
- MEDIA ENCIPHERMENT TECHNIQUES

Development Objectives

A set of five development objectives, listed on the slide, have been identified as necessary for fulfilling the needs and requirements cited previously. The following discussion touches on the relevance and nature of each objective.

Secure central computer hardware and software are required to satisfy basic user needs for computer security. A secure computer/operating system combination can be used in both general programming and restricted application environments. A central computer development must show the possibilities of certifying system security and allowing for evolution of application-related components. Such a development should also show the practicality of developing secure, restricted-application subsystems and of applying existing application programs in a secure environment.

The provision of data management software to allow effective use of the secure computer environment is another important development objective. A great many Air Force applications involve handling large multilevel data bases. Data management developments are intended to provide tools for specializing the secure computer system to data-base-oriented tasks. The key objectives of this development are to provide effective data base security by exploiting the operating system (rather than by extending the security perimeter) and to allow the handling of a useful variety of multilevel classified data bases.

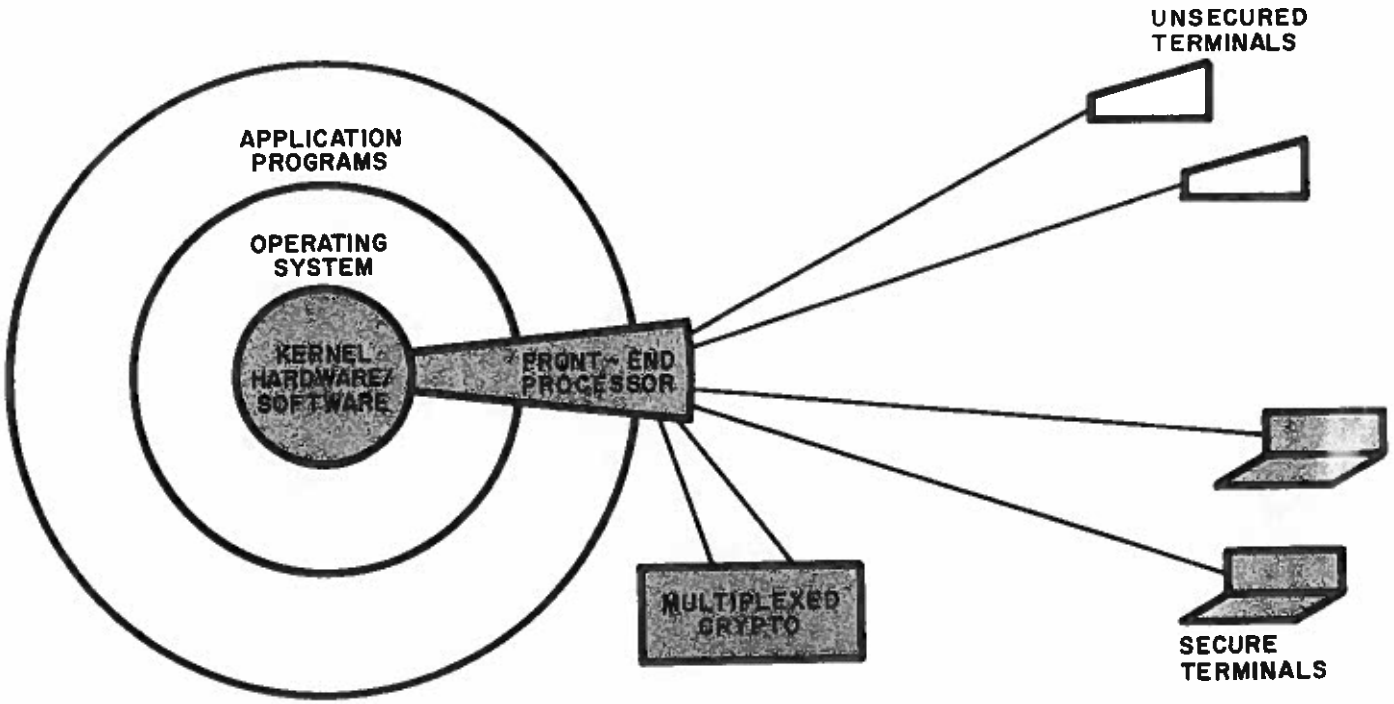
A secure front-end processor (or communications processor) is required as an adjunct to a secure central computer. The front-end processor is also a logical vehicle for controlling the encryption of communications with a large number of remote terminals. The objectives of this development,

then, are to provide an economical multiterminal communications security facility and to provide a secure front-end processor compatible with the central computer.

