AD-A037 210 ELECTRONIC SYSTEMS DIV HANSCOM AFB MASS F/G 9/2
SECURITY IN AUTOMATIC DATA PROCESSING (ADP) NETWORK SYSTEMS.(U)
DEC 76 R R SCHELL, P A KARGER

UNCLASSIFIED ESD-TR-77-19 NL

| OF |
AD
A037210

END

DATE
FILMED
4-77

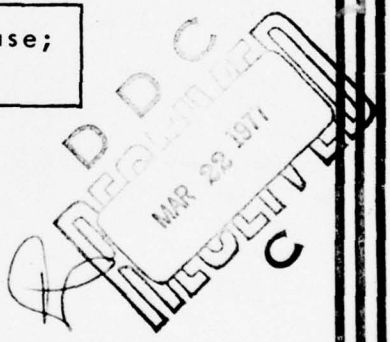
ESD-TR-77-19

SECURITY IN AUTOMATIC DATA PROCESSING (ADP) NETWORK SYSTEMS

12
NW

December 1976

Approved for Public Release;
Distribution Unlimited.



Prepared for

DEPUTY FOR COMMAND AND MANAGEMENT SYSTEMS
ELECTRONIC SYSTEMS DIVISION
HANSCOM AIR FORCE BASE, MA 01731

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER (14) ESD-TR-77-19	2. GOVT ACCESSION NO.
3. RECIPIENT'S CATALOG NUMBER	
4. TITLE (and Subtitle) (6) Security in Automatic Data Processing (ADP) Network Systems	5. TYPE OF REPORT & PERIOD COVERED (9) Technical Report
6. PERFORMING ORG. REPORT NUMBER	
7. AUTHOR(s) (10) Roger R. Schell, Lt Col, USAF Paul A. Karger, Capt, USAF	8. CONTRACT OR GRANT NUMBER(s) In-House
9. PERFORMING ORGANIZATION NAME AND ADDRESS Directorate of Computer Systems Engineering (MCI) Electronic Systems Division (AFSC) L G Hanscom AFB MA 01731	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS (16) PE64740F Project 2239
11. CONTROLLING OFFICE NAME AND ADDRESS (11) Deputy for Command & Management Systems (MCI) Electronic Systems Division (AFSC) L G Hanscom AFB MA 01731	12. REPORT DATE 15 December 1976 13. NUMBER OF PAGES 18
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office) (12) 21p.	15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

An earlier version of this paper was presented at the IEEE Electronics and Aerospace Systems Convention, Washington DC, 7-9 October 1974. The paper was not included in the conference proceedings.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Computer Security
Communications Processors
Computer Networks
Secure Networks
Security Kernels

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This paper addresses the security issues in Automatic Data Processing (ADP) elements of computer networks in both the network communication processors and the ADP hosts. The fundamental limitations of the internal security controls of conventional ADP systems are discussed. Advanced security kernel technology presently under development is presented as a viable near term solution. A precise mathematical model of security controls is applied to identify basic design options in several alternative secure network designs.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

127 100

4B

TABLE OF CONTENTS

TABLE OF FIGURES

I. Background

The networking of large ADP systems with all its attendant benefits is becoming commonplace today. However, the careless networking of ADP systems can greatly increase security risks, often in subtle and non-obvious ways. Security must be considered on a total system basis including both the ADP hosts and the communications network. This paper addresses the ADP security issues as they affect processing in both the host general purpose computers and the network interface communications processors. Recently developed "security kernel" technology for ADP systems permits construction of various alternative secure networks. The paper also addresses communications security using encryption devices in the network.

1.1 Need for Multi-Level Security

A major problem with computing systems in the military today is the lack of effective multi-level security controls. The term "multi-level security controls" means those controls needed to process several levels of classified material from unclassified through compartmented top secret with simultaneous access to the system (or network) by users with differing levels of clearance. The lack of such effective controls in all of today's computer operating systems has led the military to operate computers in a closed environment in which systems are dedicated to the highest level of classified material and all users are required to be cleared to that level. Such dedicated systems result in extremely inefficient equipment and manpower utilization and have often resulted in the acquisition of much more hardware than would otherwise be necessary. In addition, many operational requirements cannot be met by dedicated systems because of the lack of direct, rapid multi-level information sharing. One group of experts <AND72> has estimated that these additional costs may amount to $100,000,000 per year for the Air Force alone.

