304

# DEPARTMENT OF DEFENSE
# COMPUTER NETWORK SECURITY:
# AN ASSESSMENT OF THE STATE OF THE ART

by

JAMES DAVID SCHARF

B.A., Purdue University, 1963

---

A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree of

MASTER OF SCIENCE

Department of Computer Science

KANSAS STATE UNIVERSITY
Manhattan, Kansas
1980

Approved by:

Virg Wallentine

Virgil E. Wallentine

# TABLE OF CONTENTS

## LIST OF FIGURES

# CHAPTER 1

# INTRODUCTION

## 1.1. REPORT OVERVIEW

This report will provide a managerial and user survey of those secure DOD computer networks currently in being and others for which research is being done, and will provide an assessment of DOD efforts with reference to current developments in computer network security. The report is based upon current literature, especially Department of Defense (DOD) computer network security implementation guides, as well as planned implementations and DOD areas of research in computer network security. There are some technical terms and concepts used, but a tutorial and a glossary are provided for the reader who may not be familiar with them.

The need for computer network security is particularly pressing within the DOD, since some of the DOD computer networks deal with classified information handling and many others carry information regulated by the Privacy Act of

1974. Some of the initial impetus in the computer security field and particularly in computer network security came from the DOD, and research is constantly underway to find a "trusted" computer network - something which has not been done to date. This report may be used by personnel both within and outside the DOD to provide computer network security sources and techniques already implemented as well as information on areas currently under research.

The technical scope of this report will not be sufficient for implementation of a secure computer network, but the bibliography will provide a basic framework plus a guide to other sources which will permit implementation, and these will be identified in the report.

## 1.2 DOD SECURITY POLICY

The Department of Defense (DOD) has set forth its security standards for resource-sharing computer systems, to include computer networks, in DOD Publication 5200.28, and has provided draft procedures for implementation in DOD publication 5200.28-M, entitled "Techniques and procedures for Implementing, Deactivating, Testing and Evaluating Secure Resource-sharing Computer Systems". These documents, augmented and refined by each of the departments and agencies within the DOD, provide the framework for the presently-established security levels for computer networks operated by and between elements of the DOD.

The objectives of the DOD computer security program which will apply to this paper are:

> 1. To implement secure resource-sharing automatic data processing (ADP) systems so that with reasonable dependability, deliberate or inadvertent access to classified material by unauthorized personnel or the unauthorized manipulation of the computer and its associated peripheral devices, which could lead to the compromise of classified information, can be prevented.
>
> (2) To develop, acquire, and establish methodologies, techniques, standards, and procedures for the design, analysis, testing, evaluation, and approval of the security features for resource-sharing ADP systems.

The DOD approach to computer security is a flexible approach, as much driven by current technology as by well-established requirements. DOD 5200.28-M contains the caveat that "rigid adherence to all techniques, methodologies, and requirements...could adversely impact upon the present and future use of the system under today´s rapidly changing ADP technology.".

## 1.3 CLASSIFIED vs. UNCLASSIFIED SYSTEMS

Paragraph 1-101b of DOD 5200.28-M states that the

"...manual is applicable to...all(DOD agencies)...which process, use or store classified data or produce classified information in resource sharing ADP systems.". The military services have largely interpreted this to exclude application of those provisions to systems which do not process classified information, with the result that a large number of DOD ADP systems and networks which handle unclassified data have only that security which the local site supervisor or his commander feels is necessary. This security ranges from none to some portion of that required by DOD 5200.28-M, with the result that some systems which process large amounts of cash or high dollar-value materiel are open to easy penetration.

The implementation of DOD 5200.28-M for classified systems requires the preparation of security checklists, as will be covered by Chapter 2 of this report. Although not required for sites processing unclassified information, a publication which provides comprehensive guidelines for computer facility physical security and risk management is Federal Information Processing Standards Publication 31 (FIPS31). Another very excellent publication on total ADP system security, covering all phases of operation, is the American Federation of Information Processing Societies

(AFIPS) System Reference Manual on Security (AFIP74). This manual covers topics such as personnel, physical, communications, organizational, administrative, and some ADP security and provides extensive checklists in each area covered. This document would be a valuable aid to both military and civilian computer installations in providing a ready means to check on security.

## 1.4 REPORT OUTLINE

Chapter 2 of this report contains some background on computer system and network security principles and will describe techniques used within the DOD to implement computer network security. Chapter 3 contains a discussion of some of the current areas of research which the DOD is undertaking to improve computer security and will provide sources of information on those research areas. Chapter 4 contains the author's assessment of both the effectiveness of current computer and network security as well as the direction of current DOD research with relation to the state of the art in computer network security. Appendix A is a glossary, compiled from several sources, of the more technical terms used in this report. The Bibliography for this report has been annotated, and the annotations will hopefully provide some assistance to the reader in locating references for the subjects covered.

# CHAPTER 2.

# PRESENT DOD IMPLEMENTATION OF NETWORK SECURITY

## 2.1. INTRODUCTION

There are several terms and concepts in computer network security which, if explained to the reader, will make the remainder of this paper more comprehensible and will establish a reference framework for some of the computer network security implementations and research that is described. Section 2.2 is a computer network security tutorial which establishes that framework. Some of the terms explained here are also defined in Appendix A, but the examples provided in this section will clarify the use of those terms in this report.

The remainder of this chapter presents DOD computer security implementation philosophy, provides a background for DOD computer network implementation, and describes current DOD computer network security procedures.

## 2.2. COMPUTER NETWORK SECURITY TUTORIAL

### 2.2.1. PRIVACY

Privacy is a concept which applies to people. With the advent of computers and their associated large data banks, a great deal of concern arose (and is still present) over how much information about an individual was in a particular data bank, how correct the information was, and who could get access to that data. As a result of this concern, particularly over personal information in Federal government files, Congress passed the Privacy Act of 1974 (PUBL74), which establishes the rights of individuals to review any records which contain personal information about them, to know which other agencies have been given this information, and to amend or correct any information that is necessary.

Although privacy is a term applying to people, it has had a vast effect on the methods by which data is stored and handled in computer systems. An Association of Computing Machinery monograph (HSIA79) outlines the computer security impacts of privacy:

> "The enactment of privacy legislation has several technical implications. Policies and procedures must be established to assure the <u>operational security</u> of the computer system. The <u>physical security</u> of the

> system must be maintained. The computer hardware must have features that augment security. Information transmitted to or from remote sites must be protected, possibly using data encryption. The operating system and the data management system must also have features to augment security."

These areas are naturally of great concern to the DOD, and the part of the purpose of this report is to outline some of the methods currently in use and under study to respond to the problems involved in protecting individual privacy. A good reference document for those involved with information systems affected by the Privacy Act of 1974 was written by Bushkin and Schaen (BUSH76).

### 2.2.2. SECURITY

Security is a general term used to describe the application and management of protection measures to computer systems and networks. Security has many facets, and some of these will be discussed in detail in this report. Data security, according to Hoffman (HOFF77), is "...the protection of data against accidental or intentional destruction, disclosure, or modification." Hoffman describes computer security as "...the technological safeguards and managerial procedures which can be applied to computer hardware, programs, and data to assure that organizational assets and individual privacy are protected." From a DOD computer security viewpoint (WASS77), automatic data processing (ADP) security includes:

> "...all hardware and software functions, characteristics, and features, operational procedures, accountability procedures, and access controls at the central computer facility, remote computer and terminal facilities, and the management constraints, physical structures, and devices, and personnel and communications controls needed to provide an acceptable level of protection for classified material to be contained in the system."

This rather involved DOD definition may be broken into the areas of personnel, organizational, physical, administrative, communications, and ADP security as will be described in other sections of this chapter. When approached from this viewpoint, security becomes a collection of large and interlocking procedures and disciplines which can protect a computer system or network from almost any threat, or at least enable reasonable recovery from the effects of a threat to the data or the facilities involved in processing it.

### 2.2.3. PROTECTION

Protection may be expressed in terms of the measures which are taken to provide security. It is the set of actual mechanisms available in hardware, software, procedures, and practices which enable security to be implemented. Examples of protection, some of which will be more fully described in Chapters 3 and 4 of this report, include the guards, locks, and alarms necessary for physical security; the manuals and other guidance which must be written for administrative and organizational security, investigations and security clearances which must be established for personnel security; the encryption devices and other protection necessary for communications security; and the myriad of existing and proposed techniques, such as data encryption, secure operating systems, and access control mechanisms which are required for ADP security.

### 2.2.4. COMMUNICATIONS ENCRYPTION

Communications encryption is one of the protection measures taken to insure communications security in a computer network or in any communications facility. It is implemented by separate pieces of encryption hardware which must be placed in the communications line to "scramble" transmitted signals and "unscramble" received signals in a network. These hardware devices are keyed to each other by various means, including physical switch settings on the equipment, insertion of a physically changeable keying device, and insertion of computer generated punched cards with random patterns of punches. In each case, the key which is set at one end of the communications link must match exactly the key set at the other end or communication cannot take place. This method provides very good assurance of authentication of the user at each end of the circuit, as the encryption key is generally complicated enough and/or is changed often enough to prevent any intercept and decryption by someone attempting to break in on the communications line.

There are two general methods of implementing communications encryption: the end-to-end method and the link method. These are illustrated in Figure 2-1. The end-to-end method has only two encryption devices on the commmunication circuit, and the signal remains encrypted as it passes through any intermediate communications control and switching facilities. The link encryption method may have a number of encryption devices protecting a single communications circuit, with the communication becoming readable in plain text at each facility and a new set of encryption devices handling each link in the system. This method is particularly applicable to systems which

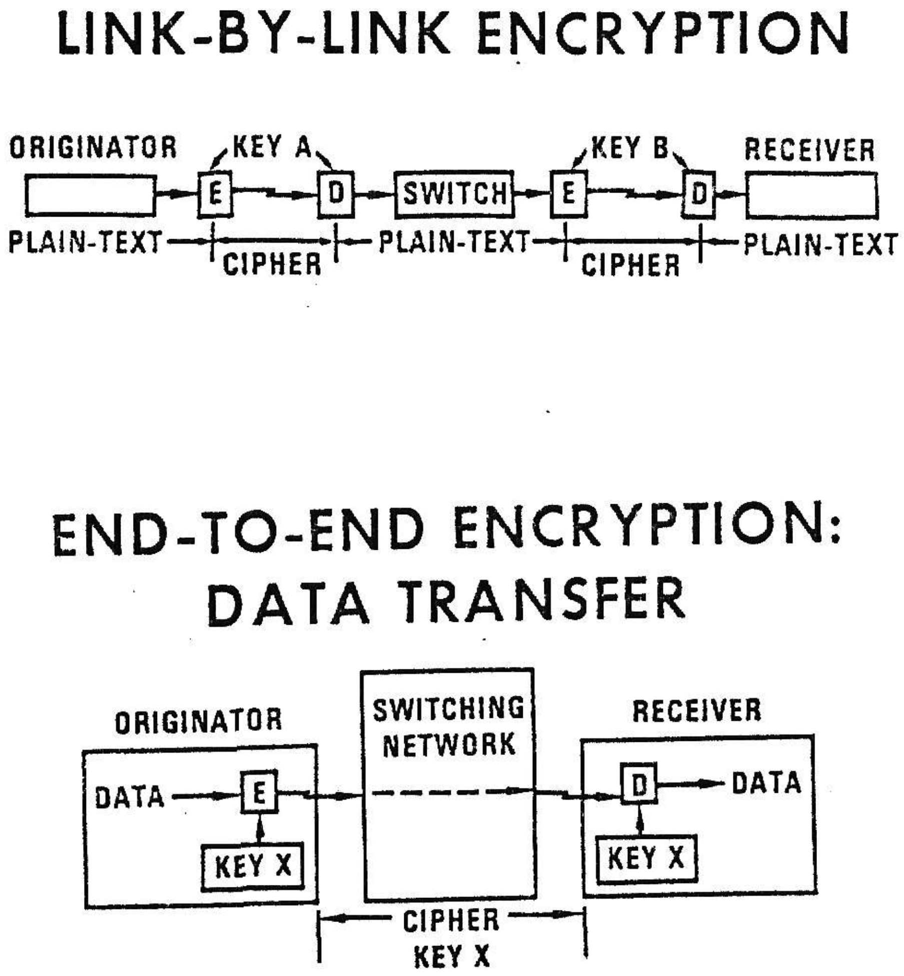


FIGURE 2-1

TWO GENERAL ENCRYPTION METHODS

pass more than one communication circuit over one link and which are required to switch individual circuits at an intermediate facility. Heinrich (HEIN78) lists the following advantages of end-to-end encryption over link encryption:

> "(1) Information is protected in intermediate switches as well as on the communication links. This also minimizes the authentication concerns for the switches.
>
> (2) Any misdelivered messages are unintelligible to the recipient.
>
> (3) The ongoing (properly deciphered) communication gives implicit and continual authentication of the two communicating devices."

Some DOD agencies which handle extremely sensitive compartmented information use a technique called super-encryption, in which both methods of encryption are implemented serially, providing end-to-end encryption for the contents of a message and link encryption for that portion of the message containing the routing information necessary to process the message through a network. This is a very expensive process, but it provides a level of protection for the information handled.

### 2.2.5. DATA ENCRYPTION

Data encryption is a new concept in protection mechanisms which may be implemented in either hardware or software. Uses to which data encryption may be put include encrypted storage of data in computer memory so that anyone not having access to the key may not read the data; authentication of messages over a network where only the recipient and the sender have a key to the message; and user or terminal authentication in a network where the user or terminal provides an encryption key upon access to the network. The characteristics of a good data encryption algorithm as presented by Browne and Branstad (ABRA77) are:

(1) that it provide a high level of Security,

(2) that it be unambiguous and understandable,

(3) that the design be publicly known and available,

(4) that it be flexible in its application to varying requirements, and

(5) that only the key to the algorithm be kept secret.

The National Bureau of Standards Data Encryption Standard (DES) meets these standards as it is applied to computer systems not processing classified information

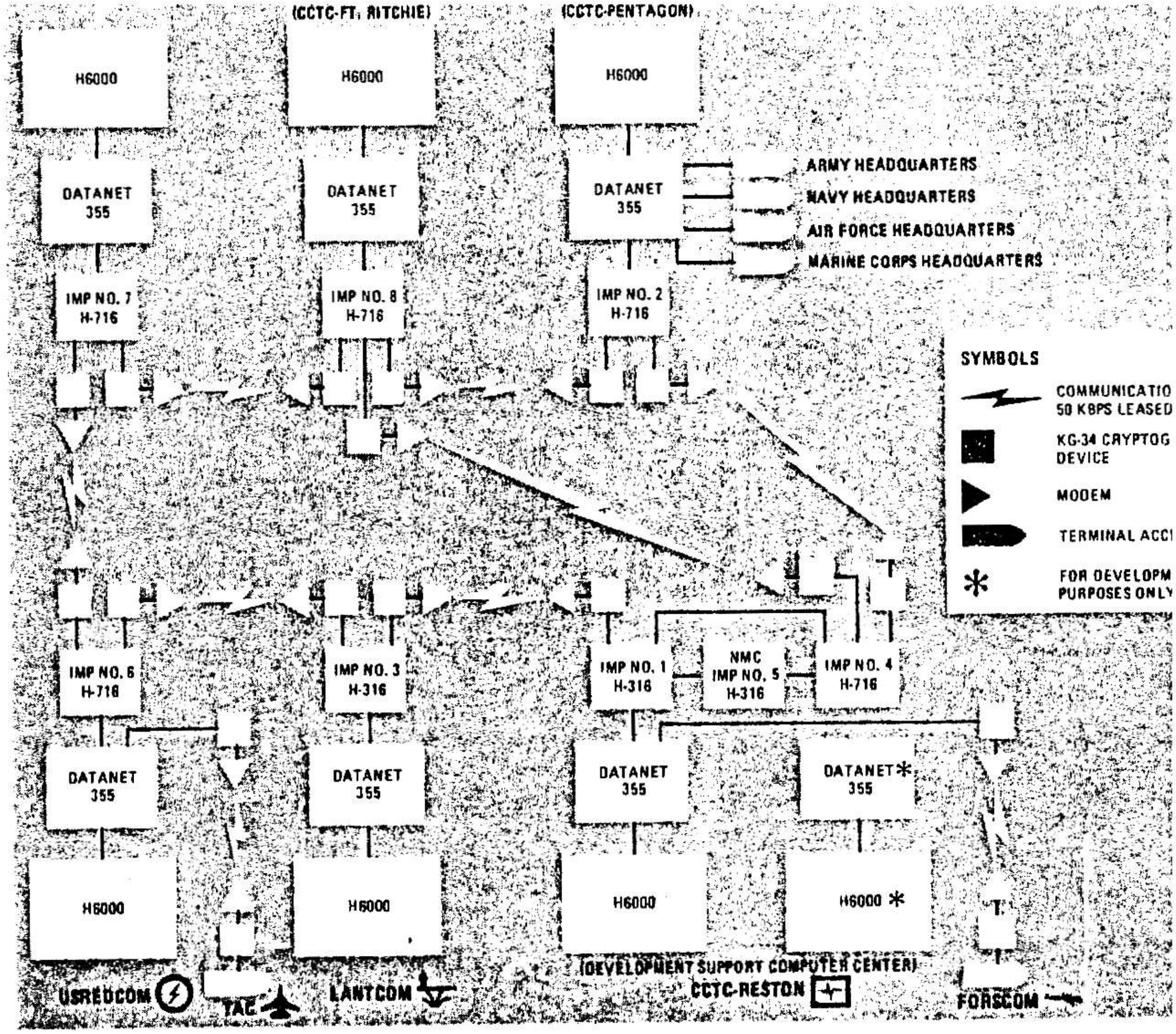


FIGURE 2-2
COMMAND AND CONTROL
PACKET SWITCHING NETWORK

pertaining to national security. A description of the DES is provided in FIPS Publication 46 (FIPS77).