The final development objectives identified on the slide are intended to provide increased economy and versatility for users that must process classified data. An integrated secure terminal should be capable of being used in any office environment where there is a requirement for remote-access processing of classified data. Such a terminal should be capable of being installed wherever a safe could be installed, without imposing requirements for costly physical protection of cryptographic equipment or for cryptographic access by user personnel. Integrated design of communications, security, and terminal components should make the complete terminal a relatively low-cost device suitable for wide application.

Media encipherment techniques will permit users who must store classified information on magnetic media to render those media unclassified quickly and effectively. Placing a suitable cryptographic device between a computer and (say) a disk renders information on the disk unclassified. Thus the capture or disposal of the disk by itself cannot cause a compromise. For information on the disk to be compromised (or used), that information must first be deciphered with the correct key by the cryptographic device. If the key is not available, the information is irretrievably lost. Thus, destruction of the physical and/or electrical representation of the key effects denial of access to classified information on the disk. The destruction of the key can be rapid, effective, safe, and inexpensive compared to methods involving physical destruction of the disk itself.

INTEGRATED SECURE COMPUTER SYSTEM COMPONENTS



SECURITY - RELATED (CERTIFIED) ELEMENTS

An Integrated Secure Computer System

The overall objective of the planned development effort is to provide a complete and integrated secure computing environment. This slide shows the relationships among major components — the data management software is one particularly important set of application programs, while the connection to media encipherment devices is not shown on this slide. The secure computing system shown is intended to provide convenient, economical, and secure processing of classified data from remote user to central computer and back.

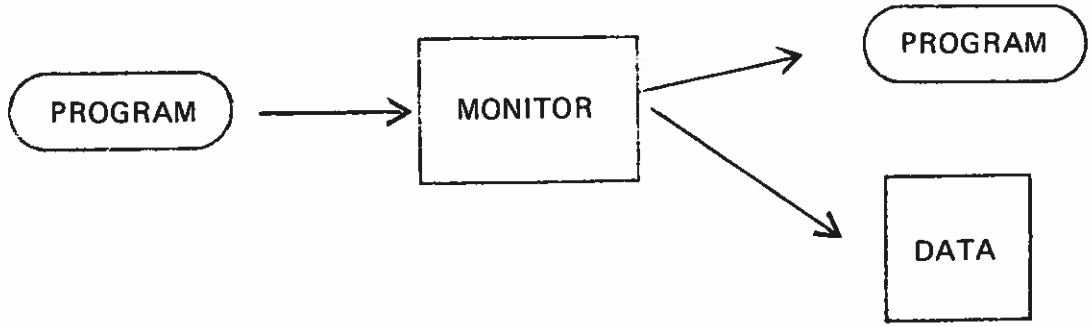
THE MITRE CORPORATION

COMPUTER SECURITY
R & D REQUIREMENTS

CENTRAL COMPUTER

PROJ.
VG. D72-V-607

- REFERENCE MONITOR PRINCIPLES
  - REFERENCE MONITOR TAMPERPROOF
  - REFERENCE MONITOR ALWAYS INVOKED
  - REFERENCE MONITOR SUBJECT TO CERTIFICATION



TECHNICAL APPROACH

Meeting each of the stated development objectives requires the identification of an appropriate technical approach. However, the most difficult technical problems are presented by the development and certification as secure of a central computer and its operating system. The preceding slide, and those that follow, present some key facets of the approach for providing a secure general-purpose computer and operating system.