1.2 Vulnerability of Current Systems

The internal controls of current computers have repeatedly been shown insecure through penetration exercises on such systems as GCOS, WWMCCS, IBM 360/370, UNIVAC 1100, PDP-10 TENEX, and others <AND71, KAR74, ALE74, ABB76>. This inability to provide effective security is a fundamental weakness of contemporary systems and cannot be corrected by merely modifying or patching conventional operating systems.

Even if every known security weakness in a particular system were repaired, there would be no basis to believe that every existing weakness had been found. Further, the modifications required to repair the weaknesses are typically so complex as to have a high likelihood of introducing new vulnerabilities. Thus, the approach of penetrating the system and fixing the holes never reaches completeness and cannot achieve computer security (although it can provide job security for system penetrators).

1.3 Impact of Networks on Security

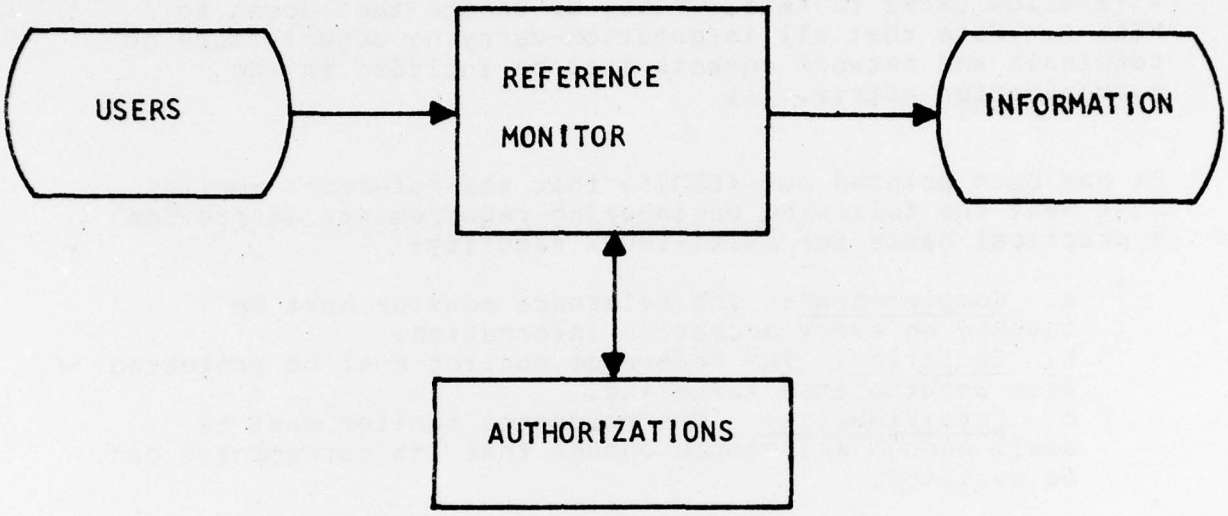
The computer networks that are being constructed today (ARPANET, PWIN, etc.) do not have adequate security for the military. As a result, these networks can have a major adverse security impact by:

1. Dramatically increasing the number of users with potential unauthorized access.
2. Potentially making the security controls on a specific host irrelevant by making information accessible to other hosts that do not have effective security controls.
3. Introducing additional vulnerabilities through the lack of effective security controls in network elements, e.g., insecure network communications processors.

II. Fundamental Basis for Effective ADP Security Controls

To develop a demonstrably secure system, one must start with fundamental understanding of what it means for a computer system to be "secure." To do this, one can model security processing using the concept of a reference monitor which mediates all accesses to information. This reference monitor concept must be applied to all parts of a network -- the ADP host systems and the network interface processors.

The reference monitor (See Figure 1) must implement two basic functions: REFERENCE and AUTHORIZE. The REFERENCE function mediates users' accesses to information and decides whether to allow an access based on an authorization matrix. The AUTHORIZE function updates the authorization matrix based on already existing authorizations.



FUNCTIONS

REFERENCE: USER X INFO X AUTHORIZATION → ACCESS
AUTHORIZE: USER X AUTHORIZATION → AUTHORIZATION

FIGURE 1 REFERENCE MONITOR

The authorization matrix is like that of Lampson <LAM71>. An example of an authorization matrix is shown in Figure 2. In this example, USER1 has READ access to FILE A, while USER2 has READ, WRITE, and CONTROL access. Therefore, the reference monitor will only allow USER1 to read FILE A, but will allow USER2 to read, write, or change the access to FILE A. Note that all information-carrying objects such as terminals and network sockets must be included in the authorization matrix. (1)

It has been pointed out <ESD75> that the reference monitor must meet the following engineering requirements to provide a practical basis for multi-level security:

a. Completeness: The reference monitor must be invoked on every access to information.
b. Isolation: The reference monitor must be protected from unauthorized tampering.
c. Certifiability: The reference monitor must be small enough and simple enough that its correctness can be verified.