### 2.2.6. PACKET SWITCHING

Packet switching is a communications concept which has been readily adapted to computer networks. The ARPANET, under the sponsorship of the Defense Advanced Research Projects Agency (DARPA) was the first practical implementation of a computer network using packet switching technology (SCHW77). An example of the packet switching network which is used by the DOD for command and control purposes is shown in Figure 2-2. Associated with each host computer node in the network is an interface message processor (IMP), which handles the "packeting" and switching of packets for the network. As messages are fed into the IMP from the host, the IMP divides the messages up into uniform packets and attaches packet sequencing information, packet error checking information, and message routing information to each packet. The packets are then sent out to the network by what the IMP determines to be the most direct route. If for some reason that route is not available, the IMP will send the packet to another IMP which is connected to the message destination. Not all packets of the same message will take the same route to get to their destination, but as they arrive at their destination, the receiving IMP again begins to assemble them in packet order to form a complete message, and transmits the message to the host when it is complete. This method was found to be faster and more reliable than trying to transmit a complete message over a single link, and is the basis for most of the computer networks which are operational in the DOD today.

## 2.2.7. ELEMENTS OF TOTAL SECURITY FOR COMPUTER SYSTEMS.

Although security is totally dependent on the implementation of the mechanisms which provide it and the willingness of the users of a secure system to adhere to the restrictions imposed upon them by the system, total security can be defined as a set of elements which assist the security manager in establishing a workable program. Excellent checklists covering all of the security components listed below are found in the AFIPS System Review Manual on Security (PATR74), and other sources are identified within the individual areas. As will be explained later in the "Security Algorithm", all of these parts contribute to total system security and may exist in varying degrees, but all _must_ be present in order for security to be effective.

### 2.2.7.1 Organizational Security.

This requires that the organization which is being provided the security must perform and document those checks required to insure effective implementation of the security system. Some areas to be covered under organizational security include:

- assigning PERSONAL responsibility for sensitive or classified assets.
- preparing "double-check" rules for all actions relating to sensitive or classified assets.
- preparing a security manual for guidance to all personnel.
- separating security duties among personnel to require collusion if intentional violation is to occur and to provide built-in "double-check" capability for normal operation.
- limiting tenure of personnel in security-related positions.

### 2.2.7.2 Administrative Security.

This is an area sometimes defined as providing classification for sensitive information items or establishing a hierarchy of protection for them. The formal area of security classification within the DOD (CONFIDENTIAL, SECRET, TOP SECRET, etc.) is included under administrative security. A table illustrating this hierarchy and its relationship to compartmented information is in Figure 2-3. This area is most often combined with organizational security, as the two are closely related.

### 2.2.7.3 Personnel Security

Personnel security requires that all personnel working with or using classified assets possess a properly verified security clearance equal to or higher than the classification of the material with which they work. In a civilian context, this loosely corresponds to the "bonded agent" concept, where individuals trusted with sensitive assets provide evidence of their trustworthiness before they are allowed to assume the duties of a sensitive position.

### 2.2.7.4. Physical Security.

Physical security covers not only the provision of those measures required to prevent unauthorized access to the facilities, but also those measures to prevent damage or

COMPARTMENTS

| | A | B | C |
|---|---|---|---|
| TOP SECRET | | | |
| SECRET | | | |
| CONFIDENTIAL | | | |
| UNCLASSIFIED | | | |

PARTIALLY ORDERED RELATIONSHIP:

TOP SECRET > SECRET > CONFIDENTIAL > UNCLASSIFIED

COMPARTMENTS A,B,C ARE MUTUALLY EXCLUSIVE

EXAMPLE:

User in Compartment B, Level Secret can have access to all information at Secret and below (e.g., Confidential and Unclassified) in that compartment, but no access to information in Compartments A or C.

POLICY IS NON-DISCRETIONARY - THE SECURITY LEVELS ESTABLISHED BY NATIONAL POLICY MUST BE ENFORCED.

FIGURE 2-3.
DOD SECURITY POLICY

Source: WALK78

destruction by natural or man-made accidents and those measures required for the protection of all of the support facililties (air conditioning, heat, fire protection, backup power, etc.). Comprehensive checklists for physical security appear in several sources (MART73, HEMP73), and are also addressed in the literature which covers specific areas such as power and air conditioning. The physical security comments in such sources as these are not designed specifically for computer facilities, but they may be applied and should be considered.

2.2.7.5. Communications Security.

This area covers the provision of proper encryption for any communications lines which may go out of the computer facility as well as the establishment of procedures to detect, measure, and prevent or mask any spurious electronic radiation which may exist at the computer facility. This communications security also includes cognizance of the configuration of any network into which the computer is connected. Network configuration control is particularly difficult, as rapid advances are presently being made in computer networking capabilities. Abene (ABEN77) addresses communications encryption techniques.

### 2.2.7.6. ADP (or EDP) Security.

ADP security concerns itself with the security of the actual computer-related areas of software, hardware, data, and the operations performed on them. There are five basic functions of ADP security, defined as follows:

Identification.

Each element of a computer system must have a unique identifier within the system. Unique identifiers must be provided to all users of the system, all terminals connected to the system, and all applications programs, systems processes, and all data files of the system. The other elements of ADP security cannot be provided effectively without this unique identification.

Isolation.

The computer system must effectively isolate all elements of the system from one another unless specific interaction between elements is directed. Isolation extends to all system users, terminals, programs, processes, and data files. The design principle of "default to no access" helps to enforce isolation.

### Integrity.

Prevention and detection of undesirable actions or events as well as minimization of damage to data are primary considerations in integrity. Recovery and reconstruction procedures must be designed to cover those occasions when data is lost or altered.

### Access Control.

Access control, implemented through positive identification of system assets, provides the isolation necessary for good ADP security. File access privileges (read, write, modify, etc.) must be closely controlled, as must access to the various classification levels of the system. Multi-level security is still an unsolved problem in computer systems, although much more control is available now than in the past. User security profiles and system authorization tables are some present means of establishing access control.

### Surveillance.

Surveillance may be divided into two areas: preventive and detective. Preventive surveillance consists of threat monitoring and risk analysis - "insuring that there are locks on the door". Detective surveillance is the establishment of performance monitoring subsystems and audit trails to determine the existence of anomalies in the system and to find the source of these anomalies. Performance monitoring will often show arrests in the system, and audit trails should enable security personnel to trace the source of the breaks. Many computer systems have little or no surveillance facilities available.

### 2.2.8. ALGORITHMIC REPRESENTATION OF COMPUTER SECURITY

Although not quantifiable, the following "security algorithm" represents one method of viewing the interaction between the various aspects of computer security. The algorithm expresses security as a multiplicative function of the six components which were previously described. The function, f, is expressed as:

$$S = f(P1 * O * P2 * A * C * E),$$

where

S is total system security,
P1 is personnel security,
O is organizational security,
P2 is physical security,
A is administrative security,
C is communications security,
E is EDP security .

Each element of the algorithm may be thought of as varying between 0 and some weighted value determined by the approving authority for site security, with 0 providing no security and the upper bound providing the maximum amount of security possible for the site. It is easily seen from the multiplicative nature of the algorithm that if any one area is totally deficient, there is no system security, and the less security that is provided in each area, the larger the effect will be on the total system.

### 2.2.9. SECURITY DESIGN PRINCIPLES

Lance J. Hoffman (HOFF77) provides a list of five security design principles which he terms as applicable to the design of both computer and non-computer systems, he claims that adherence to these principles will reduce the number and severity of security faults which occur.

The first of these principles is default to access denial. Users must justify their need for access to a system, catalog, or file before access may be granted. As Saltzer (SALT74) points out, design or implementaion breakdowns will result in access denial, a safe situation for system integrity rather than in unauthorized access and possible compromise of information contained in the system.

The second principle is that of nonsecret design. Dr. Willis Ware (WARE79) uses the analogy of a combination lock to describe the principle. The design of the lock, its mechanical functions, and the method by which it is opened may all be published without compromising the security of the lock. The numbers for the combination (the "arming parameters") are kept secret, thus the security of the lock´s function is maintained. Exposing the design of a secure computer system to as many talented minds as is feasible will aid in the identification of bugs and enable the designer to eradicate them before the system is implemented. If the security provisions are kept secret, they are often inadvertently or purposely discovered by browsers or penetrators, and a breach of the system occurs. Dr. Ware (WARE79) also maintains that certification of software is essential for the introduction of nonsecret design. If software cannot be certified in some manner, it is not secure enough from possible penetration to have the design unclassified.

The third of Hoffman's principles is user acceptability. A security system which is complex and hard to use or time consuming in its implementation will be subverted by its users. Hoffman uses the analogy of bypassing of interlocking automobile ignitions and seat belts by large numbers of dissatisfied users when they get into their cars. The human interface must be as simple, natural, and easy to use, or users will bypass it and thus render the security system ineffective. An example of this is a complicated handshaking routine involving one or more randomly generated, long, alphanumeric passwords. Users of this type of system tend to write down the entire routine, complete with passwords, and carry it in their wallets or (worse yet) tape it up somewhere near their terminal access to the system.

Fourth is the principle of complete mediation. Every time a user of program ("subject") on the system attempts to access any system resource - files, operating system functions, other users programs, etc. ("objects"), that subject's authority for access must be checked. A repeated access to an object by a subject cannot depend on "remembered" access authority, but must be rechecked upon repeat access.

The last principle is that of least privilege. All subjects on a system should be examined to insure that the system privileges given them with respect to an object are enough to accomplish an assigned task and no more. A user who only has the need to read the contents of a file should not be given the privilege of modifying the file structure.

## 2.3. CURRENT DOD SECURE COMPUTER NETWORK IMPLEMENTATION PHILOSOPHY

DOD implementation of computer networks came about more as the result of necessity than of design. Although much design work went into the formation of the existing DOD computer networks, many of the networks were formed from hardware which was already installed and software which was in current use for production work. Thanks to the constant DOD emphasis on standardization, most of the systems which were implemented had homogeneous hardware and at least a partially common set of systems and applications software. Unfortunately, this standardization did not extend outside the design of individual systems, so there is very little standardization in the design and implementation of even systems which perform similar functions within the same branch of service of the DOD.

Examples of computer systems which were first implemented as individual sites with standard hardware and some standard software are the Worlwide Military Command and Control System (WWMCCS), which uses Honeywell 6000-series computers and DEC PDP-11 series minicomputers; the Community On-line Intelligence Networking System (COINS), which is implemented on the DEC PDP-11 series; and the US Army Forces Command operations network and WWMCCS Entry System, which is a nationwide network of terminals and concentrators connected to the Honeywell 6000 computer at the US Army Forces Command headquarters in Atlanta, Georgia. This network may be selectively connected through a communications facility to the WWMCCS network, which will be described in detail in the next section of this chapter.

Even these systems, however, were allowed the development of site-specific applications for their systems, both in operating system software and in applications software. Some systems, such as the US Army Tactical Fire Direction System (TACFIRE) and the prototype Division Level Data Entry System (DLDES) in use at Ft. Stewart, Georgia, were developed with network design as one of the design criteria, and software changes are limited to those promulgated at the system level; the users are allowed no site-specific modifications.

The prevailing network security philosophy in the DOD and the only one which can be certified for implementation at present is the establishment of a benign environment system envelope which encompasses every portion of the network to be secured. All computer centers, every remote device connected to the network, all users, and all software must be protected at the level of classification established for the most highly classified portion of the network. All communications links in the network must be protected with approved communications encryption devices which meet the required level of classification. Some links in the system are super-encrypted for the protection of compartmented information. This super-encryption is strictly in the communications processes at present, although research is being conducted in the use of data encryption techniques for this purpose.

## 2.4. BACKGROUND FOR DOD NETWORK IMPLEMENTATION

The DOD has several secure computer networks, but the configuration and methods of operation of most of them is classified, as they support the national intelligence missions of the various departments of the DOD. The Worldwide Military Command and Control System (WWMCCS), however, uses a computer network in support of the operational role of the DOD and the configuration and much of the methods of operation of this network are unclassified and will be used in this report as an example of current DOD computer network security implementation.

As background, WWMCCS facilities around the world provide a means for the Joint Chiefs of Staff (JCS) to exercise daily control over deployed US military forces both in crisis and non-crisis situations. WWMCCS consists of over 35 Honeywell 6000-series computers located at sites throughout the world wherever a significant number of US forces are stationed. Most of these computers operate in a stand-alone mode with information fed into them by manual means or by removable magnetic media which can be transported between sites. WWMCCS also includes an extensive communications network which is the prime means of control for the JCS. This communications network provides the redundant circuitry necessary to insure constant control, and it is tested continuously to maintain its configuration.

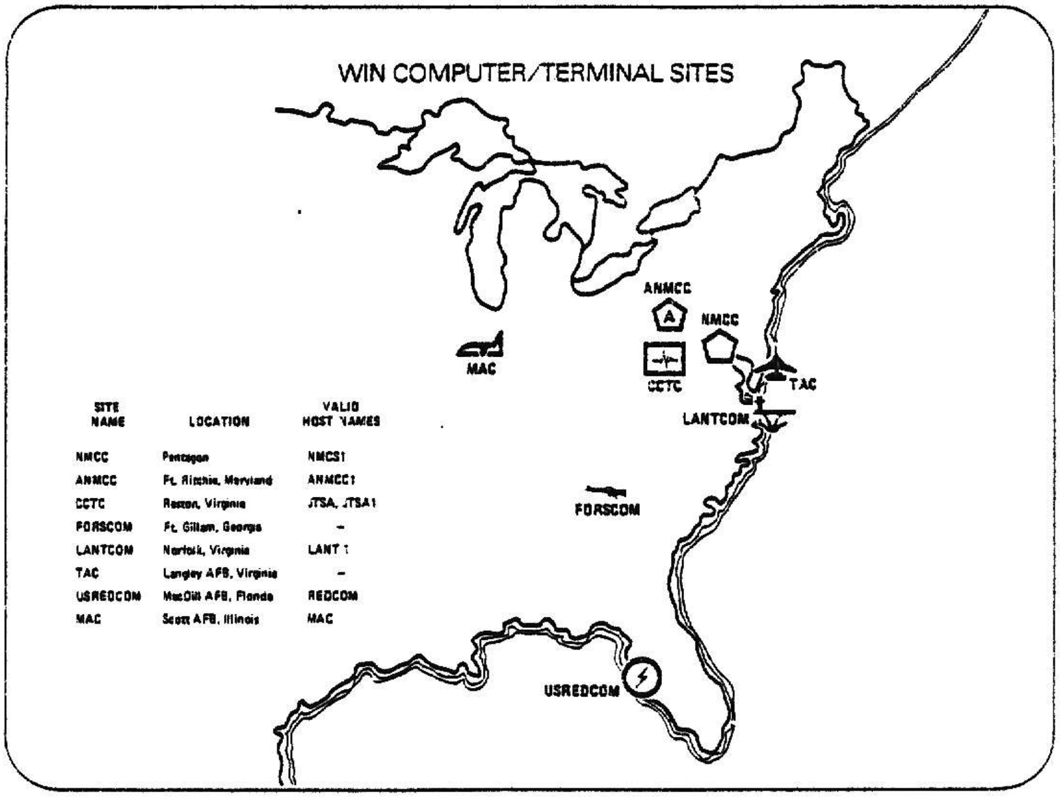
In September 1971 the JCS (JCSM71) identified the need for "...faster and more accurate information flow in support of crisis management actions and for continuity of operations of the National Command Authorities...". The solution which was proposed for this need was a network of the computers which comprised the heart of the WWMCCS operation. A development plan (JCSM75) for this network was written in 1975, and a prototype network was designed which included three of the WWMCCS computers in the Washington, D.C., area. This network was later extended to the locations shown in Figure 2-4, and two operational experiments were conducted in 1976.