Reference Monitor

The ESD computer security panel identified the concept of a reference monitor as fundamental to the design and certification of a secure computer system. The reference monitor is that portion of the computer's hardware and software that restricts user processes (programs in execution) so that they may only access information in an authorized way. The reference monitor of a secure system must meet the three requirements shown on the slide.

First, the reference monitor must be tamperproof. It does no good for us to develop a reference monitor that correctly protects programs and data if we cannot protect the reference monitor and its data bases. The reference monitor should (in the most elegant form) be protected by the same mechanisms it applies to protect other information. There are alternatives, however, such as the isolation of some or all parts of the reference monitor in a read-only memory, or in a separate processor.

Second, the reference monitor must be invoked on every attempt by a user's process to access information. This requirement clearly does not mean that every reference is subject to extensive software checks. However, it does mean that every reference must be checked either by software or by hardware that is provided with sufficient information to make the correct decision on granting or denying access to information.

Third, the reference monitor must be subject to certification. "Subject to certification" implies that the reference monitor's correctness must be provable, or that it must be subject to exhaustive (enumerative) tests, or that it must be capable of being understood completely at one time by any competent programmer. (Preferably, all three interpretations would hold.)

The question may now be raised, "What about the reference monitor in a current operating system?" Some current off-the-shelf systems do provide checking of every reference to main memory, through base and bound registers or other memory protection features. However, the application of this checking is usually incomplete, and the user can often alter critical information stored within his memory partition, or gain illegal access to areas of secondary storage. Current systems frequently fail to provide their supervisor code and data bases with adequate protection from user processes. With the reference monitor equal to the entire supervisor in such systems, the user can exploit this inadequacy to gain control of and access to an entire system. The fact that the supervisor and the reference monitor are synonymous (for there is no further division in the supervisor) effectively precludes certification. The idea of proving, testing, or even understanding tens or hundreds of thousands of lines of supervisor code

would be laughable were it not necessary for securing current hardware/software systems.

The next three slides identify the approach to defining requirements for a reference monitor, and to implementing a secure computer that includes a reference monitor.

THE MITRE CORPORATION

COMPUTER SECURITY R & D REQUIREMENTS

CENTRAL COMPUTER

PROJ. VG. D72-V-610

$S_u \geq S_i$ (u = user; i = information; S = level)

and $C_u \supseteq C_i$ (C = formal access category) and

OBJECTS

SUBJECTS	USER A PROCESS	USER B PROCESS	. . .	SECURITY OFFICER PROCESS	FILE 1	FILE 2	FILE 3	. . .	ACCESS FILE
USER A PROCESS					R	R	RWO		
USER B PROCESS						RA	RG		
USER C PROCESS					RW				
. . .									
SECURITY OFFICER PROCESS	Start Stop	Start Stop							RWA

R = Read; W = Write; A = Append; Start = Start Process; Stop = Stop Process; O = Owner; G = Grant Access

Reference Monitor Requirements

A reference monitor which meets the requirements described must implement a well-defined set of access restrictions or rules. In a secure computer system for military use, these rules are defined by the military security regulations. Thus it is necessary that the reference monitor refuse a user's process (as agent for the user) access to information unless the user is cleared for that information. In addition, it will be required that a user hold any formally defined special access permissions for information that his process attempts to access. Finally, the fact that a user is cleared and has the formal access required for information is necessary, but not sufficient, grounds to grant his process access to that information; the user must also have the "need to know" the information. Need-to-know is a concept tied to that of individual responsibility for classified information. In the computer system, it imposes the constraint that a user either be the originator of classified information (that is, that he have entered it into the computer himself), or that he be given access to the information by its originator or by another user authorized to grant further access to the information. In addition, of course, the user who is granted access must hold any required clearance and formal access permission.