The requirement of certifiability leads one to conclude that conventional operating systems, communications processors, and network processors cannot achieve multi-level security. Not only is the software in such systems is so complex and so monolithic that it is impossible to certify correct, but also there is no precise, sufficient security criterion upon which to base the verification.

The engineering requirements of the reference monitor lead to the conclusion that an actual implementation requires a mixture of hardware and software support. The most promising approach for implementing the reference monitor has been called the "security kernel". <LIP74-2> To meet the completeness requirement efficiently, descriptor driven hardware (2) is used to mediate all references by the CPU to

---

(1) In fact, the state of the matrix itself is also information and must be controlled by the monitor. For a full discussion of this issue, see Bell <BEL75>.

(2) Descriptor driven processors include the Honeywell Level 68, the DEC PDP-11/45, and the Burroughs 6700.

	FILE A	FILE B	TERMINAL 17	• • •
USER 1	READ	READ WRITE	RECEIVE TRANSMIT	
USER 2	READ WRITE CONTROL	NULL	NULL	
USER 3	NULL	READ WRITE CONTROL	NULL	
• • •				

FIGURE 2 AUTHORIZATION MATRIX

memory. (1) To meet the isolation requirement, the security kernel software runs in the most privileged state of a multiple state machine. The other states are used for the operating system and the user code. Finally, to meet the certifiability requirement, the security kernel software must be separated from the bulk of the operating system and subjected to a proof of correctness. <MIL76>

III. Goals of ADP Networks

The primary purpose of a network of ADP host systems is to provide convenient responsive data communication between systems. The host computers are general purpose ADP systems that directly interface with local users. The network interfaces are communications processors that in some fashion interface between the host computers and the rest of the network. Such a network must be designed to:

1. Provide information sharing by distributing data bases among many host computers.
2. Provide resource sharing by making unique hosts available on the network and by load sharing among host computers.
3. Provide information security by ensuring that no user obtains unauthorized access to information.

This paper primarily addresses the requirements to meet the goal of information security; however, security should not degrade other functional requirements. These include lucid user interfaces for terminal protocols, file transfer protocols, and remote job entry protocols. Reasonable performance requirements include both the ability to echo

---

(1) Machines such as the PDP-11/45 and Honeywell Level 68 provide descriptor based addressing from the CPU to memory, but not from I/O devices to memory. To maintain security in these machines, I/O must be performed by the security kernel rather than by user programs resulting in an increase in kernel complexity and an adverse performance impact. The Electronic Systems Division has sponsored development of a Security Protection Module (SPM) which can provide upwards compatible descriptor based addressing for a minicomputer and its I/O devices, thus solving the complexity and performance problems. The SPM is being first tested with a ruggedized version of the Honeywell Level 6 minicomputer to perform as a secure ruggedized network front-end processor. <GIL76>

input characters to remote full duplex terminals over thousands of miles in under half a second and also the ability to transfer large (>100,000,000 bits) files at effective transfer rates of better than 10,000 bits per second, with error rates less than 1 bit in 100,000,000 messages.

IV. Issues in Network Security

The basic requirement of a secure network is to provide a protected path between known subjects and information <LIP74-1>. Meeting this requirement decomposes into two logical tasks:

1. Establishing the protected path; and
2. Protecting the protected path.

These tasks may be accomplished automatically by the network or manually by procedures.

Establishing the protected path is the issue of identification and authentication. An external convention must be agreed upon to identify users and some type of authentication to validate the claimed identity. The login name-password combination of the traditional time sharing system may be used. Alternatively, the possession of a cryptographic key may provide evidence of a valid identity.

Protecting the protected path breaks down into two issues: protected communications and access control. Communications links, of course, must always be protected. Any traffic that passes over physically insecure communications paths must be enciphered. Encipherment normally occurs today on communication links between interface processors using outboard cryptographic devices. (See figure 3). Research is on-going in end-to-end encryption <KEN76> in which encipherment occurs at the originating processor and decipherment occurs at the destination processor. Intermediate processors would see only enciphered text. The feasibility of secure end-to-end encryption has yet to be demonstrated in a packet switched computer network.