In July 1977 the JCS approved and validated the the operational requirement for WWMCCS computer internetting, and the WWMCCS Intercomputer Network (WIN) was established. The WIN consists of a set of independent computer systems that are interconnected as shown in Figure 2-5. The network uses the ARPANET packet switching technology for handling intercomputer transactions. Each host computer in the system uses a communications front-end minicomputer to handle transactions with both local users and the interface message processor (IMP). The IMP provides the packet switching capability for the network, and a special configuration of the IMP at Reston, Virginia, allows it to monitor and collect statistics on the entire network. The main trunks in the network, indicated by the numbered lines in Figure 2-5, are 50,000 bit per second commercially leased communications lines which are specially conditioned for data transmission. There is an on-going effort to expand this network to include as many of the WWMCCS sites as possible, both in the continental United States as well as in the European and Pacific theaters of operation.

# ILLEGIBLE DOCUMENT

THE FOLLOWING DOCUMENT(S) IS OF POOR LEGIBILITY IN THE ORIGINAL

THIS IS THE BEST COPY AVAILABLE



| SITE NAME | LOCATION | VALID HOST NAMES |
|---|---|---|
| NMCC | Pentagon | NMCS1 |
| ANMCC | Ft. Ritchie, Maryland | ANMCC1 |
| CCTC | Reston, Virginia | JTSA, JTSA1 |
| FORSCOM | Ft. Gillem, Georgia | – |
| LANTCOM | Norfolk, Virginia | LANT 1 |
| TAC | Langley AFB, Virginia | – |
| USREDCOM | MacDill AFB, Florida | REDCOM |
| MAC | Scott AFB, Illinois | MAC |

FIGURE 2-4
WWMCCS COMPUTER NODE LOCATIONS

THIS BOOK CONTAINS NUMEROUS PAGES WITH DIAGRAMS THAT ARE CROOKED COMPARED TO THE REST OF THE INFORMATION ON THE PAGE.

THIS IS AS RECEIVED FROM CUSTOMER.

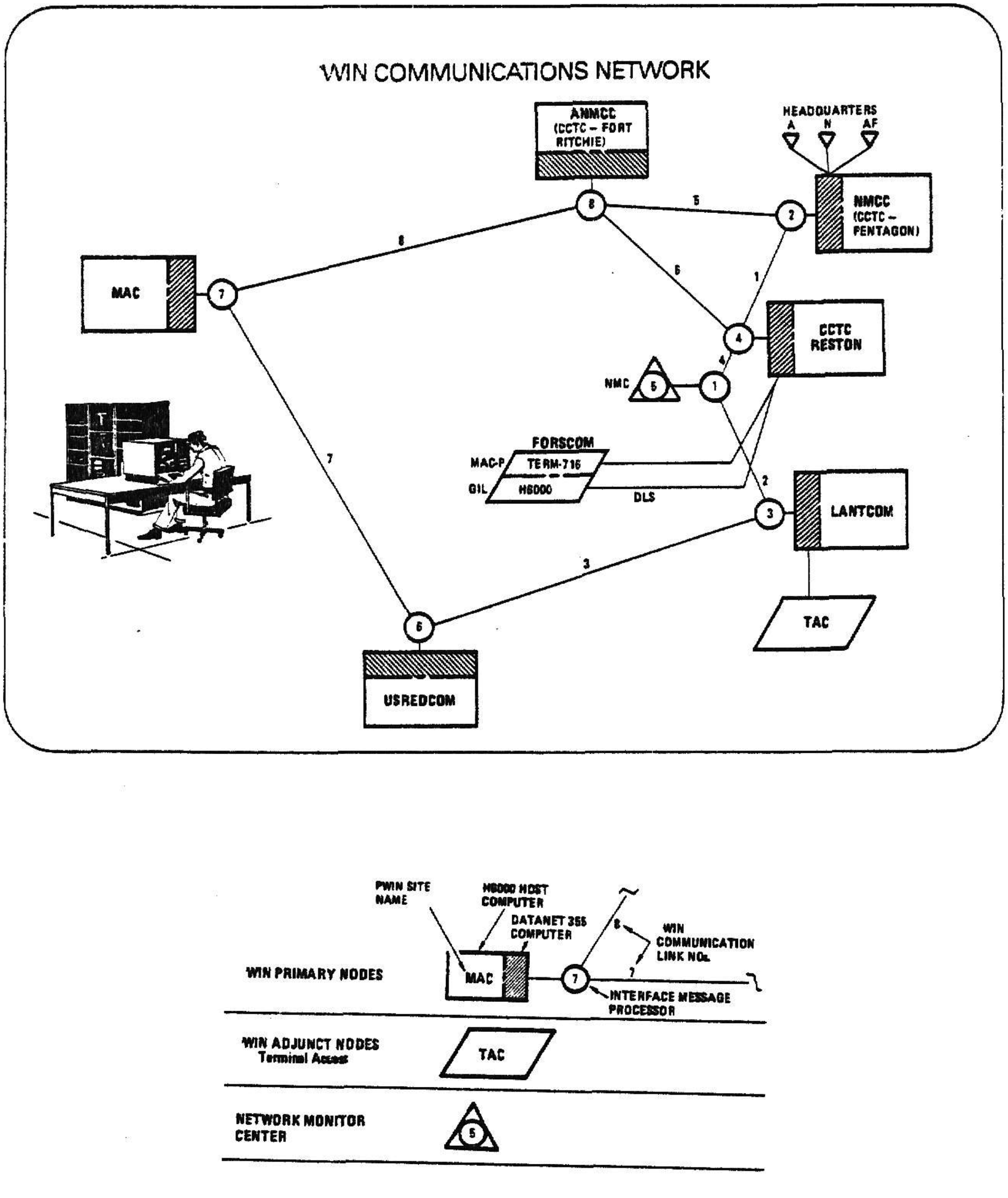


FIGURE 2-5
DOD COMPUTER NETWORK
INTERCONNECTION SCHEME

## 2.5. NETWORK SECURITY PROCEDURES

The WWMCCS ADP System Security Officer Manual (WASS77) describes all of the security measures to be taken in establishing the benign system envelope for the WIN. This section will use those measures to establish a reference framework for computer network security as it is currently implemented within the DOD.

### 2.5.1. ORGANIZATIONAL AND ADMINISTRATIVE SECURITY

Each computer site in the WWMCCS is required to have its own full-time WWMCCS ADP System Security Officer (WASSO), whose responsibility is to insure that the WWMCCS security provisions are carried out at that site. The WASSO is not only the security manager for the site, but (s)he is also the lead technician in establishing site security. The qualifications for appointment as a WASSO include security training, experience as a systems software programmer, experience in computer facility operations, and completion of the Honeywell GCOS (systems software) analysis course for the H6000 series computers. Each site which is remote from the central computer facility of a WWMCCS site is required to have an individual appointed who is responsible for the security of that site. Although this individual does not work directly for the site WASSO, (s)he obtains all needed security guidance from the WASSO and deals directly with the WASSO on any security problems that might arise.

The creation, dissemination, control, and destruction of of classified information within the DOD is regulated by a DOD-level directive (DODD73) along with supplementary regulations published by each of the departments and agencies of DOD. The hierarchy of classification shown in Figure 2-3 is promulgated in DODD73, and the department and agency regulations refine this directive and provide for compartmentation of information as needed. Special instructions for handling computer generated classified material within the WWMCCS are contained in WASS77 and in similar documents for each of the DOD departments and agencies. Much of the guidance and part of the checklists provided in WASS77 have been incorporated into the other military services computer security documents.

### 2.5.2. PERSONNEL SECURITY

The DOD personnel security program is a long-established program which requires extensive background investigation before a security clearance can be granted. The WWMCCS benign environment is protected in this area by the requirement for individuals to have a Top Secret security clearance before a user account on any part of the WWMCCS can be initiated. Physical access to any part of a WWMCCS computer facility, including remote terminal areas, requires a properly cleared escort if the individual requesting access does not have an adequately verified Top Secret clearance.

### 2.5.3. PHYSICAL SECURITY

Physical security provisions for the WWMCCS provide a large portion of the benign environment which has been established. DOD-level security guidance (DODP73) and WWMCCS regulation (WASS77) specify physical security requirements, which include vault-type operations facilities, guards, access control lists, alarms, etc. Almost all of the physical security requirements discussed in FIPS74, MART73, and PATR74 are implemented for the WWMCCS.

### 2.5.4. COMMUNICATIONS SECURITY

Communications security is established for the WWMCCS by implementation of communications encryption measures and regulation of compromising emanations. DOD approved communications security encryption devices are used on every link in the WIN which extends outside a physically secured area. Protected wireline distribution systems are used within the security control zone, and all communications facilities comply with established RED/BLACK separation requirements (MILH75). Encrypted and plain-text signals are electrically separated, and isolation devices in the facilities provide electrical isolation of even the encrypted signals until they have left the interface. Control and switching of all WIN computer assets and peripherals is accomplished by a small technical control facility established within the Top Secret control zone of the computer facility.

### 2.5.5. ADP (OR EDP) SECURITY

The GCOS III operating system used throughout the WWMCCS has been proven to be insecure from a penetration viewpoint (CARL75, LIND75), but the benign environment which has been described previously protects the security of the system as a whole to the point that it may be certified for operation at the Top Secret level. There are various security precautions taken from an operating system viewpoint which enhance the security of the system, but none of them are foolproof.

Some of these precautions (WASS77) include assignment of unique system user identifications (USERID) and passwords; passwords of eight characters which are randomly generated; frequent changes of passwords; and an audit trail system which provides the system security personnel a very good means to track user activity through the system. Unfortunately, this audit trail system is not real-time, but a system of checks and alarms to the security console of the system gives a real-time indication of arrests such as system log-on violations, file access violations, and attempts to perform privileged functions.

Data encryption is not used in the WWMCCS system. The operating system protection of files and programs provides sufficient isolation for normal users, and, since all users are required to possess a Top Secret clearance, any inadvertent release of information would not result in a security compromise. The other reason that data encryption is not used within WWMCCS is that there is no DOD-certified method of encrypting data which may be implemented at the Top Secret level.

# CHAPTER 3.

# DOD COMPUTER NETWORK SECURITY RESEARCH

## 3.1 CURRENT DOD SECURE SOFTWARE REQUIREMENTS.

A large area of on-going research in the DOD concerns certifiably secure software and its uses in developing secure and trusted operating systems. Because of the emphasis on establishing multi-level security and thus being able to dispense with the benign environment or "system-high" concept of operating a secure ADP system, the DOD has expended large amounts of resources in the development of securable, certifiable software. The DOD Computer Security Initiative was established in 1978 by the Assistant Secretary of Defense for Communications, Command, Control and Intelligence (C3I) to achieve the widespread availability of trusted ADP systems for use within the DOD. Mr. Steven T. Walker, Office of the Assistant Secretary of Defense (C3I), described the DOD Computer Security Initiative in an address (WALK79) to the Second US Army Automation Security Workshop in September 1979. He stressed that widespread availability implies the use of commercially developed trusted ADP systems wherever possible. He was careful to delineate between "trusted" and "secure" ADP systems, stating that the DOD already has secure ADP systems because of the benign environment established for them, but that the systems still could not be trusted to know who needs what information. In his address he reviewed the progress of the DOD Computer Security Initiative and described the current interaction with computer manufacturers and their progress in implementing trusted computer systems. He identified the three critical elements of the DOD Computer Security Initiative as:

> (1) the effective demonstration of the technology for building usable trusted ADP systems;
>
> (2) a mechanism for approval of trusted ADP systems instead of the ad hoc, case-by-case, independent system approval means presently used; and
>
> (3) vendor involvement in security development to spread the availability of trusted ADP systems.

He pointed out that today's approval methodology provided no technical assistance for the Designated Approving Authority (DAA) other than that available in his organization. Under the DOD Computer Security Initiative, certification techniques for design and implementation will be developed and a single, central, DOD "laboratory" will be designated as the technical approving authority. This laboratory will develop an "evaluated product list" of hardware and software to be furnished to the DAA, who may then apply site-specific threat and risk analyses to select the level of protection required. Walker pointed out that specifications for trusted ADP systems are still being defined as to levels of trust involved and operating environments to be designated. When these specifications are coordinated through the DOD and its departments and agencies and are approved (tentative estimate is 1982), a single DOD agency will be designated or created to be the trusted ADP system laboratory. This agency would possibly be modeled after the Electromagnetic Communications Analysis Center (ECAC) which is the DOD agency providing coordination of electromagnetic frequency spectrum use for all agencies and departments of the DOD.

## 3.2 SECURITY KERNEL DEVELOPMENT

The primary area of development for secure software is the security kernel approach. Steven Walker also has written extensively on this approach (WALK78) and provided quite a good background leading to its development. A chronology of the development of the security kernel and some of the interaction involved is shown on the chart at Figure 3-1. Walker's background indicated that early research efforts (1968-1974) organized "Tiger Teams" to penetrate the access control mechanisms of existing operating systems. These teams succeeded in subverting every commercial operating system that they attempted. Evaluations of some of these penetrations may be found in ATTA74, KARG74, LACK74, CARL75, and FLAT76. One of the methodologies used in the penetrations is explained in LIND75. The research community was so concerned with the ease with which these systems could be broken that a major effort was organized to inform the public of the vulnerability of computer systems. It is the author's opinion that there is still a large percentage of senior managers, both within the DOD and outside of it, who are unaware of the vulnerability of computer systems. As was stated in Chapter 1 of this report, computer system security is very low except in the cases of computer systems which handle classified information, when they meet the standards of secure computer systems through the establishment of a benign environment.

```
------------------------------------------------------------------
       ESD/MITRE
1973   SECURITY MODEL &
       SECURITY
       KERNEL
         :
---------:--------------------------------------------------------
         :       MULTICS    UCLA
1974     :          :       SECURITY
         :          :       KERNEL
         :          :          :
---------:----------:----------:----------------------------------
         :          :          :      HONEYWELL
1975     :          :          :      SECURE
         :          :          :      COMMUNICATIONS
         :          :          :      PROCESSOR
         :          :          :        :
---------:----------:----------:--------:-------------------------
         V          :          V        :
        SECURE      :        SECURE     :            SYSTEM
1976    UNIX        :        UNIX       :            DEVELOPMENT
        PROTOTYPE   :        PROTOTYPE  :            CORPORATION
                    :                   :            KVM/370
                    :                   :               :
--------------------:-------------------:---------------:---------
                    V                   V               :
                FORD                   HONEYWELL        :
1977            AEROSPACE              LEVEL 6          :
                KSOS-11                HARDWARE         :
                    :                  IMPLEMENTATION   :
                    :                   :               :
--------------------:-------------------:---------------:---------
                    V                   V               V
                DOD KSOS               KSOS-6          DEVELOPMENT
1978            CONTRACT               INTERNAL        ON
                                       DEVELOPMENT     ITEL AS/5
------------------------------------------------------------------
```

FIGURE 3-1.
SECURITY KERNEL DEVELOPMENT CHRONOLOGY.