The slide shows the first results of an attempt to translate the requirements stated above into a notation suitable for algorithmic implementation on a computer. The user's clearance must be greater than or equal to the classification of the information to be accessed, and the user's set of formal access permissions must contain (cover) the set of permissions required for access to the information. Finally, the access matrix of Lampson has been adopted to represent the system-wide set of need-to-know constraints. The matrix shows which users have access to which

collections of information and other users' processes, and the types of access allowed (e.g., read, append, grant further access, stop a process). The sample access matrix shown includes a security officer's process that has the privileges of stopping other users' processes and of operating on an access control file.

THE MITRE CORPORATION

COMPUTER SECURITY
R & D REQUIREMENTS

CENTRAL COMPUTER

PROJ.
VG. D72-V-606

SYSTEM BASE

- SELECTED HARDWARE REQUIRED
- SEGMENTED VIRTUAL MEMORY WITH PER-SEGMENT ACCESS CONTROLS
  - UNIFORM PROGRAM ENVIRONMENT
  - MANAGEABLE LEVEL OF CONTROL
  - RAPID CHANGE OF PROTECTION ENVIRONMENT
- MULTIPLE EXECUTION STATES
  - ISOLATE KERNEL,
  - OPERATING SYSTEM,
  - USER PROGRAMS

System Base

If a usable, secure computer system is to be implemented, the access control functions of the reference monitor must be identified, and a hardware/software system that can support (and be controlled by) the reference monitor in an efficient manner must be defined. The hardware requirements for such a system are particularly important, for to start with inadequate (or wrong) hardware, is to insure failure to achieve a secure and usable system. Three key points about the hardware base for a secure computer are identified on the slide.

A secure computer system must be built on hardware that is appropriate for security. It cannot be said that some set of hardware features is necessary (in the mathematical sense) for security, for any such hardware can be simulated on a Turing machine — or another computer. But practicality dictates otherwise. The simulation approach may be possible in theory, but it is likely to exact a significant cost in system performance. A more serious problem is that simulation of appropriate hardware is likely to require complex reference monitor software that will confound our attempts at certification. Fortunately, hardware with the features identified below is already becoming commercially available. It need only be specified before a purchase is made.

The key feature that is required of a processor for use in a secure computer system is support for a segmented virtual memory with access control on a "per-segment" basis. This feature is required for three reasons:

(1) In a segmented virtual memory system, a user's process accesses segments only. Thus, it is necessary to control only one path for access to information — the path between user process and segment. The implementation of system storage of segments on various media can be handled by the operating system (but largely outside the reference monitor) in a simple, uniform, and efficient way. In contrast, the more usual operating system requires separate access controls over the distinct paths from user process to drum, disk, tape, cards, etc. Even differing modes of access to the same medium may require different controls. Thus, segmentation will help define a small, certifiable reference monitor.

(2) In a segmented virtual memory system, a fine subdivision of access rights may be provided between processes, or between levels of privilege of a single process. For example, the reference monitor may be able to read and write a segment in a user's process, while other operating system programs are allowed only to read it, and the user's program has no access to the segment at all. In a model of the reference monitor, it should be possible to represent the access to this segment by various processes and levels of privilege, and to prove the access rights consistent with security. In contrast, a conventional computer protects most storage from the user program, but its operating system has full access to all of storage. Thus, to model the access controls in a conventional computer and opera-

ting system, each word (or character or bit) of storage must be represented separately. Such complexity would clearly preclude certification and the sort of modeling discussed on the next slide. Again, segmentation helps define a certifiable reference monitor in a manageable way.

(3) Finally, provision of access controls on a "per-segment" basis permits the reference monitor to provide different processes with different access to the same segment by rapidly switching the set of "segment descriptors" known to the processor. This organization facilitates the sharing of data by processes in a flexible way. In a system that provides access controls on a physical block basis, the reference monitor must inspect each storage block and "change keys" when a new process is given control, or when the segment (or page) population of memory is altered. This operation complicates the reference monitor (hindering certification) and slows its handling of key system transactions.