However, encryption solves no problem except transmission security. If any host or interface computer handles unenciphered data of any form of multiple security levels,

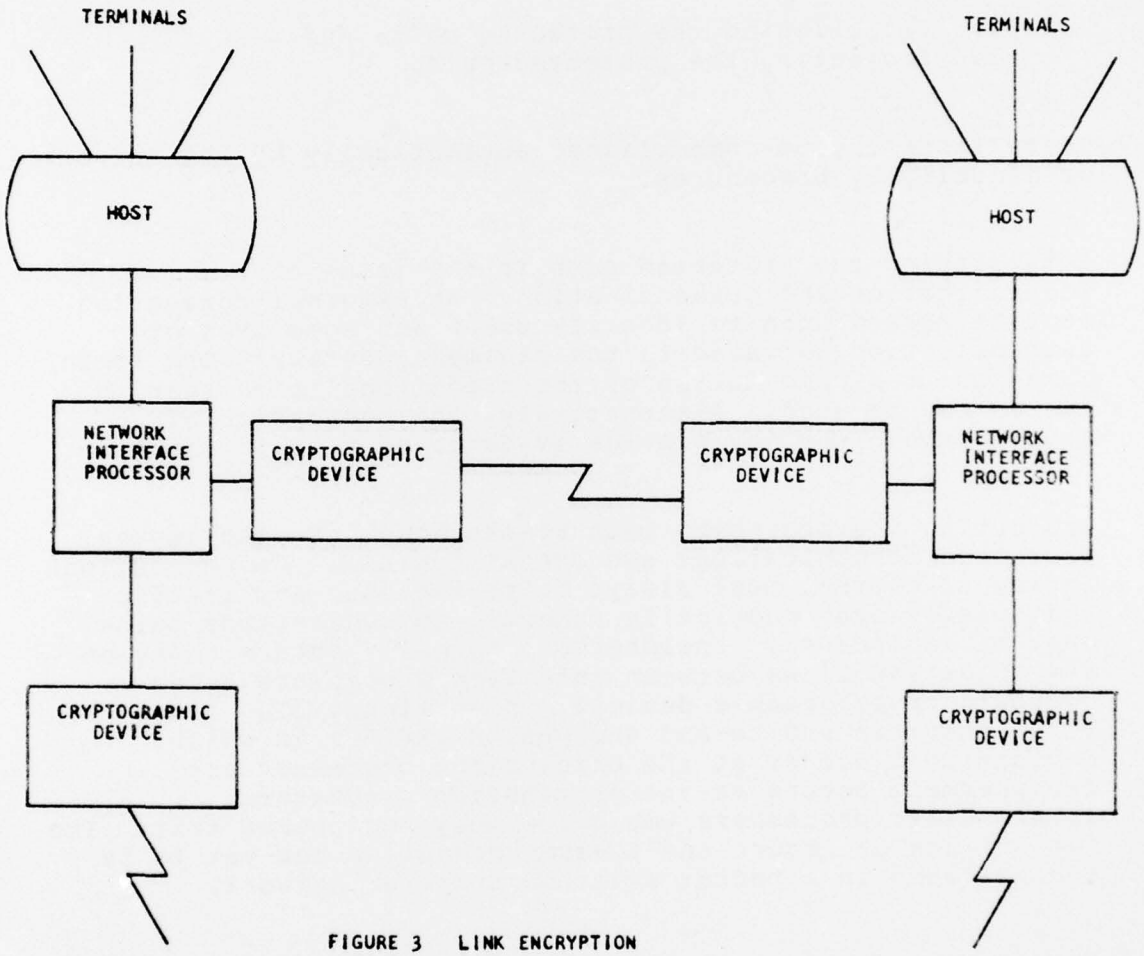


FIGURE 3 LINK ENCRYPTION

then that computer must provide certified secure access control to ensure that data is not released to unauthorized users. In the one-level network of Section 5.1 below, no internal access controls are required. In the one-level host network of Section 5.2, access controls are required in the interface processors. In the multi-level host network of Section 5.3, access controls are required in the host and the interface processors.

V. Network Structures

This section will briefly describe several alternative network structures, all of which effectively protect classified information.

5.1 One-Level Network

The single-level network structure (See Figure 4) provides security without dependence on effective hardware/software controls in either the host or the interface. There is no need or purpose for security labels, although both the host and interface may contain nominal controls and "security features" for administrative convenience. Procedural controls must insure that only authorized users can access any component of the network; these external controls constitute the reference monitor. Protected communications are required to counter the threat of phone taps. It must be recognized that all the users can potentially access all the information contained in all the hosts of the network. The one-level network is the only network structure that can be readily realized without the application of advanced ADP security technology.