Walker goes on to say that in the early 1970's the Air Force Electronic Systems Division (ESD) conducted in-depth analyses of the requirements for secure systems (ANDE72). The concepts which emerged from their efforts are today the basis for most major secure computer system developments. The basic concept is a Reference Monitor or Security Kernel which mediates the access of all active system elements (people or programs) referred to as subjects, to all system elements containing information (files, records, etc.) referred to as objects. A good technical description of this concept is provided in LIND76, and an example of a protection matrix within the kernel using this concept is in Figure 3-2. In the example, the protection matrix establishes privileges for User "B", a systems software analyst, far in excess of those given to User "A", an applications programmer. The protection matrix can also establish privileges for programs, such as the Editor Command module in the example, to insure that they act only within the purview of their established limits. Matrices of this type are established for all subjects and all objects which must interact in the system, and they are contained within the security kernel to preserve their integrity. All of the security relevant

| OBJECTS<br>SUBJECTS | TIME SHARING SUBSYSTEM | EDITOR | FILE A1 | FILE B1 |
|---|---|---|---|---|
| USER "A" | ENTER | ENTER | CREATE<br>DELETE<br>READ<br>WRITE<br>EXECUTE | EXECUTE |
| USER "B" | ENTER<br>MODIFY | ENTER | READ<br>WRITE<br>EXECUTE | CREATE<br>DELETE<br>READ<br>WRITE<br>EXECUTE |
| EDITOR COMMAND MODULE | ENTER | READ | | |

FIGURE 3-2.
PROTECTION MATRIX ACCESS DIAGRAM

decision making functions within a conventional operating system are collected into a small, primitive but complete operating system known as the security kernel. The three essential characteristics of this kernel are:

(1) that it be complete (i.e., that all accesses of all subjects to all objects be checked by the kernel),

(2) that it be isolated (i.e., that the code that comprises the kernel be protected from modification or interference by any other software within the system), and

(3) that it be correct (i.e., that it perform the function for which it was intended and no other function).

The reference monitor system and the formal methodology employed in its development were described in a 1978 Congressional report submitted by the General Accounting Office (CONG78). Since these Air Force studies were completed, considerable effort has gone into building security kernels for various systems. The reference monitor concept was the basis for work by Massachusetts Institute of Technology, the MITRE Corporation and Honeywell Information Systems in restructuring the MULTICS operating system (SCHR77). MITRE and UCLA have built prototype security kernels for the Digital Equipment PDP-11 minicomputer system (WOOD77, KAMP77). System Development Corporation (SDC) is at this time building a security kernel for the IBM VM370 operating system (GOLD77).

Walker further states that a difficult challenge for computer security researchers has been how to effectively demonstrate secure systems concepts. One way is to build a neB operating system from scratch, but development of this type with all the necessary support tools is a complex and expensive operation, and often too difficult for limited computer security research budgets. The alternative approach of patching flaws in an existing system to provide add-on security (the "patch and pray" methodology, as described by DeLashmutt (DELA78)) is known to be unsuccessful, with patches often causing more flaws than they correct.

The ideal solution would be to create a new secure operating system with the external appearances of an existing operating system so that the existing support software and applications programs could be used without modification. The secure operating system would be a completely new system but it would emulate the external characteristics of the existing operating system. Walker maintains that the most difficult aspect of this approach is finding an operating system to emulate whose user interface will not be severely altered by the process of creating the secure system. Any primitive user functions on a system which cannot be performed in a secure manner must be eliminated or restricted in the secure version of the system, and these changes alter the compatibility of the operating system with its environment. Most operating systems today would be so altered in a secure version that compatibility would not exist, but the emulator approach was still considered to be the most effective if a suitable operating system could be found which would remain compatible after being secured.

After examining a wide range of operating systems, DOD researchers selected the UNIX operating system which was developed by the Bell Laboratory at Murray Hill, New Jersey, in the early 1970's (RITC74). UNIX was designed as an interactive system with a simple, unified design. It is an efficient system and has widespread use within the Bell System, and Western Electric also offers licenses for non-Bell System users, so there is a growing community of UNIX users in university and commercial environments. The main reason for selection of the UNIX operating system was its characteristic of maintaining its internal data structures in a manner which was transparent to user programs, thus allowing almost complete restructuring of the system for security while maintaining its external characteristics. In 1976, both UCLA and MITRE adapted their security kernels to support a prototype secure operating system which is compatible with UNIX support software and application programs, and both systems use the reference monitor concept within different architectures.

## 3.3 DOD KERNELIZED SECURE OPERATING SYSTEM (DOD KSOS)

Based upon the preceding research background, the DOD initiated an effort in 1977 to design and implement a production quality, certifiably secure operating system which emulates the UNIX system. This effort is entitled the DOD Kernelized Secure Operating System (DOD KSOS), and a chart of the development to date is contained in Figure 3-3.

The decision to emulate the UNIX system in DOD KSOS was driven by the facts that UNIX has a widespread installed computer base on the PDP-11/70 series of computers and that Bell Laboratories as well as other manufacturers are in the process of implementing UNIX on hardware other than the PDP-11/70, which will make its use even more widespread.

The major deliverable product at the end of the Design Phase of the DOD KSOS was a detailed system level specification. This specification contains functional descriptions of each module of the security kernel and the operating system, and could be used to direct the efforts of other manufacturers in the development of the DOD KSOS on other hardware. As is shown in Figure 3-3, the Implementation phase contract for the DOD KSOS was awarded to the Ford Aerospace and Communications Corporation in May 1978.

It should be pointed out that the actual UNIX software from Bell Laboratories will not be used in the development of the DOD KSOS, but that the operating systems which are developed will interface with all support software and application programs currently in use with UNIX.

## 3.4 APPLICATIONS ENVISIONED FOR THE DOD KSOS.

The DOD KSOS will fulfill a number of requirements for increased security in DOD ADP systems. Three general classes of applications are presently envisioned by Walker (WALK78).

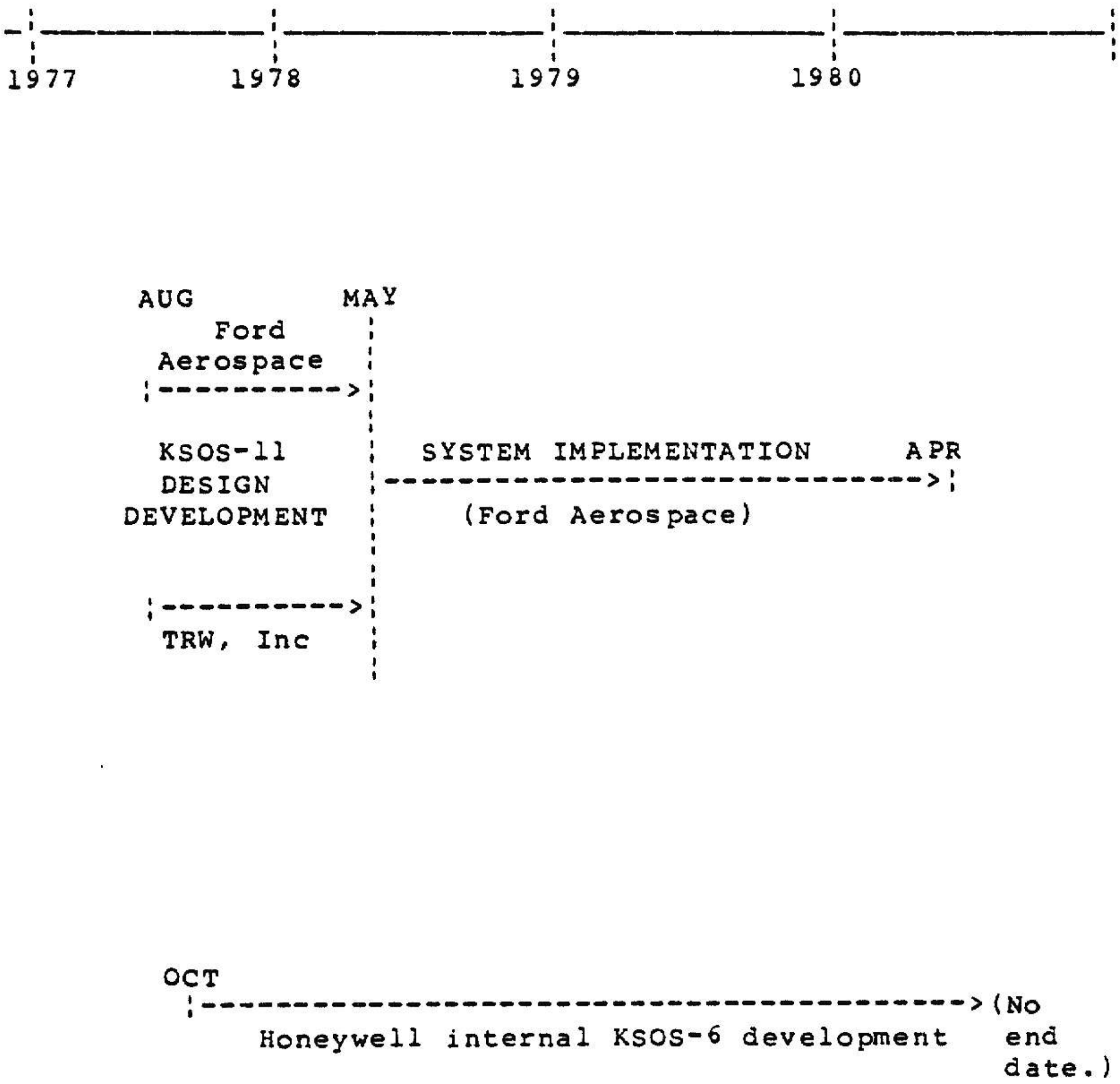


FIGURE 3-3.
DOD KSOS DEVELOPMENT

The first application will enable the implementation of multi-level security links between ADP systems, something which has not been substantially accompished to date. The DOD KSOS is used in what is termed a Guard mode, as shown in Figure 3-4. Two commercially available, untrusted data management systems, each operating at a different security level, are connected through a Guard, which is a DOD KSOS based security filter. Queries from the lower level system which might require answers containing a high security classification have the replies sanitized by either operators or software on the Guard system. Before any information is passed to the system with the lower security level, it is presented to the Security Watch Officer for a determination of the appropriate classification of the reply. If the sanitized classification is releasable to the lower-level system, the reply is forwarded; if not, it is returned for further sanitization.

The functions of the Guard mode are now being performed manually, with editing assistance from computer systems, at some of the compartmented intelligence activities of the DOD. The KSOS will enable more of these sanitization functions to be automated, thus relieving the SWO of some of the time-consuming sanitization duties and allowing more time for proper inspection of the outgoing traffic.

## KSOS APPLICATIONS

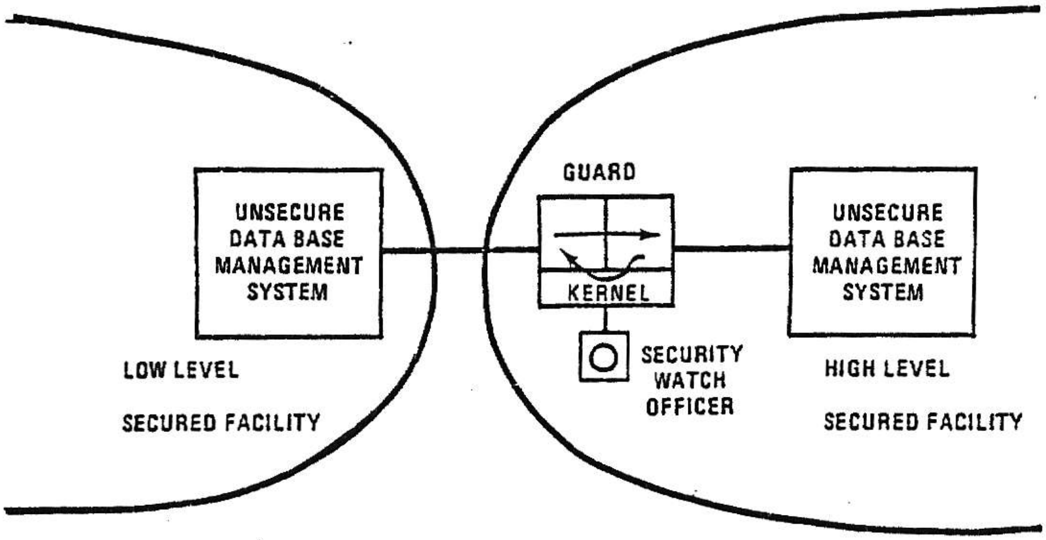


FIGURE 3-4
DOD KSOS USED IN GUARD MODE

Although this is a relatively simple application of the KSOS, it will fill a very useful function for the DOD and will have widespread application.

The second applicaton of the DOD KSOS is proposed (WALK78) for use as a secure network front-end (NFE), as shown in Figure 3-5. The DOD is rapidly expanding its use of computer networks, and many of the networks which are being built require the use of untrusted host computers. In accordance with current network design philosophy, much of the network protocol and terminal access functions are being moved from the host machine to a smaller NFE. As was described for the WWMCCS ADP system in Chapter 2, a benign environment must be established for the entire computer network, and this can be a very expensive undertaking as well as possibly precluding the establishment of some needed interconnections in the network. Walker (WALK78) proposes that NFE′s be implemented as KSOS′s and the network be established as a secure interconnection of subnetworks, each operating at its own security level. As was stated by Walker, "A set of cooperating secure network frontends could provide a significant improvement to today′s system high operating environment with no change required to large systems.".

## KSOS APPLICATIONS
### SECURE NETWORK FRONT END

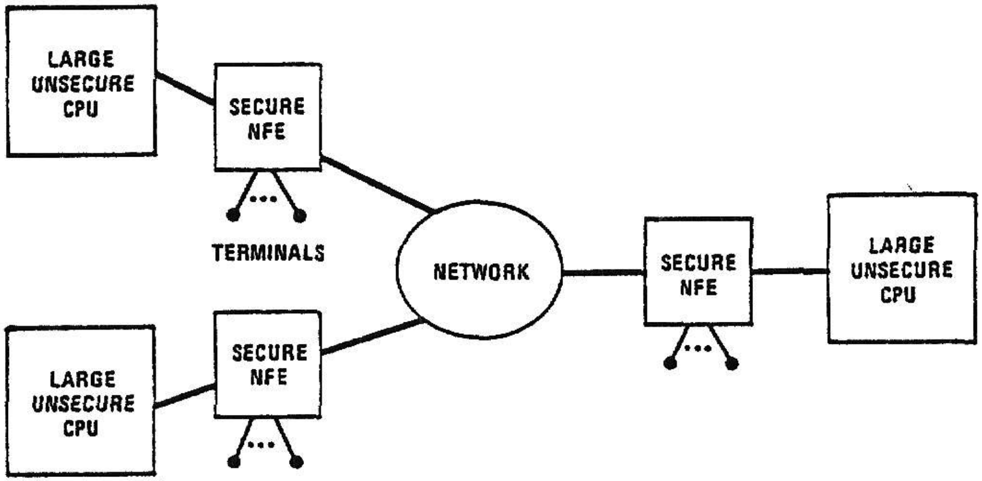


FIGURE 3-5
DOD KSOS USED AS A NETWORK FRONT END

The DOD´s multitude of message handling systems provide a third very useful application for the DOD KSOS. A characteristic which is common to all of the DOD message handling systems is the requirement for internal integrity with the systems. Security constraints in the handling of some highly classified information may preclude the transmission of this information over a message handling system because all of the organizations connected by the system do not have the complete set of security accesses necessary for receipt of the information. This has led to proliferation of special purpose message handling systems to serve different users and to the denial of ready access to needed information by an organization not connected to the proper message handling system. If the access isolation mechanisms of the DOD KSOS could be applied to the design of message handling systems, message sources with different security levels could be integrated into a single message handling environment with enough isolation guaranteed to protect the sensitive information involved.