A second hardware feature that is necessary for the secure computer system is provision for multiple execution states with different levels of privilege. This feature permits protection of the security control software (kernel) that implements the reference monitor from the bulk of the operating system, and protection of the bulk of the operating system from user programs. The latter element of protection is not necessary for security, but is certainly required for reliable and effective system operation. The strategy

that is envisioned for designing a secure computer system involves allocating to the "kernel" only those functions that are necessary for security, and relegating to the operating system all other management functions. In this sort of system, it will be necessary to have efficient facilities for switching among user, operating system, and kernel. Thus, hardware support for multiple execution states will be necessary. The handling of multiple execution states must be effectively tied to the memory segmentation system, as indicated by point (2) above.

CERTIFYING AND BUILDING A SECURE SYSTEM

- IDENTIFY
  - REFERENCE MONITOR REQUIREMENTS
  - SYSTEM BASE
  - PROCESS OPERATIONS
- MODEL
  - REFERENCE MONITOR
  - SYSTEM BY LAYERS
- IMPLEMENT KERNEL
  - STRUCTURED PROGRAMMING
  - PROOFS OF CORRECTNESS
- WRITE AND PUBLISH SPECIFICATIONS

Certifying and Building a Secure System

Given the high-level reference monitor requirements and system base identified above, the problem is to design and certify a reference monitor, and to design an operating system to interface with it. In implementing a solution to the problem, a complete and formal statement of the reference monitor requirements that were outlined previously will be made. It will be assumed that the reference monitor is provided with user (process) identification and the classification and formal access restrictions of newly input information as external inputs. Then the operations that can be performed by a process to access data in our segmented virtual memory environment will be defined.

Given the definition of access operations, the mathematical statement of reference monitor requirements will be used to define a finite state model of the reference monitor and to identify rules that preclude its entering an unsecure state. Then the model will be expanded to reflect the required system operations using a series of levels to guide and structure the expansion. At each step of the expansion, it will be shown that the security of the basic finite state model has not been invalidated. The expansion will be guided from above by the statement of process operations and from below by the hardware organization. Intermediate levels of the expansion may reflect such operations as directory management, segment descriptor management, and page management. The expansion is complete when the hardware level is reached.

Once the model and associated proof are complete, the modeled reference monitor will be implemented in a software security kernel using structured programming and proof of correctness techniques to insure

correspondence between completed software and finite state model. An operating system may then be developed that calls on the kernel as needed and provides users' processes with a usable operating environment.

Finally, verified experience with the secure computer, kernel, and operating system will be translated into specifications. These specifications will allow users to buy, and vendors to build, certifiably secure, general-purpose computer systems.