5.2 One-Level Hosts

This structure with one-level hosts and secure interfaces (See Figure 5) can provide effective (although limited) security controls in spite of the inherent weaknesses of the host computers. The network interfaces must enforce the security rules to prevent data from flowing to the wrong hosts. A given host can receive from "lower level" hosts and send to "higher level" hosts. This control can be achieved by treating each host as a single user with only well-defined privileges. The network cannot believe the security labels assigned by the host, but must assign labels based on the level of the host. Communication paths, of course, must be protected. As a practical matter, to be

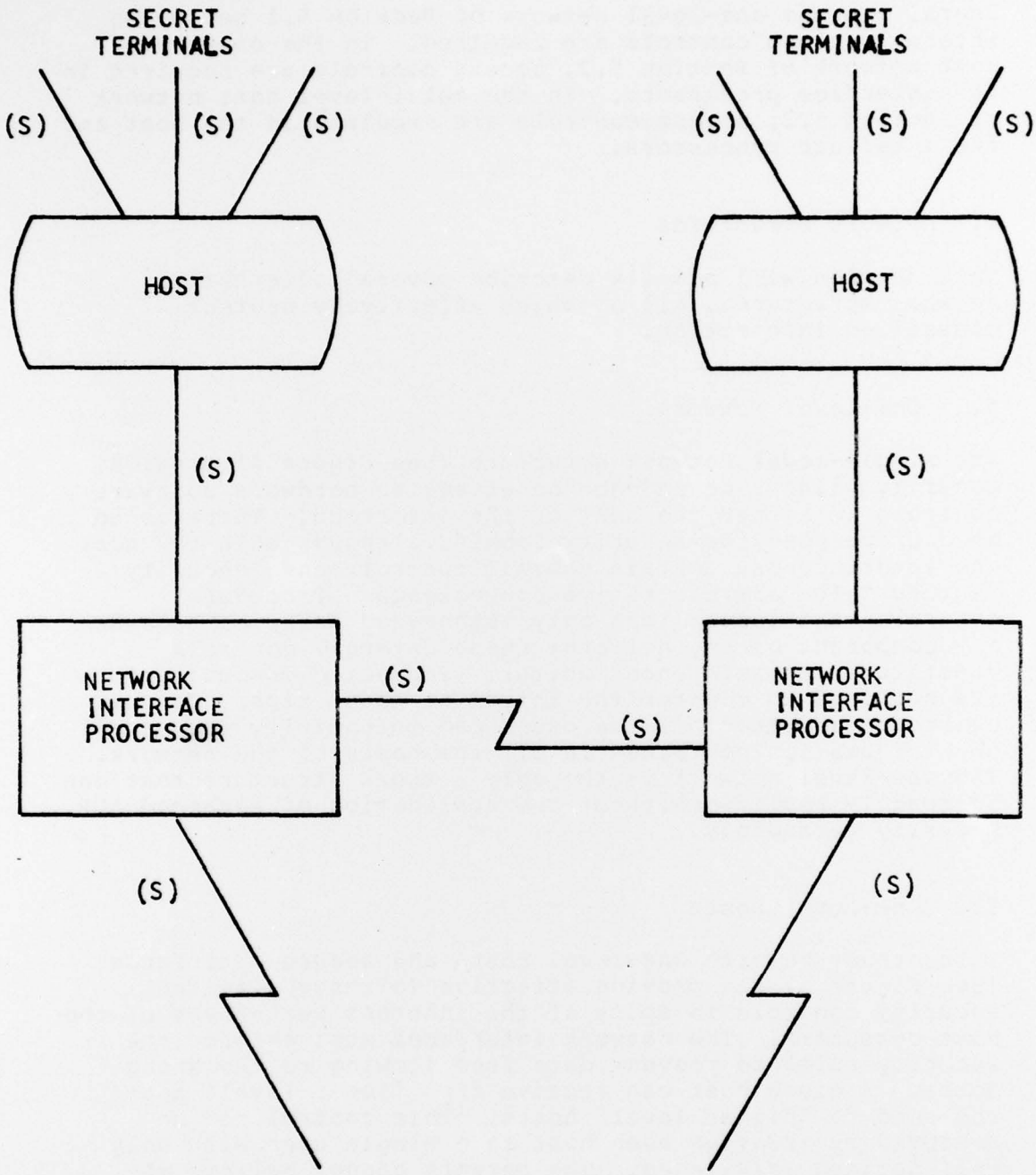


FIGURE 4 ONE-LEVEL NETWORK

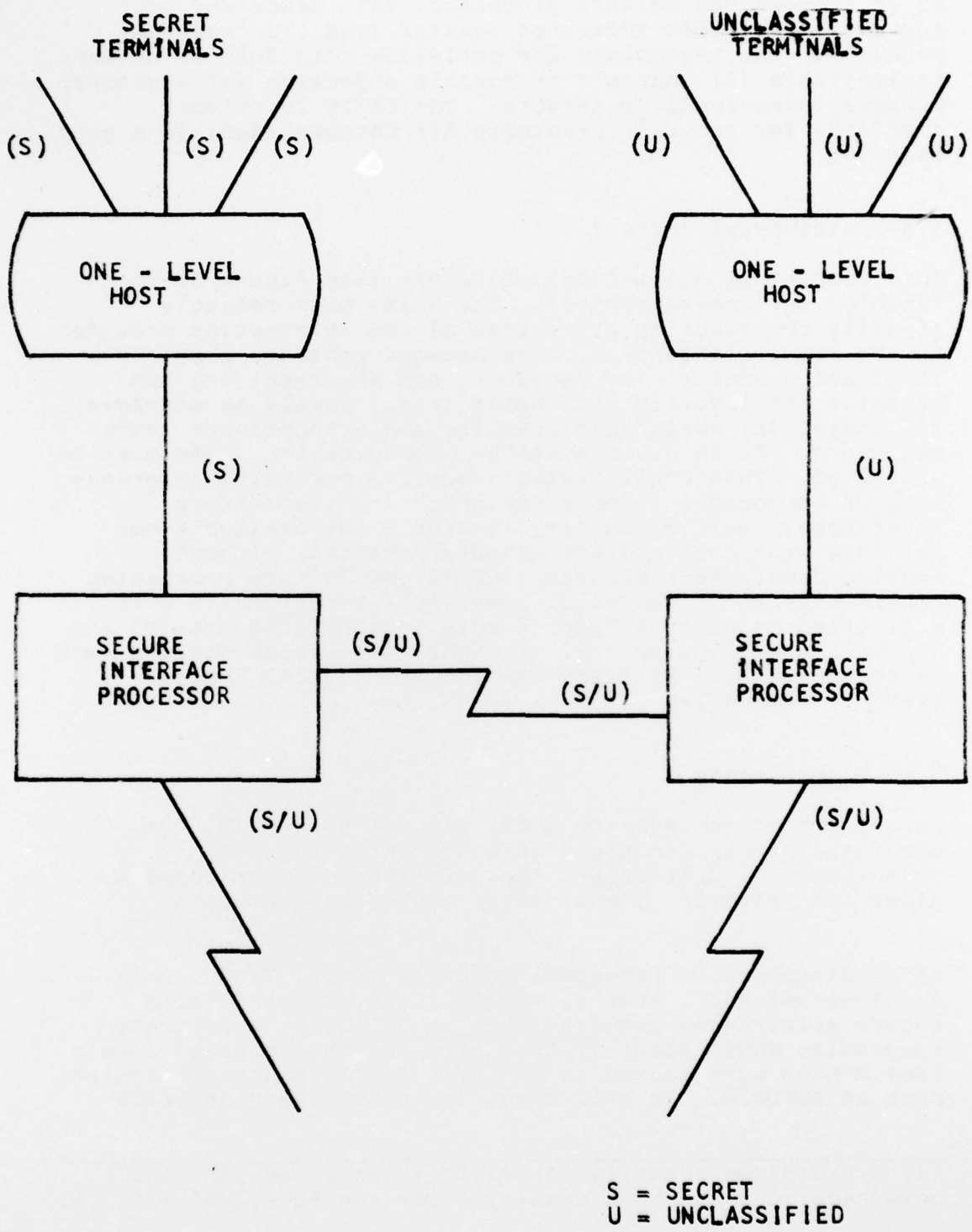


FIGURE 5 ONE-LEVEL HOSTS

effective (for security) the interface must be implemented as an independent network processor; this processor must provide a certified reference monitor (viz., a "security kernel"). The technology for achieving this form of network is available (1) and is a reasonable objective for a general purpose communications network. The SATIN IV network <PAS74-2> for the USAF Strategic Air Command (SAC) is a good example.

5.3 Multi-Level Hosts

This completely multi-level structure (See Figure 6) is "stable" for access control. The hosts must reliably identify the security attributes of the information provided to the network interface. The network protects the information sent to the receiver, and the receiving host believes the security attributes (e.g., labels on messages). The individual hosts must identify and authenticate their own users. As in other systems, communication paths must be protected. This configuration requires certified reference monitor components in both the hosts and the network interfaces; this capability is simply not available nor feasible with contemporary computer systems, although ongoing development efforts <SCHR75, ADL75> are proceeding toward this end. The multi-level host structure is what is most often meant by a "secure data internetting system" and has been the illusive goal of highly integrated designs such as the World Wide Military Command and Control System (WWMCCS) <PAS74-1>.