With the identification of the above applications, interest in the DOD KSOS increased in the computer manufacturing community. In addition to Ford Aerospace, which had the DOD development contract, Honeywell Avionics

Division initiated an internally funded project called KSOS-6, and Systems Development Corporation entered their Kernelized Virtual Machine/370 (KVM/370) into consideration for use as a security mechanism for the DOD, thus partially realizing Walker's third DOD Computer Security Initiative goal of manufacturer involvement. The Ford Aerospace KSOS-11 and Honeywell's KSOS-6 will be discussed in this report. Other efforts which support the DOD Computer Security Initiative are verification and validation standards for software (SHOR79), software specification languages (ANDE79, MATH78, NEUM78, NEUM79), and software proving mechanisms (NEUM78, NEUM79, MATH78). These will not be addressed in this report.

## 3.5 FORD AEROSPACE KSOS-11 DEVELOPMENT

Dr. E.J. McCauley of Ford Aerospace defines the long term goal of the Ford Aerospace KSOS-11 effort as the development of a commercially viable operating system for the DEC PDP-11/70 which:

(1) is compatible with the Bell Laboratories UNIX operating system,

(2) is capable of efficiency comparable to the standard UNIX,

(3) enforces multilevel security and integrity, and

(4) is demonstrably secure.

As described in the KSOS Executive Summary (MCCA78), the basic design of KSOS-11 consists of a Kernel that supports multilevel security, the trusted Non-Kernel Security Related Software which, though outside of the Kernel, is trusted to deviate from the multilevel security policy to provide critical system functions, an Emulator that provides UNIX support and User interface, and the untrusted Non-Kernel Security Related Software, which provides user services such as secure mail and output spooling. A block diagram of the KSOS design is shown in Figure 3-6. The diagram is hierarchical in that a given design level is permitted to depend only on lower design levels. Note that the design has three modes of operation: the User mode, the Supervisor mode, and the Kernel mode, and that the Supervisor mode is split between trusted and non-trusted software. This allows the UNIX Emulator to be nontrusted but to make calls on the Kernel and the Non-Kernel Security Related software.

## 3.6 DESIGN METHODOLOGY

Ford Aerospace and its subcontractor SRI International

```
......              V  K+T+E+U+A                   .......
          |----------------------------------|
          |        UNIX*tm Applications      |
          |             Untrusted           A|
          |----------------------------------|
User                    |
mode                    V  K+T+E+U
          |----------------------------------|
          |Non-Kernel Security-Related Software|
          |         Untrusted portion        |
          |             KSOS.U              U|
          |----------------------------------|
..................      |
                        V  K+T+E
          |----------------------------------|       ^
          |          UNIX*tm Emulator        |       |
          |            Untrusted             |      Not
          |             KSOS.E              E|    Trusted
          |----------------------------------|
Supervisor              |                     ....................
mode                    V  K+T
          |----------------------------------|    Trusted
          |Non-Kernel Security-Related Software|      |
          |          Trusted portion         |       V
          |             KSOS.T              T|
          |----------------------------------|
..................      |
                        V  K
          |----------------------------------|
          |          Security Kernel         |
Kernel    |            trusted               |
mode      |             KSOS.K              K|
          |----------------------------------|
......                                             .......
```

Note: K,T,E,U,A denote the functions provided by the five components in upward order, respectively. The interfaces potentially visible at each level are cumulative upwards, e.g., as indicated by K+T+E+U+A. In actual implementation there will be restrictions on function visibility.

FIGURE 3-6
DOD KSOS COMPONENTS

are using SRI's Heirarchical Development Methodology (HDM) in the KSOS-11 design and implementation. This is the first full use of HDM for development of a complete system, but SRI has used it in the design stage of other projects. As presented by Lawrence Robinson (ROBI78), HDM represents a set of concepts, procedures, languages, and tools that is intended to aid in the production of correct, reliable, and maintainable software.

Three specification languages are used in the implementation of an HDM project. The first is used in the Formal Specification Stage, the second in the Formal Representation Stage, and the third in the Abstract Implementation Stage.

The first language used is SPECIAL (SPECIfication and Assertion Language), described by Roubine and Robinson (ROUB77). SPECIAL module descriptions have been likened to the description of a computer instruction set given in a programmer's manual, except that SPECIAL is mathematical, being based on logic and set theory. SPECIAL enables the system designer to express an operation as a single entity, rather the conventional approach of describing a sequence of smaller included operations.

The second language used with HDM is called HSL (Heirarchy Specification Language). The specifications written in HSL are used to check consistency of decisions which are shared by two or more modules written in SPECIAL.

The language which is used to create the abstract programs used with HDM is called ILPL (Intermediate Level Programming Language). This is an extremely simple language which has no built-in data structures. The user must explicitly specify any data structures used, which allows ILPL to be used for a wide variety of applications. After the abstract program is written in ILPL, the user may use whichever programming language is appropriate for the final coding. The data structures of that language are built in ILPL as a set of abstract modules, and then coded in the appropriate language. Since ILPL is based on the same concepts as SPECIAL and HSL, consistency checking on the abstract design may be performed in either of these languages.

The automated tools used in HDM provide material assistance to the system designer through the performance and documentation of checks on the consistency of the design of the system. The complete set of tools proposed by SRI

(ROBI78) will provide automated tools to perform consistency checking throughout all but the first phase of HDM, but not all of the tools have been implemented at this time. Those tools which have been implemented and are in use include the module checker, the representation checker, the interface checker, and the hierarchy checker. A diagram representing the actions and interactions of these tools is shown in Figure 3-8. The tools for abstract implementation and verification are still under development, with the verification set still being three years from implementation.

A summary of the stages of HDM is shown in Figure 3-7, and the stages are described by Robinson as follows: (Subparagraphs under some of the descriptions relate to the KSOS-11 design as outlined by McCauley (MCCA78, MCCA79)

> "(1) Conceptualization Stage -- The designer analyzes the environment of the proposed software system and states precisely the problem to be solved. This environment contains constraints imposed by the user (manifested at the top level of the system) and constraints imposed by the hardware or programming language (manifested at the bottom level). Efficiency

| Stage | Activity | Output | Language | Tool(s) |
|---|---|---|---|---|
| Conceptualization | Analysis of problem | Informal statement of the problem | -- | -- |
| External Interface Definition | Defining external behavior of system and decomposing external interfaces into modules and functions | List of modules at each interface and the functions of each module | HSL | Interface checker |
| Intermediate Interface Definition | Defining hierarchical structure and behavior of intermediate levels; decomposing intermediate levels into modules and functions | List of intermediate levels, the modules of each level, and the functions of each module | HSL | Interface checker,<br>Hierarchy checker |
| Formal Specification | Formally specifying all modules of the system | Formal specifications for each module | SPECIAL | Module checker |
| Formal Representation | Describing data structures at one level in terms of data structures of lower level | Formal representations of the data structures of each level in terms of those of the lower level | SPECIAL | Representation checker |
| Abstract Implementation | Writing abstract programs to implement each function of the system | Abstract programs for each function of each module | ILPL | Implementation checker |
| Coding | Translation of abstract programs into concrete programs | Concrete programs for each function of each module | Conventional programming language | Preprocessors, compilers, assemblers, etc. |
| Verification | Mathematically proving that the system implementation meets its specifications | Transcript of proof | -- | Verification system |

FIGURE 3-7
HEIRARCHICAL DESIGN
METHODOLOGY STAGES

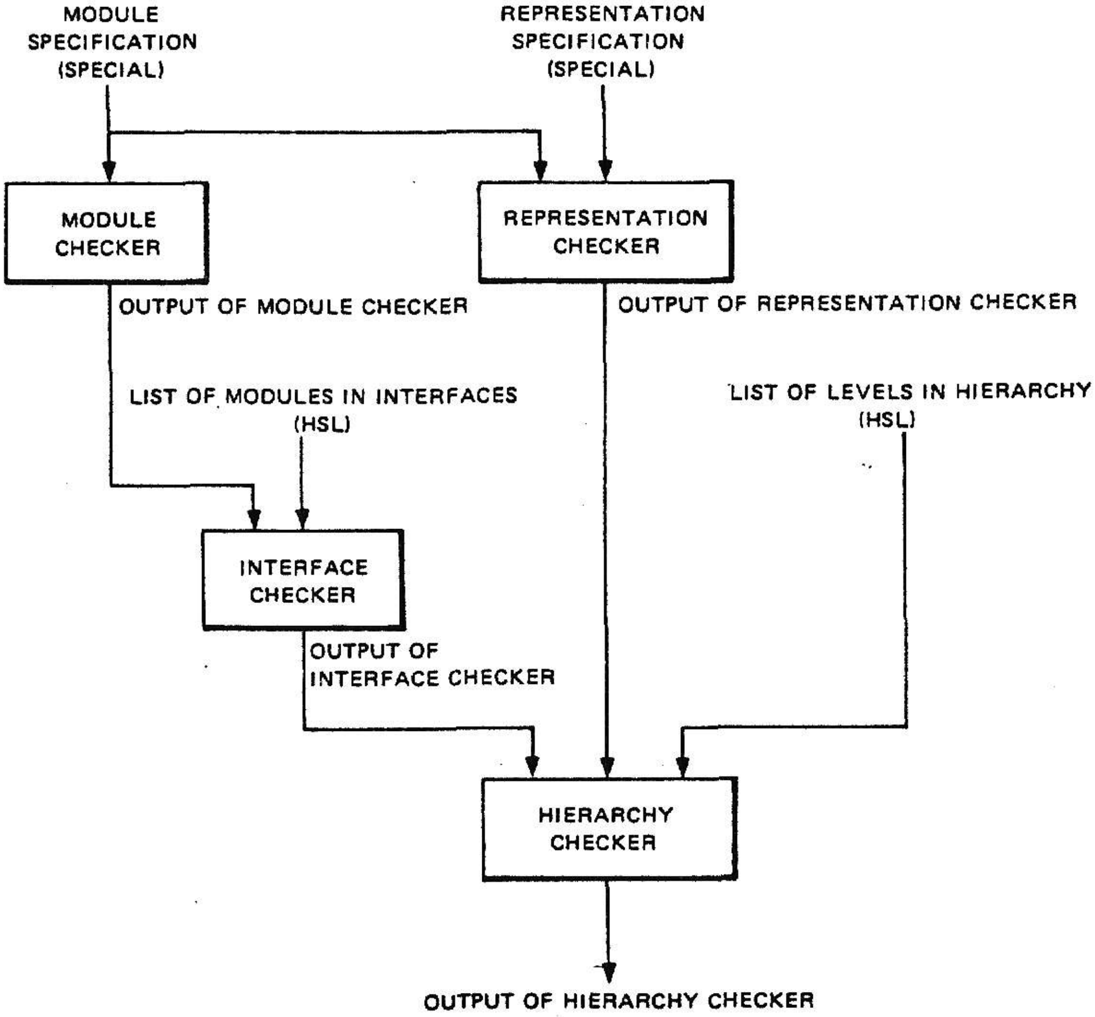

MODULE SPECIFICATION (SPECIAL)
REPRESENTATION SPECIFICATION (SPECIAL)
MODULE CHECKER
REPRESENTATION CHECKER
OUTPUT OF MODULE CHECKER
OUTPUT OF REPRESENTATION CHECKER
LIST OF MODULES IN INTERFACES (HSL)
LIST OF LEVELS IN HIERARCHY (HSL)
INTERFACE CHECKER
OUTPUT OF INTERFACE CHECKER
HIERARCHY CHECKER
OUTPUT OF HIERARCHY CHECKER

FIGURE 3-8
HDM AUTOMATED
TOOL INTERACTIONS

constraints, such as throughput, can also be expressed at this stage. At present, the output of the Conceptualization Stage is stated in terms of precise English, because HDM currently provides no formal language to support conceptualization.

> The concept for KSOS-11 has been developed by Ford Aerospace as the "designer" and approved by the Defense Advanced Research Projects Agency (DARPA) as the "user". The precision of the problem statement appears to be sufficient as described (MCCA79), but only implementation and certification will reveal the true sufficiency.

(2) External Interface Definition Stage -- The external interfaces of the system (i.e., the top and bottom levels) are conceived. Each of these levels provides some functional capability in terms of a set of <u>operations,</u> and consists of one or more <u>modules,</u> or groups of related operations (note the discrepancy with the conventional usage of "module" meaning a single program or subroutine). A module is chosen on the basis of localizing certain decisions (concerning for example, representation or implementation) within the module, so that different modules can be implemented (or have their implementation changed) without regard to the implementation of any other module. While the conceptualization stage poses the problem to be solved, this stage describes the functional capability of a system that solves the problem. The output of this stage is a list of the modules of the top and bottom levels of the system, and a list of the operations of each module.

> The KSOS-11 external interfaces have been written in HSL, and serve as part of the input to the automated interface checker.

(3) Intermediate Interface Definition Stage -- The intermediate levels of the hierarchy are conceived. This process of defining intermediate levels can proceed in any manner: top-down, bottom-up, or randomly. For example, in conceiving levels top-down, one asks "What level best realizes the level I already Have?". In conceiving levels bottom-up, one asks, "What level best utilizes the level I already have?". This process continues until the entire hierarchy is conceived. Each intermediate

level is also decomposed into modules. The number of intermediate levels depends on the complexity of the problem and on the taste of the designer. The output of this stage is a list of the modules of each of the intermediate levels, and a list of the operations of each module.

> The KSOS-11 intermediate interfaces have also been written in HSL and the hierarchy levels have been specified, primarily from a top-down development. These also serve as part of the input to the interface checker, and the hierarchy level development serves as input to the heirarchy checker.

(4) Formal Specification Stage -- The formal specifications for each module are written. In addition to its operations, which are invoked by a user or an external program, each module contains a set of internal data structures that can be accessed or modified only via its operations; a specification of each operation is written in terms of the values of the internal data structures. The operations of a given module may also reference, in a restricted way, the operations and internal data structures of other modules at the same level; all such references must be explicitly stated. One goal in decomposing a system is to minimize intermodule references, making each module as self-contained as possible. The output of this stage is a set of formal specifications for each module of each level in the hierarchy.

> The KSOS-11 formal specifications have been written in SPECIAL for the Kernel and the Non-Kernel Security Related (NKSR) software, but according to McCauley (MCCA79), the proof of these is still on-going.

(5) Formal Representation Stage -- Eventually each non-primitive module (i.e., a module that does not appear at the bottom level) will be realized in terms of the next lower level. For each such module, its realization consists of the representation of its internal data structures in terms of the internal data structures of the modules at the next lower level, and (at the next stage) the implementation of each of its operations as a program that invokes the operations of modules at the next lower level. The Formal

Representation Stage reflects the need to define the internal data structures of each nonprimitive module, which have no meaning by themselves, in terms of more primitive internal data structures. The formal representation of the modules at a level is written as a set of expressions (called mapping function expressions ), one for each internal data structure of each module at the level; each expression defines its corresponding data structure in terms of the internal data structures of the modules at the next lower level. The output of this stage is a mapping (i.e., a set of mapping function expressions) for each level in terms of the next lower level.

> Formal module representations written in SPECIAL for the KSOS-11 Kernel and NKSR software have been developed, but these are in the same state of proof as the formal specifications.

(6) Abstract Implementation Stage -- Each operation of each module is implemented as an abstract program invoking the operations of the modules at the next lower level. It is in this stage that the implementation decisions are made. The programs are termed abstract because they describe only the sequence of calls to the operations of the next lower level, without regard to other details associated with the final code (see the next stage). The output of this stage is a set of abstract programs, one for each operation of each nonprimitive module.

(7) Coding Stage -- To produce a running system, a set of programs that run on the target machine must be generated. Here the target machine may be either a piece of hardware (in which case the programs are written in assembly language) or a high-level programming language (in which case the programs are written in that language). These programs can be generated by translating the abstract programs (either by hand or machine) into concrete programs that can actually be run. The concrete programs thus contain much detail that has been omitted from the abstract programs. The output of this stage is a set of concrete programs -- one for each abstract program -- that can be compiled, interpreted, or assembled with existing on-line tools.

The language selected for the implementation of

KSOS-11 is MODULA, developed by Nicholas Wirth as a derivation of the PASCAL language.