THE MITRE CORPORATION

COMPUTER SECURITY R & D REQUIREMENTS

RELATED EFFORTS

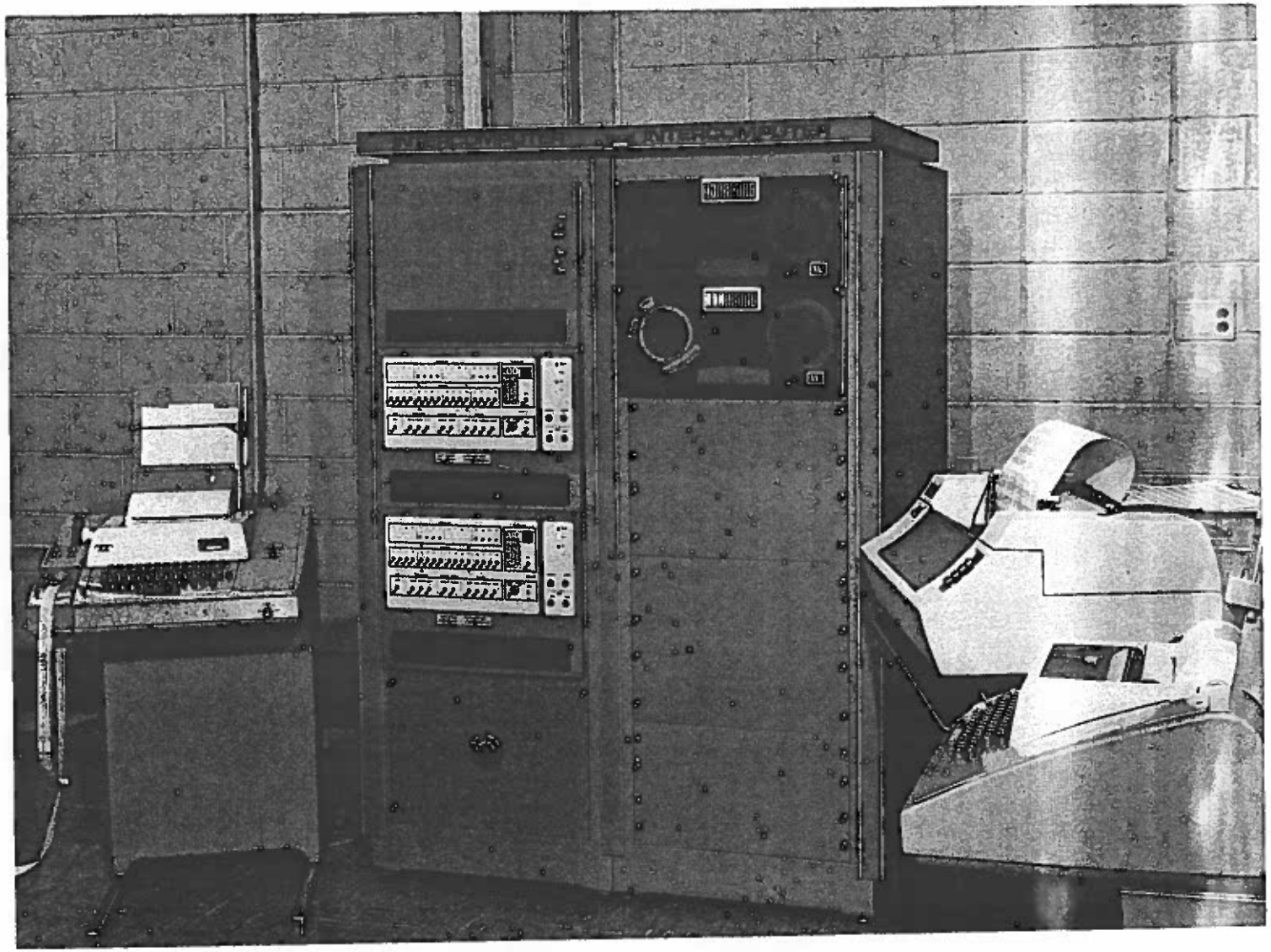
PROJ. VG. D72-V-605

- SECURE COMMUNICATIONS PROCESSOR TECHNOLOGY
- SATIN APPLICATIONS
- FRONT-END APPLICATIONS
- NETWORK APPLICATIONS

RELATED EFFORTS

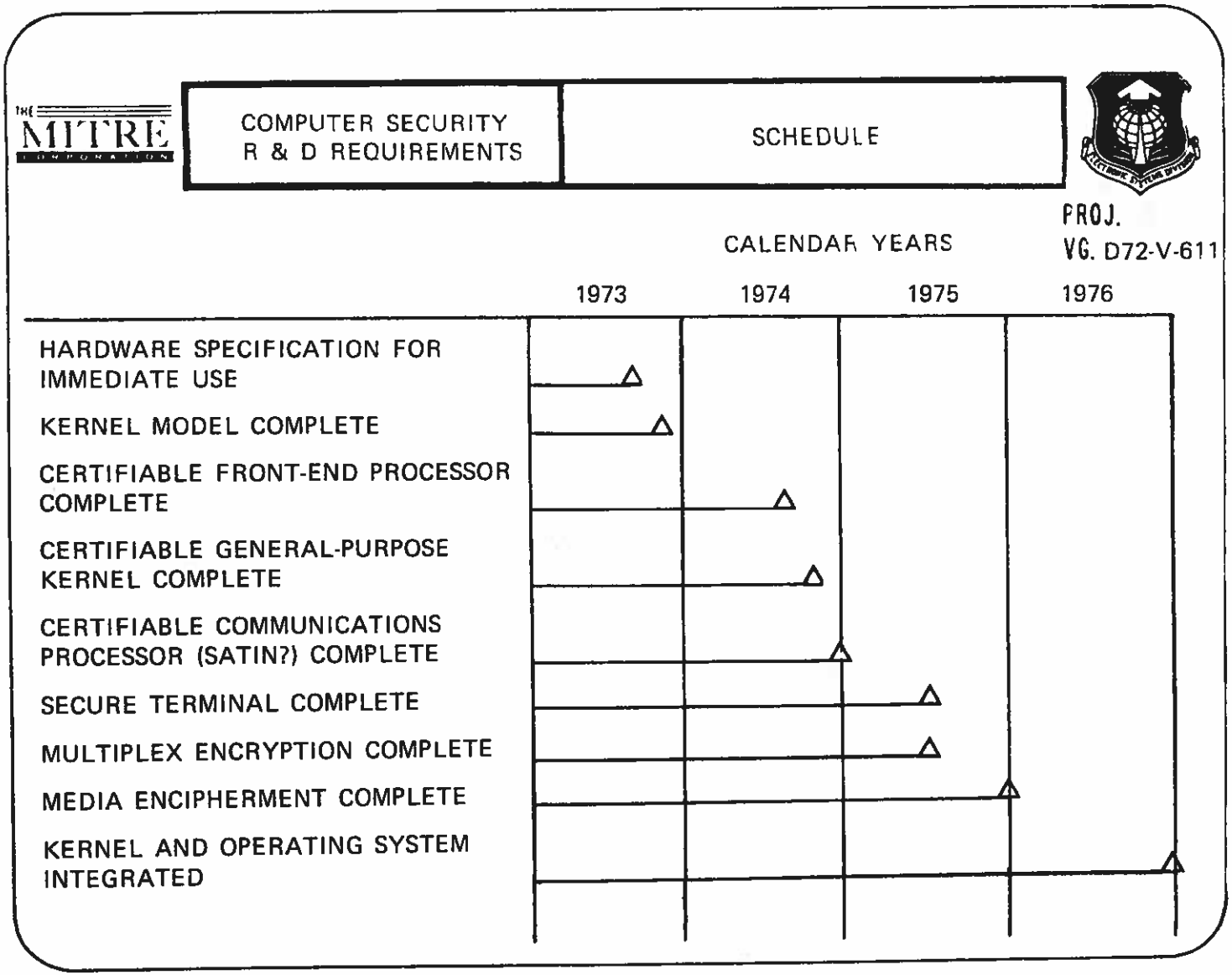
The preceding slides have identified major development objectives and approaches in the area of secure general-purpose computer systems. In addition to planning for these developments, MITRE and ESD personnel have undertaken the design and implementation of an experimental secure communications processor. The processor is a packet or message switch with access controls implemented through microprogramming. The general techniques identified by this effort are reflected in the development plans and technical approaches already discussed.

In addition to identifying general approaches, the secure communications processor effort has provided the personnel involved with the ability to design secure message switches for a variety of applications. The applications of such switches to the SAC SATIN network, as secure front-end processors, and for military computer and communications networks are now being explored.



Secure Communications Processor

This slide shows the Intercomputer i-50 that is being used to implement the experimental secure communications processor mentioned previously in the discussion. The two i-50 processors have been microprogrammed to implement restricted forms of segmented memory and multiple execution states. In addition, key elements of the processor's reference monitor are implemented in microcode. Thus, a wide variety of communications processor applications can be implemented by programs that are outside of the security perimeter. The experimental processor's microprogrammed access controls exact a noticeable cost in execution time, but microprogramming has provided the flexibility to experiment with security controls and determine requirements that can now be satisfied with better performance by processor hardware.