5.4 Combinations

Pure forms of the systems above are not necessary, but combinations must be based on fundamental security principles, In particular, the reference monitor concept gives the criteria on what is a secure structure.

As an example of a potential security error, if a single-level host, such as WWMCCS, were attached to a secure multi-level network, such as SATIN IV, a security compromise could occur if the untrustworthy security labels from WWMCCS were passed on by SATIN IV to some other system, such as AUTODIN. In this case, the WWMCCS machine could

---

(1) A prototype security kernel that can be adapted for communications has been developed for the PDP-11/45 <SCH75>.

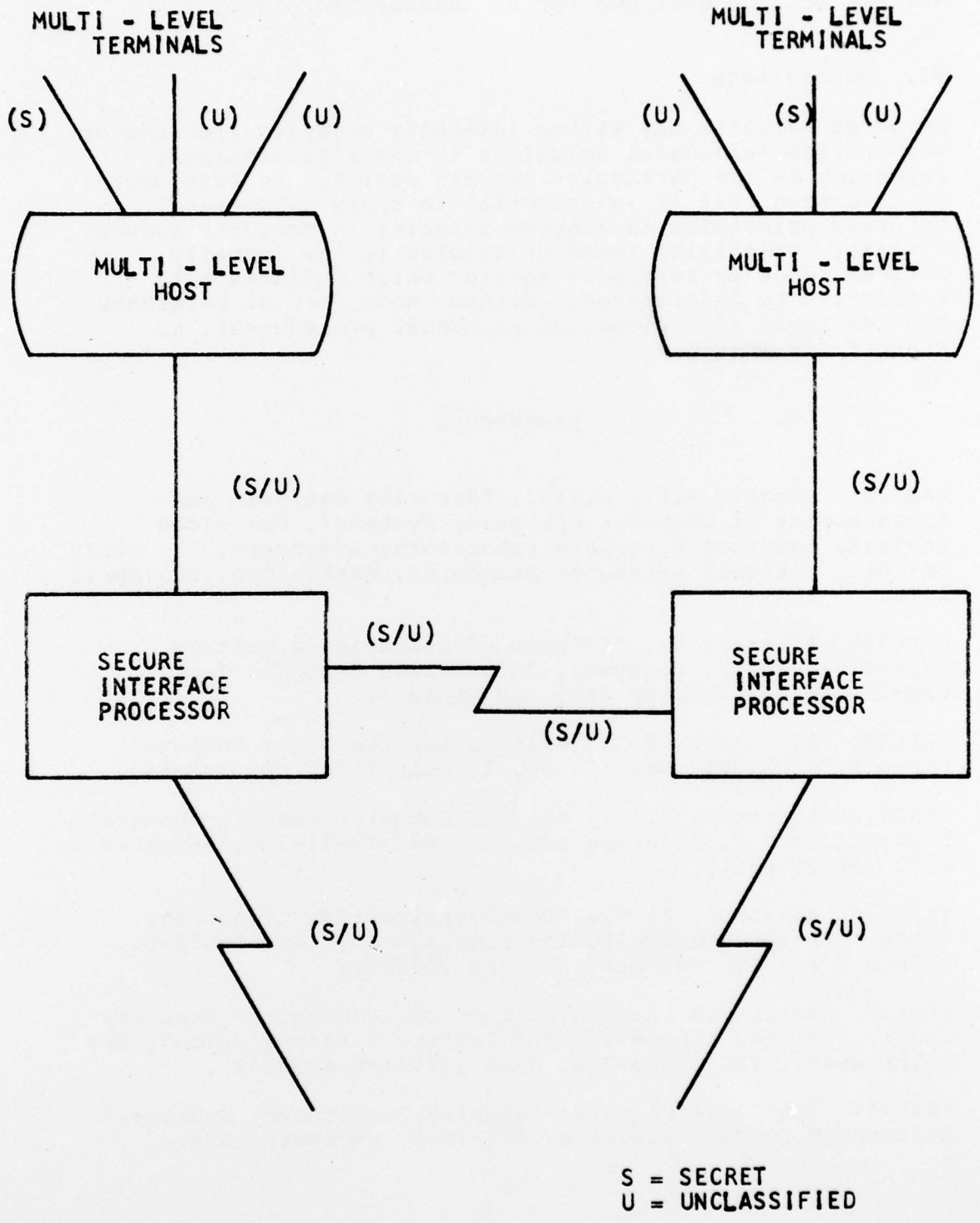


FIGURE 6 MULTI-LEVEL HOSTS

include classified material in an allegedly unclassified AUTODIN message destined for an insecure terminal.