(8) Verification -- As stated above, verification is an extremely precise and complex consistency checking operation. The object of verification in the specific case of HDM is to see that the module specifications are correctly realized by the representations and abstract programs that have been supplied. Verification requires a formal mathematical proof, which can be performed either by hand or with the aid of an on-line program verification system. A verification technique especially suited to HDM has been developed (ROBI77). Because verification is so difficult, it can be considered to be an optional stage of HDM. In that case, other methods of validation, such as debugging and testing, would be used to ensure the operation of the developed system. The output of this stage is a transcript of the proof of the correctness of the system."

The verification of KSOS-11 will be performed manually by established debugging and testing techniques, as these are the only techniques available at present.

## 3.7 HONEYWELL KSOS-6 DEVELOPMENT

Honeywell Information Systems, Inc., is developing what DOD representatives are calling KSOS-6, based on the Honeywell Level 6 series of computers. The Honeywell name for this internally funded development project is "Secure Communications Processor" (SCOMP). The Honeywell Level 6 hardware used for the project has an add-on hardware component called the Security Protection Module (SPM), and the software consists of a security kernel and a UNIX emulator. The Project was described as follows by Matti Kert (KERT79) of Honeywell:

> "The SCOMP hardware is based on the Level 6 minicomputer. The Level 6 is a bus structured mini with an optional memory management unit and a MULTICS-like heirarchical ring structure. The basic bus structured architecture makes it amenable to enhancement. The changes and additions to the hardware were motivated by a combination of security, functionality, and performance considerations. The resulting hardware provides access control functions for both memory and I/O, minimizes process switching overhead, and provides a general memory management capability that includes support for a demand paging system. These hardware features reduce the security kernel size and minimize its complexity. For example, both terminal I/O and the file system are implemented outside the kernel. The hardware support has also simplified process switching and ring crossing functions."

The Honeywell presentation (KERT79) did not specify dates for completion of the software development, but did state that software development was lagging hardware development "somewhat". The formal specification for the kernel is being written in Stanford Research Institute's SPECIAL, and the detailed design and coding of the program will be done in UCLA PASCAL. The preliminary design of the UNIX emulator is complete and the emulator will be coded in Bell Laboratory's C language, as UNIX itself is, because the Level 6 computer already has a C compiler.

# CHAPTER 4.

# ASSESSMENT

## 4.1 PRESENT DOD SECURITY ENVIRONMENT

The DOD has the capability at present to establish secure computer systems and to combine those systems into a certifiably secure network at almost any classification level that is required. Any data that is transferred between systems with different levels of protection at present must be manually sanitized before release, and the volume of data that must be transferred is growing rapidly. The present secure network capability does not satisfy all operational requirements, because the establishment of a benign environment as a total system or network envelope is both very expensive to accomplish and is limited in its dissemination of needed information.

As was pointed out in Chapter 3, "secure" does not connote "trusted" in the sense that the system can infallibly direct the information flow to the required users with no possibility of outside interference with or change to the flow methodology. What is needed is a multi-level security system which can be certified for operation at the highest, most compartmented levels of classification, yet have the facility to allow access by users with low-level security clearances. A multilevel security system has been designed and certified by the US Air Force for use at the USAF Data Services Center in the Pentagon (DAVI76), but none of the DOD intelligence agencies will certify the Air Force approach as acceptable for processing compartmented intelligence data, because the system will not pass the rigorous and exhaustive testing required for the wide range of classifications involved.

### 4.2. DOD Network Communications Environment

DOD communications encryption technology is very good at present. The capability exists to implement both link-by-link and total end-to-end circuit encryption in existing communications systems, and the level of protection provided by the encryption systems is adequate to protect even the most sensitive of compartmented information. As was stated in Chapter 3, however, data encryption is still an unsolved problem. Although there have been many data encryption algorithms proposed and some of them are quite good, certification and approval for use in functions requiring access to compartmented information is still being witheld because of the lack of ability in the DOD to certify any software system, which is what the data encryption algorithms are. Implementation of a data encryption algorithm in hardware with a changeable key similar to that used on the communications circuits is one solution, but a very expensive one in terms of implementation. A separate piece of hardware would have to be provided per user or possibly per file on the computer system, depending on the sensitivity of the information to be protected. If a technique to prove and therefore be able to certify software is developed, data encryption will very quickly become an everyday part of the implementation of secure DOD computer systems and networks.

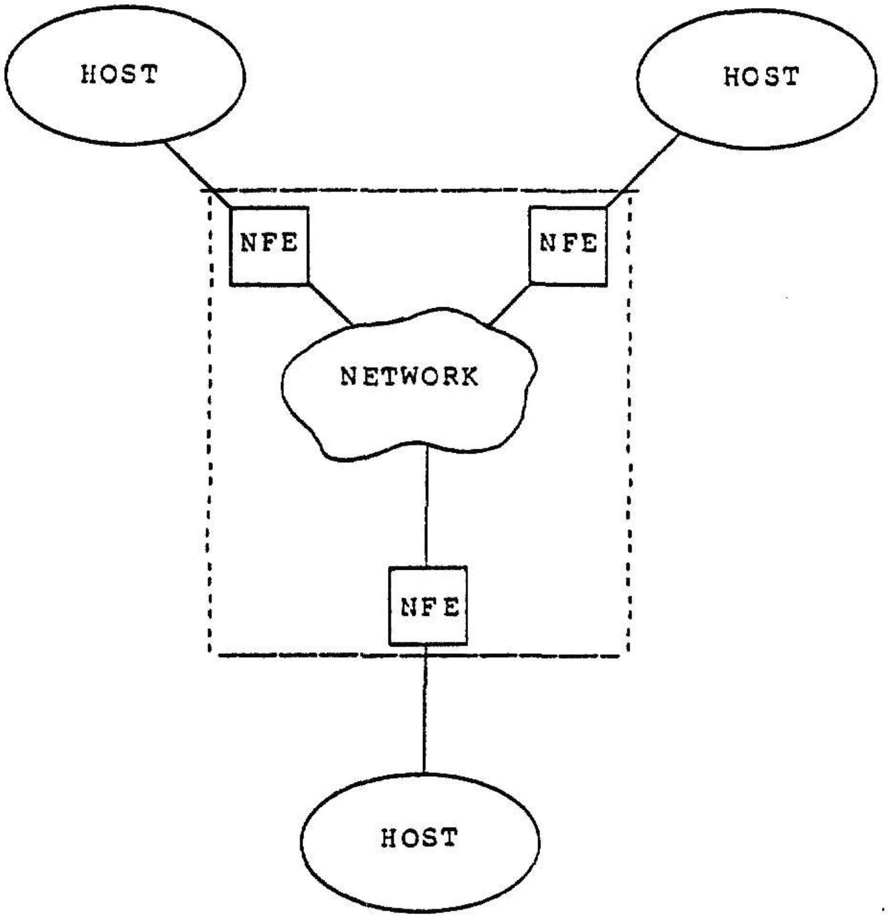
### 4.3. DOD Secure Operating System Research

The kernelized subsystem approach to secure operating system development has been widely touted as the solution to operating system software multilevel security problems (BEAC77, GOLD77, KAMP77, KERT79, MCCA79, SCHR77, WALK78, WOOD77, and others). The basic concept as explained in Chapter 2 is sound, but, as in the development of data encryption mechanisms, the problem of proving that a program does exactly what it is supposed to do and nothing more has prevented any secure software from being certified for use with highly sensitive information. Ford Aerospace has a delivery date of April 1980 for the KSOS-11 secure operating system to selected test sites, and this is with a system which still has had no formal proof methodology applied to the actual code of the software. They have been able to certify the design of the system (MCCA79), which is a positive step toward a certifiable system, but the proof of the code is still at least three years away (ROBI78).

The applications planned for the DOD KSOS appear to be in some respects incompletely developed. The Guard application, described in 3.4, is a valid automated adaptation of an existing technique which will provide significant security improvements to links between two systems with differing security levels. The network front-end concept, however, with its "set of cooperating secure network front ends" (WALK78) and claim of improvement to the "system-high" or benign environment appears to be incomplete. The security environment established as shown within the dotted line in Figure 4-1 implies the establishment of some network operating system in which each network front end (NFE) is cognizant of the security requirements of each of the hosts -- a very complicated process in a network of any size.

One possible alternative for reduction in the size of the workload required for the NFE is the proposed network is shown in Figure 4-2. A security kernel would be added to each host, and the workload required for each NFE in the network would be shared with the security kernel. If a Guard application were necessary for the host to operate effectively in a multilevel security environment, it could be incorporated into the host kernel, and the kernel would also enhance the network security by its interface with the NFE´s. The NFE´s could then provide network security functions while the host security kernel effectively screened the host environment from the network.

A second alternative presupposes the development of a data encryption algorithm which is certifiable by the DOD intelligence agencies. None to date have certified any of the existing data encryption techniques as being secure and trusted enough to handle compartmented intelligence data. FIPS Publication 46 (FIPS77) states that the DES will be used by Federal departments and agencies when the data to be encrypted "...is not classified according to the National Security Act of 1947...or the Atomic Energy Act of 1954...". This effectively precludes the use of the DES in



*"NFE" is Network Frontend*

FIGURE 4-1
SECURITY ENVIRONMENT
USING NETWORK FRONTENDS ONLY

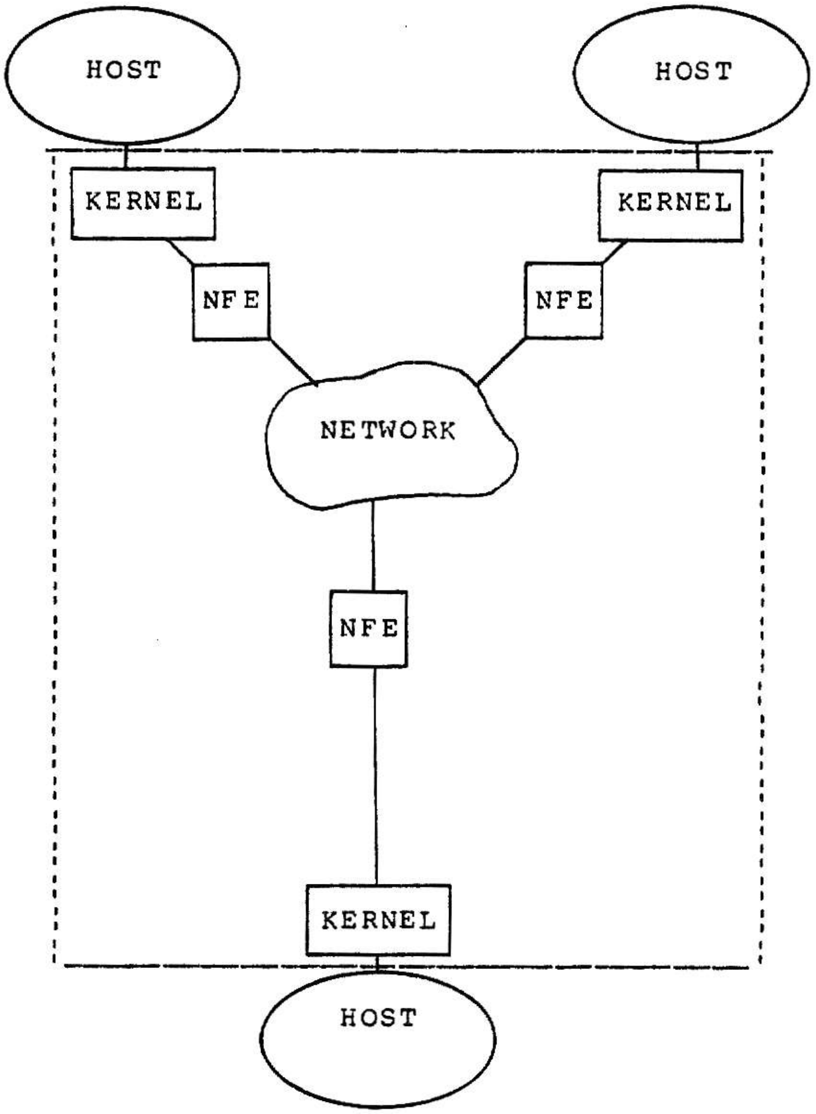


FIGURE 4-2
SECURITY ENVIRONMENT USING
SECURITY KERNELS AND
NETWORK FRONTENDS

any DOD computer network where network computer security is badly needed at present. This second alternative is described by Heinrich (HEIN78), and an illustration of the technique is in Figure 4-3. Heinrich's approach uses the NBS Data Encryption Standard (DES) for data encryption, but describes the network security center concept so that any certifiable data encryption standard could be used.

The basis for the concept is the authentication which is forced by the use of the data encryption algorithm. The network security center as shown in Figure 4-3 is the central repository for the keys to the data encryption system, and the NSC also provides network access control and collects audit trail data for the network security functions. In the example given by Heinrich and illusrated in Figure 4-3, each user and host in the network is connected through a data encryption device called a network Cryptographic device (NCD) which is remotely keyed from the NSC. The NCD is initially keyed so that the user or host may only communicate with the NSC, which performs network authentication and authorization checking prior to allowing entry into the network. After a user or host is checked, connection is established to the desired location or the requestor is informed that the connection cannot be made and the attempt is logged as a security incident by the NSC.

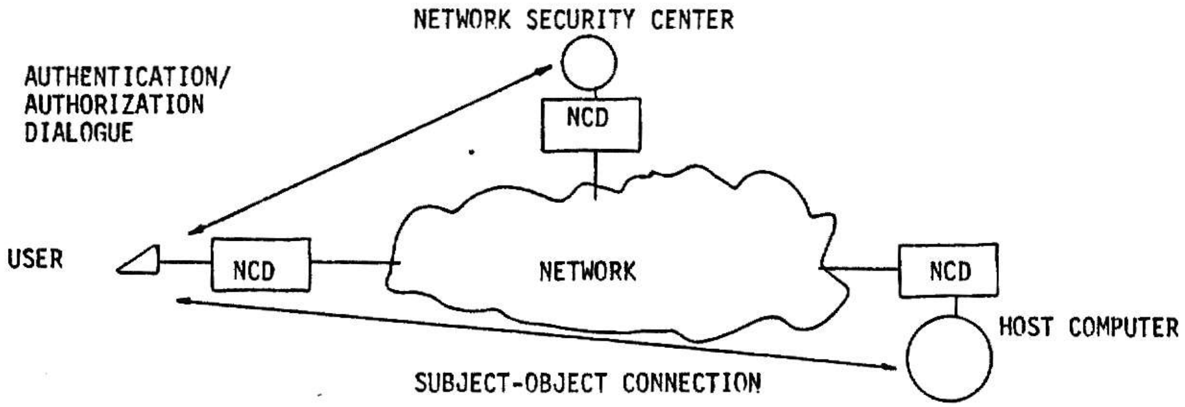


FIGURE 4-3
NETWORK SECURITY
CENTER CONCEPT

The subnetworks connected to each host are kept logically isolated, even though they share a common comunications net, because the NSC allows communication only between NCD's which have been given access permission to other NCD's. If additional security was required or if the subnetworks were very large, a concept similar to that shown in Figure 4-4 could be established, with each subnetwork having its own NSC, with the NSC's providing any cooperation required for internetting between hosts.