THE MITRE CORPORATION
COMPUTER SECURITY R & D REQUIREMENTS
SCHEDULE
PROJ. VG. D72-V-611
CALENDAR YEARS
1973
1974
1975
1976
HARDWARE SPECIFICATION FOR IMMEDIATE USE
KERNEL MODEL COMPLETE
CERTIFIABLE FRONT-END PROCESSOR COMPLETE
CERTIFIABLE GENERAL-PURPOSE KERNEL COMPLETE
CERTIFIABLE COMMUNICATIONS PROCESSOR (SATIN?) COMPLETE
SECURE TERMINAL COMPLETE
MULTIPLEX ENCRYPTION COMPLETE
MEDIA ENCIPHERMENT COMPLETE
KERNEL AND OPERATING SYSTEM INTEGRATED

SCHEDULE

This slide shows a projected schedule of major milestones in the computer security development activities. Where feasible, early guidance should be made available to users so that they can proceed with design and acquisition of systems without precluding the inclusion of security as it becomes available. Thus, specifications for computer hardware that will be compatible with reference monitor and security kernel concepts should be available quite soon. The mathematical model of the security kernel should be completed in late 1973, and a kernel based on this model a year later.

In 1974 it is planned to have available specifications for certifiable secure communications processors for both front-end and general message switching applications. The various cryptography-related developments (secure terminal, cryptomultiplexing and media encipherment) are projected for 1975. A general-purpose operating system using the certifiable security kernel should be complete and demonstrable in 1976.

THE MITRE CORPORATION

COMPUTER SECURITY
R & D REQUIREMENTS

SUMMARY

PROJ.
VG. D72-V-549

- NEEDS DEFINED
- R & D EFFORTS IN PLANNING AND UNDERWAY FOR USAF/DOD
- SOME APPLICATIONS IN PROSPECT

SUMMARY

In summary, then, MITRE and ESD personnel have defined military needs in computer security, have identified required developments and technical approaches, and have initiated some development activities. Attempts are being made to apply the solutions to Air Force problems as rapidly as possible. The prospects for solutions to many military computer security problems are good.

BIBLIOGRAPHY

Research in Secure Operating Systems

1) James P. Anderson, Computer Security Technology Planning Study, Draft ESD-TR, October 1972, James P. Anderson & Company, Fort Washington, Pa.

2) A. Bensoussan, C. T. Clingen, and R. C. Daley, "The Multics Virtual Memory: Concepts and Design," Communications of the ACM, Volume 15, Number 5 (May 1972).

3) Peter S. Browne and Dennis D. Steinaur, "A Model for Access Control," Proceedings of 1971 ACM-SIGFIDET Workshop, November 1971.

4) M. Gasser, Design of a Secure Communications Processor — Input Output Processor, ESD-TR 72-399, The MITRE Corporation, Bedford, Massachusetts.

5) G. Scott Graham and Peter J. Denning, "Protection Principles and Practice," AFIPS Conference Proceedings, Volume 44, SJCC (1972).

6) R. M. Graham, "Protection in an Information Processing Utility," Communications of the ACM, Volume 11, Number 5 (May 1968).

7) B. W. Lampson, "Dynamic Protection Structures" AFIPS Conference Proceedings, Volume 35, FJCC (1969).

8) B. W. Lampson, "Protection," Proceedings of the Fifth Annual Princeton Conference on Information Sciences and Systems, Dept. of Electrical Engineering, Princeton University (March 1971).

9) Michael D. Schroeder and Jerome H. Saltzer, "A Hardware Architecture for Implementing Protection Rings," Communications of the ACM, Volume 15, Number 3 (March 1972).

10) P. S. Tasker, Design and Certification Approach: Secure Communications Processor, MTR-2436, The MITRE Corporation, Bedford, Massachusetts.

11) C. Weisman, "Security Controls in the ADEPT-50 Time-Sharing System," AFIPS Conference Proceedings, Volume 35 FJCC (1969).