VI. Conclusions

Computer networks may either intensify security problems or may provide meaningful solutions to security problems, depending on the particular network design. In this paper, we have seen that it is essential to apply fundamental security principles to achieve security in computer network systems. Underlying these principles is the formally defined security reference monitor which mediates all references to information. Without some form of reference monitor (even if implemented as manual procedures), no security is possible.

REFERENCES

<ABE76> Abbott, R.P., et.al., "Security Analysis and Enhancements of Computer Operating Systems", The RISOS Project, Lawrence Livermore Laboratory, Livermore, CA, NBSIR 76-1041, National Bureau of Standards, Washington, DC, April 1976.

<ADL75> Adleman, N., "Effects of Producing a Multics Security Kernel", Honeywell Information Systems, Inc., ESD-TR-76-130, October 1975 (AD A031220).

<ALE74> Alexander, Tom, "Waiting for the Great Computer Rip-off," FORTUNE, Vol XC, No. 1, July 1974, pp. 142-150.

<AND71> Anderson, J. P., "AF/ACS Computer Security Controls Study," James P. Anderson and Co., ESD-TR-71-395, November 1971 (AD 251865L).

<AND72> Anderson, J. P., "Computer Security Technology Planning Study," James P. Anderson and Co., ESD-TR-73-51, Volume I and II, October 1972 (AD 758206).

<BEL75> Bell, D.E., and L.J. LaPadula, "Computer Security Model: Unified Exposition and Multics Interpretation", The MITRE Corp., ESD-TR-75-306, June 1975 (AD A023588).

<ESD75> "ESD 1974 Computer Security Development Summary," Electronic Systems Division, MCI-75-1, December 1974.

<GIL76> Gilson, J., and J. Mekota, "Analysis of Secure Communications Processor Architecture", Honeywell Information Systems Inc., ESD-TR-76-351, Vol. I, in progress.

<KAR74> Karger, P. A., and R. R. Schell, "Multics Security Evaluation: Vulnerability Analysis," Electronic Systems Division, ESD-TR-74-193, Volume II, June 1974 (AD A001120).

<KEN76> Kent, S. T., Encryption - Based Protection Protocols for Interactive User-Computer Communication, MIT/LCS/TR-162, Laboratory for Computer Science (formerly Project MAC), Massachusetts Institute of Technology, Cambridge, MA, May 1976.

<LAM71> Lampson, B. W., "Protection," Proc 5th Princeton Conf on Information Sciences and Systems, March 1971, pp 437-443.

<LIP74-1> Lipner, S. B., Private Communication, July 1974.

<LIP74-2> Lipner, S.B., "Panel Overview (A Panel Session-Security Kernels)", AFIPS Conference Proceedings, Vol. 43, 1974 NCC, pp. 973-974.

<MIL76> Millen, J. K., "Security Kernel Validation in Practice", CACM, Vol 19, No. 5, May 1976.

<PAS74-1> Paschall, L. M., "C3 and the National Strategy," Signal, April, 1974, pp. 7-10.

<PAS74-2> Paschall, L. M., "Command and Control, Why the Air Force's New Systems are Revolutionary," Air Force Magazine, Vol 57, No. 7, July 1974, pp. 60-64.

<SCH75> Schiller, W. L., "The Design and Specification of a Security Kernel for the PDP-11/45," The MITRE Corporation, ESD-TR-75-69, May 1975 (AD A011712).

<SCHR75> Schroeder, M.D., "Engineering a Security Kernel for Multics", Proceedings of the Fifth SICOPS Symposium on Operating System Principles, November 1975.

MISSION
OF THE
DIRECTORATE OF COMPUTER SYSTEMS ENGINEERING

The Directorate of Computer Systems Engineering provides ESD with technical services on matters involving computer technology, helps ESD system development and acquisition offices exploit computer technology through engineering application to enhance Air Force systems, and develops guidance to minimize R&D and investment costs in the application of computer technology.

The Directorate of Computer Systems Engineering also supports AFSC to insure the transfer of computer technology and information throughout the Command, including maintaining an overview of all matters pertaining to the development, acquisition, and use of computer resources in systems in all Divisions, Centers, and Laboratories and providing AFSC with a corporate memory for all problems/solutions and developing recommendation for RDT&E programs and changes in management policies to insure such problems do not reoccur.