## 4.4. OTHER UNRESOLVED SECURITY ISSUES

Several issues of computer network security were raised at the Second US Army Automation Security Workshop as being unresolved and in need of research support for solution. Dr. Willis Ware of the Rand Corporation, in his keynote address to the Workshop, brought out the fact that there is no comprehensive DOD plan to integrate the solutions being found to computer network security. The DOD Security Initiative is a step in the right direction, but Dr. Ware felt that more positive effort was needed in this area. Dr. Ware also brought up the problem of hardware certification. Once the program proving enigma is solved and the software does what is supposed to be done and nothing more, the hardware needs to be tested and certified for the same

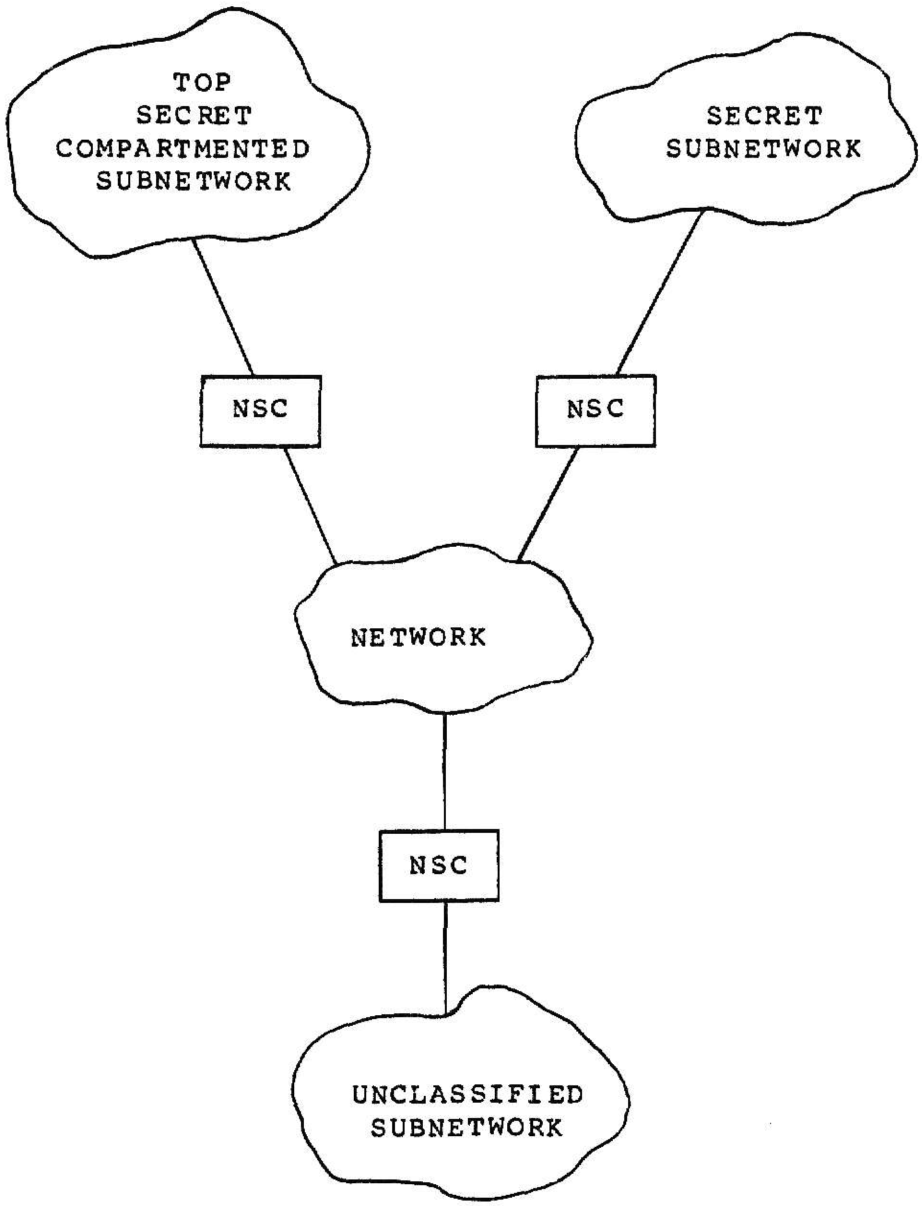


FIGURE 4-4
COMPARTMENTATION WITH
NETWORK SECURITY CENTERS (NSC)

thing. Presently, some hardware devices can be "spoofed" into performing actions that they are not supposed to perform, and this problem must be solved before a totally trusted system can be devised.

The evolution of trusted software and hardware will also place special restraints on operating procedures at computer installations. Maintenance procedures will have to be certified or post-maintenance certification tests will have to be designed to re-verify the system, and installation of new hardware will have to be done from the perspective of integrating the hardware into the security design of the total system.

## 4.5. CONCLUSIONS

Because of the critical need for secure operating systems and the rapid and voluminous proliferation of computer systems and networks, the DOD began research into secure operating systems before most of the industry and before much of the academic community. The research programs in secure operating systems sponsored by the DOD are on the forefront of research in this field, and there is a strong effort by the DOD to get the computer manufacturing community involved in computer security much more heavily than it is at present. This involvement effort is slowly paying off as more manufacturers initiate internal computer security development programs. Secure operating systems have not been successfully implemented to date, but they are slowly becoming a reality. The current trends in hardware improvements will help the effort as more and more software functions become implemented cost effectively in hardware form. Application of secure operating systems will be limited at first until the systems are certified and accredited.

The "hand-waving" and rationalization done by most of the vendors concerned with respect to program proving cannot be allowed to continue. If software is ever to be able to be certified as secure, it must be mathematically provable. Efforts in this area should be emphasized and accelerated toward the development of proof techniques which can be automated and which are inextricably combined with design techniques so that design and proof proceed simultaneously. If a proof does not check, the design must be further decomposed or altered until the proof does check. Dr. Willis Ware of the Rand Corporation, in his keynote address to the Second US Army Automation Workshop, stated the difficulty of the software certification effort: "It isn't clear whether the country has the intellectual capital to do the job more than once.". Since the DOD is presently driving the effort, the leader in the field by default may well be the DOD, with industry and other users adapting DOD secure operating system developments for their use as needed.

# APPENDIX A

## GLOSSARY AND SOURCES OF TERMS

This glossary contains computer security terms from several sources, which are indicated after each term as a bibliographic entry code. Terms in definitions which are capitalized are defined elsewhere in this glossary.

ACCESS

The ability and the means necessary to approach, to store or retrieve data, to communicate with, or to make use of any resource of an ADP system. (FIPS76)

ACCESS CONTROL

The process of limiting ACCESS to the resources of an ADP system only to authorized users, programs, processes, or other ADP systems (in computer networks). (FIPS76)

ACCOUNTABILITY

The quality or state which enables violations or attempted violations of ADP system security to be traced to individuals who may then be held responsible. (FIPS76)

ACCREDITATION

The authorization and approval granted to an ADP system or network to process sensitive data in an operational environment, and made on the basis of a certification by designated technical personnel, of the extent to which design and implementation of the system meet pre-specified technical requirements for achieving adequate data security. (FIPS76)

ACTIVE WIRETAPPING

The attaching of an unauthorized device, such as a computer terminal, to a communication circuit for the purpose of obtaining access to data through the generation of false messages or control signals, or by altering the communications of legitimate users. (FIPS76)

ADD-ON SECURITY

The retrofitting of protection mechanisms, implemented by hardware or software, after an ADP system has become operational. (FIPS76)

ARREST

The discovery of user activity not necessary to the normal processing of data which might lead to a violation of system security and force termination of the activity. (DODP73)

AUDIT TRAIL

A chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results. (FIPS76)

AUTHENTICATION

(1) The act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information.

(2) A measure designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator. (FIPS76)

BENIGN ENVIRONMENT

A nonhostile envelope protected from external elements by physical, personnel, and administrative security countermeasures. A controlled mode of operation where the ADP system is protected at the system's highest level; all users are cleared for the highest level, but not necessarily having a need-to-know for all data; and reliance is placed on the ADP system for routing and need-to-know separation of the data. (WASS77)

BREACH

The successful and repeatable defeat of security controls with or without an ARREST, which if carried to consumation, could result in a PENETRATION of the system. Examples of BREACHES are:

(1) Operation of user code in system supervisor mode;

(2) Unauthorized acquisition of identification password or file access passwords; and

(3) ACCESS to a file without using prescribed operating system mechanisms. (DODP73)

BROWSING

Searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought. (FIPS76)

CERTIFICATION

The technical process whereby a procedure, program, system component, or system(s) are shown to be secure; i.e., that the security design specifications are correct and have been properly implemented.

(NOTE: Certification is performed by independent technical personnel according to an acceptable standard of proof such that the level of security protection is identified with regard to a procedure, program, system component, or system. Certification is a broad and not wholly understood process at present and is undergoing further definition as a result of experimentation and research in progress.) (WASS77)

COMPARTMENTED INTELLIGENCE

Includes only that intelligence material having special controls indicating restrictive handling for which systems of information compartmentation or handling are formally established. (DODP73)

COMPROMISING EMANATIONS

Electromagnetic emanations that may convey data and that, if intercepted and analyzed, may compromise sensitive information being processed by any ADP system. (FIPS76)

CONFIDENTIALITY

A concept which applies to data. It is the status accorded to data which has been agreed upon between the person or organization furnishing the data and the organization receiving it and which describes the degree of protection to be provided. (HOFF77)

CONTROL ZONE

The space, expressed in feet of radius, that surrounds equipment that is used to process sensitive information and that is under sufficient physical and technical control to preclude any unauthorized entry or compromise. (FIPS76)

CONTROLLABLE ISOLATION

Controlled sharing in which the scope or domain of authorization can be reduced to an arbitrarily small set or sphere of activity. (FIPS76)

CRYPTANALYSIS

The steps and operations performed in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption algorithm. (FIPS76)

CRYPTOGRAPHY

The art or science which treats of the principles, means, and methods for rendering plain text unintelligible and for converting encrypted messages into intelligible form. (FIPS76)

DATA-DEPENDENT PROTECTION

Protection of data at a level commensurate with the sensitivity level of the individual data elements, rather than with the sensitivity of the entire file which includes the data elements. (FIPS76)

DEDICATED MODE

The operation of an ADP system such that the central computer facility, all connected peripheral devices, the communications facilities, and all remote terminals are used and controlled exclusively by specific users or groups of users for the processing of particular types and categories of information. (FIPS76) See also BENIGN ENVIRONMENT.

DESIGNATED APPROVING AUTHORITY (DAA)

An official designated to ACCREDIT ADP systems under his jurisdiction for the processing, use, storage, and production of classified material. (WASS77)

ELECTROMAGNETIC EMANATIONS

Signals transmitted as radiation through the air and through conductors. (FIPS76)

EMANATION SECURITY

The protection that results from all measures designed to deny unauthorized persons information of value that might be derived from intercept and analysis of COMPROMISING EMANATIONS. (FIPS76)

ENCRYPTION ALGORITHM

A set of mathematically expressed rules for rendering information unintelligible by effecting a series of transformations through the use of variable elements controlled by the application of a key to the normal representation of the information. (FIPS76)

FAILURE ACCESS

An unauthorized and usually inadvertent ACCESS to data resulting from a hardware or software failure in the ADP system. (FIPS76)

FAIL SAFE

The automatic termination and protection of programs or other processing operations when a hardware or software failure is detected in an ADP system. (FIPS76)

FAIL SOFT

The selective termination of affected non-essential processing when a hardware or software failure is detected in an ADP system. (FIPS76)

HANDSHAKE PROCEDURES

A dialogue between a user and a computer, a computer and another computer, or a program and another program for the purpose of identifying a user and AUTHENTICATING his identity, through a sequence of questions and answers based on information either previously stored in the computer or supplied to the computer by the initiator of the dialogue. (FIPS76)

INTEGRITY

Data integrity exists when data does not differ from its source documents and has not been accidentally or maliciously altered, disclosed, or destroyed. (HOFF77)

ISOLATION

The containment of users and resources in an ADP system in such a way that users and processes are separate from one another as well as from the protection controls of the operating system. (FIPS76)

MULTIPLE ACCESS RIGHTS TERMINAL

A terminal that may be used by more than one class of users; for example, users with different ACCESS rights to data. (FIPS76)

PASSIVE WIRETAPPING

The monitoring and/or recording of data while the data is being transmitted over a communications link. (FIPS76)

PENETRATION

The successful and repeatable extraction and identification of recognizable information from a protected data file or data set without any attendant ARRESTS. (DODP73)

PENETRATION SIGNATURE

(1) The description of a situation or set of conditions in which a PENETRATION could occur.

(2) The description of usual and unusual system events which in conjunction can indicate the occurrence of a PENETRATION in progress. (FIPS76)

PRIVACY

A concept which applies to an individual. It is the right of an individual to decide what information (s)he wishes to share with others and also what information (s)he is willing to accept from others. (HOFF77)

## PROTECTION RING

One of a hierarchy of privileged modes of an ADP system that gives certain ACCESS rights to the users, programs, and processes authorized to operate in a given mode. (FIPS76)

## RED/BLACK CONCEPT

The concept that electrical and electronic circuits, components, equipments, systems and so forth, which handle classified plain language information in electronic signal form (RED) be separated from those which handle encrypted or unclassified information (BLACK). Under this concept, RED and BLACK terminology is used to clarify specific criteria relating to, and to differentiate between, such circuits, components, equipment, systems, etc., and the areas in which they are contained. (WASS77)

## SANITIZING

The degaussing or overwriting of SENSITIVE INFORMATION in magnetic or other storage media. (FIPS76)

NOTE: This is also a term used in the intelligence community to denote the selective extraction of information of a highly classified or compartmented nature from a message or file to reduce it to a classification which can be disseminated outside the intelligence community.

SECURE OPERATING SYSTEM

An operating system that effectively controls hardware and software functions in order to provide the level of protection appropriate to the value of the data and resources managed by the operating system. (FIPS76)

SECURITY

Data security is the protection of data against accidental or intentional destruction, disclosure, or modification. Computer security refers to the technological safeguards and managerial procedures which can be applied to computer hardware, programs, and data to assure that organizational assets and individual privacy are protected. (HOFF77)

SECURITY KERNEL

The central part of a computer system (software and hardware) that implements the fundamental security procedures for controlling ACCESS to system resources. (FIPS76)

SENSITIVE INFORMATION

Any information which requires a degree of protection and which should not be made generally available. (FIPS76)

TECHNOLOGICAL ATTACK

An attack which can be perpetrated by circumventing or nullifying hardware and software ACCESS CONTROL mechanisms, rather than by subverting system personnel or other users. (FIPS76)

TRUSTED ADP SYSTEM

An ADP system which may be trusted to properly control the flow of information within an operation and insure its dissemination to only those users with a proven need for it. (WALK79)

## WORK FACTOR

An estimate of the effort or time that can be expected to be expended to overcome a protective measure by a would-be penetrator with specified expertise and resources. (FIPS76)

# APPENDIX B

# BIBLIOGRAPHY

ABEN77 Abene, Peter V., Secure Commercial Digital Communications, Jul 1977, Master's thesis, Air Force Institute of Technology, Wright-Patterson AFB, Oh.

This thesis provides a review of communications cryptographic techniques and examines the NBS Data Encryption Standard as applied to communications.

ABRA77 Abrams, M.D., Branstad, D.K., Browne, P.S., Cotton, I.W., Tutorial on Computer Integrity and Security , IEEE Computer Society, Long Beach, CA., 1977

This tutorial and the readings associated with it provide a practical background to the state of the art in computer security. Included is a section specifically addressing network security.

ANDE72 Anderson, J.P. Planning Study, Computer Security Technology Planning Study, Vol 1 , US Air Force Electronic Systems Division, Report No. ESD-TR-73-51-1, October 1972.

A study recommending research needed to provide secure ADP systems for command and control applications. Basis for much of the secure O/S work presently being done.

ANDE76 Anderson, James P., Computer Security Requirements: An Investigation of Computer Security Costs, A report by the James P. Anderson Co. for Electronic Systems Division, Air Force Systems

Command, Hanscom AFB, Ma, Report No. ESD-TR-77-24, Jan 1976

This report provides cost comparisons for three computer security problem avoidance techniques.

ANDE78 Anderson, E.R., "Standards for Specification Languages", paper presented at the Second US Army Automation Security Workshop, September 1979.

This paper reviews a number of desirable specification language properties and proposes them as standards. It suggests that for implementation verification applications a verifiable implementation language be extended to or designed with a matching specification language. It will be included in the proceedings of the Workshop.

ATTA74 Attanasio, C.R., "Operating System Architecture and Integrity", *IBM Data Security Forum* , September 1974.

This paper outlines the strengths and weaknesses of the IBM OS/MVT and the VM/370 operating systems through a discussion of penetrations of these systems.

BEAC77 Beach, Martin H., *Computer Security for ASSIST*, 10 Jun 1977, Master's thesis, US Army Command and General Staff College, Ft. Leavenworth, Ks.

A brief description of the Army Standard System for Intelligence Support Terminals (ASSIST) and the application of current computer security research to it.

BIBA77 Biba, K.J., *Integrity Considerations for Secure Computer Systems*, report by the Mitre Corp. for ESD, AFSC, Hanscom AFB, Ma., Report No. ESD-TR-76-372, Apr 1977.

This report examines computer system integrity in light of current operating system mechanisms. It identifies sources and types of threats and examines

several integrity policies.

BUSH76 Bushkin, A.A., and Schaen, S.I., *The Privacy Act of 1974: A Reference Manual for Compliance* , System Development Corporation, Santa Monica, CA, 1976.

This publication provides a reference for implementation of the Privacy Act. It has guidelines for privacy implementation on computerized information systems, and it addresses the problems involved in accidental or intentional violation of the act.

CARL75 Carlstedt, J., Bisbey, R., Popek, G., *Pattern Directed Protection Evaluation,* Information Sciences Institute, Univ. of Southern California, June 1975. (NTIS AD-A012 474)

This paper develops patterns of error types in operating systems based on errors found in OS/360, GCOS, MULTICS, TENEX, and EXEC-8 operating systems.

CONG78 Report to the Congress of the United States by the Comptroller General, "Challenges of Protecting Personal Information in an Expanding Federal Computer Network Environment", April 1978.

DAVI76 Davis, R.C., *A Security Compliance Study of the Air Force Data Services Center MULTICS System*, report by the Mitre Corp. for ESD, AFSC, Hanscom AFB, Ma, Report No. ESD-TR-76-165, Dec 1976.

This report by the MITRE Corporation supports claims that the MULTICS operating system at the US Air Force Data Services Center complies with the multi-level security requirements of DOD 5200.28-M.

DENN77 Denning,D.E., Denning,P.J., "Certification of Programs for Secure Information Flow", *CACM, Vol. 20, No. 7* , July 1977, pp. 504-513.

Presents a certification mechanism for verifying the secure flow of information through a program.

DODP73 *ADP Security Manual, DOD 5200.28-M*, published by Department of Defense, Jan 1973.

EKAN79 Ekanadham,K., Bernstein,A.J., "Conditional Capabilities", *IEEE Transactions on Software Engineering* , Vol. SE-5, No. 5, September 1979, pp. 458-464.

This paper considers protection in capability-based operating systems and proposes the concept of a conditional capability, on which other security features can be built.

FEIE77 Feiertag, R.J., Levitt, K.N., Robinson, L., "Proving Multilevel Security of a System Design", *Proceedings of the Sixth ACM Symposium on Operating Systems Principles , November 1977.*

This paper presents a technique for accomplishing the security proof for the design of a multilevel security system. It does not approach the proof of the actual programs involved in implementing a secure system.

FIPS74 Federal Information Processing Standards Publication 31, *Guidelines for Automatic Data Processing Physical Security and Risk Management* , US Dept of Commerce, NBS, June 1974.

FIPS75 Federal Information Processing Standards Publication 41, *Computer Security Guidlines for Implementing the Privacy Act of 1974* , US Dept of Commerce, NBS, May 1975.

Provides a set of guidelines for selecting safeguards for protecting personal information in automated information systems.

FIPS76 Federal Information Processing Standards Publication 39, *Glossary for Computer Systems Security* , US Dept of Commerce, NBS, February 1976.

Contains a vocabulary of terms related to privacy and computer systems security derived from diverse sources and refined by FIPS Task Group 15 (Computer Systems Security).

FIPS77 Federal Information Processing Standards Publication 46, *Data Encryption Standard* , US Dept of Commerce, NBS, January 1977.

This publication provides a description of the data encryption standard which is to be used by almost all Federal departments and agencies.

FLAT 76 Flato, L., "Navy Sinks 1108.", *Computer Decisions* , Vol. 8, No. 7, July 1976, pp. 35-36

This article provides a brief review of a US Navy penetration of the EXEC III operating system on the UNIVAC 1108 computer.

GASS76 Gasser, M., Ames, S.R., and Chmura, L.J., *Test Procedures for MULTICS Security Enhancements*, report by the Mitre Corp. for ESD, AFSC, Hanscom AFB, Ma., Dec 1976.

This report describes actual test procedures used to test a US Air Force MULTICS system. The majority of the report is listings and actual test documentation.

GOLD77 Gold,B., Linde,R., Schaefer,M., Scheid,J., "VM370 Security Retrofit Program", *Proceedings of ACM Conference* , October 1977.

This paper gives an overview of the Kernelized VM/370 project and discusses how the security flaws discovered in previous penetrations can be overcome.

HEIN78 Heinrich, F., *The Network Security Center: A System Level Approach to Computer Network Security* , NBS

Special Publication 500-21, Volume 2, Dept. of Commerce, Washington, D.C., January 1978.

This publication provides a tutorial on an approach for achieving computer network security using a data encryption methodology coupled with a network security center computer to manage all network security.

HEMP73 Hemphill, C.F., Hemphill, J.M., Security Procedures for Computer Systems , Dow Jones-Irwin, Homewood, Ill., 1973.

Security text for managers with no detailed knowledge of computer systems. Covers physical, organizational, and parts of ADP security, with security checklists in each area covered.

HOFF77 Hoffman, Lance J., Modern Methods for Computer Security and Privacy , Prentice-Hall Inc., Englewood Cliffs, N.J., 1977.

This book is a text on computer security which provides up-to-date coverage of current security technology. The book presents its material in a technical manner and assumes a basic reader knowledge of computer hardware and software.

HSIA79 Hsiao, D.K., Kerr, D.S., Madnick, S.E., Computer Security , ACM Monograph Series, Academic Press, New York San Francisco London, 1979.

This book was subsidized by the Office of Naval Research and consititutes an up-to-date survey of research in computer security. It is not written at a high technical level, and it presents excellent annotated bibliographies at the end of each chapter.

JCSM71 Joint Chiefs of Staff Memorandum 593-71, Research, Development, Test and Evaluation Program in support of the Worldwide Military Command and Control System (U). , 7 September 1971.

This document states the objectives of the RDT&E program in support of WWMCCS ADP program and establishes the need for an intercomputer network.

JCSM75 Joint Chiefs of Staff Memorandum 286-75, Prototype WWMCCS Intercomputer Network Development Plan , 7 July 1975.

THis document provided a plan for the technical development of the intercomputer network and for its test and evaluation in a user environment.

JONE78 Jones, A.K., "Protection Mechanisms and the Enforcement of Security Policies", Lecture Notes in Computer Science: Operating Systems , Springer-Verlag, Berlin Heidelberg New York, 1978, pp. 228-250.

This set of notes discusses information control and access control policies and describes protection mechanisms used to provide security for them. It assumes a basic knowledge of computer operating systems.

KAMP77 Kampe,M., Popek,G., The UCLA Data Secure UNIX Operating System , UCLA, 1977.

KARG74 Karger, Paul A., and Schell, Roger R., MULTICS Security Evaluation: Vulnerability Analysis, a report for ESD,AFSC, Hanscom AFB, Ma., Jun 1974

This report gives the results of penetrations of a US Air Force MULTICS system.

KERT79 Kert, Matti, "Secure Communications Processor (SCOMP)", paper presented at the Second US Army Automation Security Workshop, September 1979.

This presentation covered a brief history of the SCOMP project, described the SCOMP hardware, and summarized the status of the project development. It will be included in the proceedings of the workshop.

LACK74 Lackey, R.D., "Penetration of Computer Systems -- An Overview", The Honeywell Computer Journal , Vol. 8, No. 2, 1974, pp. 81-85

This paper provides a taxonomy of penetration techniques and recommends measures that should be taken to secure computer systems.

LIND75 Linde, R.R., "Operating Systems Penetration" AFIPS Conference Proceedings - 1975 NCC , Vol. 44, 1975, pp. 361-368

This paper explains the Flaw Hypothesis Methodology used in computer system penetrations and describes some basic vulnerabilities of operating systems. It includes some of the specific attack methods used on operating systems.

LIND76 Linden, T.A., Operating System Structures to Support Security and Reliable Software , NBS Technical Note 919, US Dept. of Commerce, National Bureau of Standards, August 1976.

This survey describes capability-based addressing as used to implement secure software modules. It assumes a general knowledge of operating systems concepts on the part of the reader.

MART73 Martin, James, Security, Accuracy, and Privacy in Computer Systems, Prentice-Hall, Inc, Englewood Cliffs, N.J., 1973.

A good introduction to security subjects and an excellent reference for physical and organizational security. Some of the operating systems material is out of date, but the book contains extensive security checklists.

MATH78 Mathieu, H.F., "The GYPSY Software Design and Verification System", Proceedings of the First US Army Automation Security Workshop , December 1978.

This paper outlined the development of the GYPSY specification language and described some of the features of the language.

MCCA78 McCauley, E.J., "KSOS Executive Summary", *Proceedings of the First US Army Automation Security Workshop* , December 1978.

This paper provides a summary of the progress in Phase I of the KSOS development by Ford Aerospace and its subcontractor SRI International and outlines the plans for Phase II work.

MCCA79 McCauley, E.J. "Status of the KSOS Effort", paper presented at the Second US Army Automation Security Workshop, September 1979.

This presentation covered the status to date of the Phase II (implementation) work on KSOS and presented efforts at program verification. It will be included in the proceedings of the Workshop.

MILH75 "RED/BLACK Engineering - Installation Criteria", *Military Handbook (MILHDBK) 232* , published by the Defense Communications Agency, Washington, D.C., July 1975.

This is a Confidential document outlining the measures to be taken to prevent electrical crossover of classified information in communications facilities.

NEUM78 Neumann, P.G., "A Position Paper on Attaining Secure Systems: A Summary of A Methodology and its Supporting Tools", *Proceedings of the First US Army Automation Security Workshop* , December 1978

This paper provides a summary of HDM and describes its use in development of secure operating systems.

NEUM79 Neumann, P.G., "A Second Position Paper on the

Attainment of Secure Systems: Recent Advances in the State of the Art", paper presented at the Second US Army Automation Security Workshop, September 1979.

This presentation outlined SRI´s advances in automated development tools and proposed needs for further research into program verification techniques. It will be included in the proceedings of the Workshop.

PATR74 Patrick, Robert B.,(editor), *AFIPS System Review Manual on Security* , AFIPS Press, Montvale, N.J., 1974.

The results of a two-year study, it consists of a set of guides in specific computer security areas (physical, administrative, personnel, etc.) as well as very extensive, detailed checklists in each area. A definite aid to the manager or supervisor in establishing a security program.

POPE78 Popek, G.J., Kline, C.S., "Design Issues for Secure Computer Networks", *Lecture Notes in Computer Science: Operating Systems* , Springer-Verlag, Berlin Heidelberg New York, 1978, pp. 517-546.

This section of notes describes the design problems and alternatives available for secure networks , discusses network use with respect to data security, and provides a discussion of the use of encryption in a network. It assumes a basic knowledge of Computer Operating systems.

PUBL74 Public Law 93-579, "The Privacy Act of 1974", 93rd Congress, S.3418, December 31, 1974.

This is the actual text of the law as passed by the Congress.

RITC74 Ritchie, D., Thompson,K., The UNIX Timesharing System", *CACM, Vol 17 No 7* , July 1974, pp 365-375.

This paper covers implementation of the UNIX file system and the user command interface with the system.

ROBI77 Robinson,L., Levitt,K., "Proof Techniques for Heirarchically Structured Programs", CACM, Vol 20 No 4 , April 1977, pp 271-283.

This paper describes a method for descrilbing and structuring programs which simplifies program proving. Only manual proofs are outlined, but the methods used may be applied to automated proof techniques.

ROBI78 Robinson, L., HDM - Command and Staff Overview , Technical Report by SRI International for Naval Ocean Systems Center, February 1978.

This report provides a description of HDM suitable for managers or higher-level executives who are planning to use HDM for development projects.

ROUB77 Roubine,O., Robinson,L., The SPECIAL Reference Manual , SRI International, January 1977.

RZEP77 Rzepka, William E., Considerations in the Design of a Secure Data Base Management System, report by the USAF Rome Air Development Center, Griffiss AFB, N.Y., Report No. RADC-TR-77-9, Mar 1977.

This report covers problems which arise in DBMS design and operation because of security requirements placed on the system.

SALT74 Saltzer, Jerome H., Protection and the Control of Information Sharing in MULTICS, CACM, Vol 17, Nr 7, Jul 1974.

This paper covers the information transfer control mechanisms of MULTICS and discusses vulnerabilities in the MULTICS protection mechanisms.

SCHR77 Schroeder,M., Clark,D., Saltzer,J., "The MULTICS Kernel Design", Proceedings of the Sixth ACM Symposium on Operating Systems Principles , November 1977.

This paper summarizes the result of the MULTICS kernel design project and reports on the conclusions drawn from the project. The project was terminated before formal specifications for a new security kernel could be finished.

SCHW77 Schwartz, M., Computer Communication Network Design and Analysis , Prentice-Hall, Inc., Englewood Cliffs, N.J., 1977

This book is oriented primarily toward communications network design, but the author addresses computer networks. Written in technical terms, the book presupposes only a knowledge of basic probability theory on the part of the reader and provides explanations and examples for the concepts presented.

SENA77 Computer Security in Federal Programs, report prepared by the Committee on Government Operations, US Senate, Feb 1977.

SHOR79 Short, G.E., "Outstanding Issues in Certification and Accreditation", paper presented at the Second US Army Automation Security Workshop, September 1979.

This presentation provided a summary of the unsolved issues facing The DOD and the Computer community in general concerning the certification/accreditation of secure, trusted ADP systems. It will be included in the proceedings of the Workshop.

WALK78 Walker, S.T., "The Advent of Secure Computer Operating Systems", Proceedings of the First US Army Automation Security Workshop , December 1978.

This paper outlined the development of the DOD KSOS effort, and described a technology transfer program to foster the development of trusted software by computer manufacturers.

WALK79 Walker, S.T., "DOD Computer Security Initiative", paper presented at the Second US Army Automation Security Workshop, September 1979.

This presentation described the Initiative, reviewed its progress with emphasis on the involvement of computer manufacturers in the development of trusted software. It will be included in the proceedings of the Workshop.

WARE79 Ware, Willis H., Keynote address to the Second US Army Automation Security Workshop, September 1979.

WASS77 Joint Chiefs of Staff Secretary's Memorandum 635-77, WWMCCS ADP System Security Officer's (WASSO) Manual, 25 July 1977.

This document is the security "bible" for the WWMCCS computer network. It provides extremely comprehensive coverage of security requirements, and has been the model for computer security implementation documents in many of the departments and agencies of the DOD.

WOOD77 Woodward,J., Nibaldi,G., A Kernel Based Secure UNIX Design , The MITRE Corporation, November 1977.

WWM77A Worldwide Military Command and Control System (WWMCCS) Intercomputer Network (WIN) User's Guide, published by the Defense Communications Agency Command Control Technical Center, Mar 1977.

WWM77B Worldwide Military Command and Control System (WWMCCS) Intercomputer Network (WIN) Programmer's Guide, published by the Defense Communications Agency Command Control Technical Center, Reston Va., Jul 1977.

# DEPARTMENT OF DEFENSE
# COMPUTER NETWORK SECURITY:
# AN ASSESSMENT OF THE STATE OF THE ART

by

JAMES DAVID SCHARF

B.A., Purdue University, 1963

---------------------------

AN ABSTRACT OF A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree of

MASTER OF SCIENCE

Department of Computer Science

KANSAS STATE UNIVERSITY
Manhattan, Kansas
1980

# ABSTRACT

This Master´s report provides a managerial and user overview of the Department of Defense (DOD) computer network security environment as it exists today; it also provides an outline of areas of computer network security that are presently being researched by the DOD. The need for computer network security is particularly pressing within the DOD because some of the DOD computer networks deal with classified information and many others carry information regulated by the Privacy Act of 1974. Some of the initial impetus in the computer security field and particularly in computer network security came from the DOD, and research is constantly underway to find a "trusted" computer network -- something which has not been done to date. This report provides a computer network security tutorial and a glossary for those who may not be totally familiar with the terms and concepts used; it also contains an outline of current DOD computer network security implementation procedures as prescribed in DOD implementation guides.

DOD is currently conducting research into better methods of implementing computer network security, primarily through research grants and contracts to commercial vendors and the academic community. This report contains a review of that research and an assessment of where DOD stands at present; it also contains a discussion of some areas of

research which still need to be explored.

Included with the report is a partially annotated bibliography describing sources to which a user or manager may refer for additional details and techniques for implementation of a secure computer network.