1

MODELING SECURITY IN

LOCAL AREA NETWORKS

THESIS

AFIT/GE/EE/83D-10 Wesley A. Ballenger, Jr.
1st Lt USAF

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY
AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GE/EE/83D-10

MODELING SECURITY IN
LOCAL AREA NETWORKS

THESIS

AFIT/GE/EE/83D-10 Wesley A. Ballenger, Jr.
1st Lt USAF

Approved for public release; Distribution unlimited.

AFIT/GE/EE/83D-10

MODELING SECURITY IN LOCAL AREA NETWORKS

THESIS

Presented to the Faculty of the School of Engineering
of the Air Force Institute of Technology
Air University
in Partial Fulfillment of the
Requirements for the Degree of
Master of Science

by

Wesley Allan Ballenger, Jr., B.S.
1st Lt USAF
Graduate Electrical Engineering

14 December 1983

Approved for public release; Distribution unlimited.

Preface

Computer networks must have the capability to protect the information they contain, especially if the information is sensitive or classified for national security purposes. This research effort analyzes the security aspects of local area computer networks and presents a textual definition of a local area network (LAN) security model.

I would like to express my deepest appreciation to Major Walter D. Seward, who as my thesis advisor gave me guidance and encouragement throughout this research. I also thank the other members of my thesis committee, Dr. Thomas C. Hartrum and Captain John S. Gordon for their close reviews of my thesis drafts and their constructive comments to improve the content and clarity of this thesis.

Finally, I wish to thank my wife, Judi, and my son, Wesley. They endured the endless hours I spent on this research, and their patience and understanding enabled me to complete this graduate program.

Wesley Allan Ballenger, Jr.

Table of Contents

List of Figures

AFIT/GE/EE/83D-10

Abstract

The Department of Defense needs to process data at various levels of security in Local Area Networks (LAN) of computer systems. A formal computer network security model is a necessary first step in certifying a computer system to process classified data. Several computer security models have been developed to identify what is required to enable multilevel certification of a computer system, and a similar model is needed for LANs.

The primary objective of this research project is to analyze the requirements of a LAN security model. Conceptual design issues of LAN security modeling are presented in this thesis to identify what must be achieved to ensure security is not violated when data of various levels of security are processed in a local area network.

Due to their distributed nature, LANs involve several security issues not addressed in security models (such as the Bell-LaPadula security model) developed for single computer systems. Therefore, modeling of security in LANs and computer networks must be complemented with LAN application and implementation considerations, primarily associated with secure communications channels between LAN subscribers.

This thesis analyzes the security requirements of a local area computer network, highlighting the need for a "security architecture" approach to modeling security in LANs. A textual definition of a prototype LAN security model is presented, and the model´s application to hypothetical LAN configurations is discussed.

I. INTRODUCTION

Computer technology has advanced rapidly within the past decade, resulting in the trend away from a single "batch processing" computer environment and towards highly interactive, real-time, user-friendly computer systems. Similarly, time-sharing of computer resources has been expanded to the development of networks of computer systems. Although the interconnection of many computer systems to comprise a computer network offers numercus advantages and user flexibility, the problem of data security may be aggravated. Protection of data, particularly classified data, within a computer system or computer network is a primary concern within the Department of Defense.

Therefore, the primary objective of this research project is to identify and analyze the conceptual design requirements of ensuring the security of classified data in a local area network (LAN) of computers.

In recent research and development efforts to design and build secure computer systems, computer security models have first been developed to provide a concise and precise description of the behavior desired of the security-relevant portions of the computer system. The certification (accredidation) of a computer system to process classified data at various security levels depends on the provability of the security enforcement mechanisms within the computer system. Formal security models, such as the Bell and LaPadula model (described in Chapter 3), have provided the security enforcement criteria which must be implemented in a computer system design. Certification of local area computer networks to process classified information of various security levels is a topic of current interest and research within the Department of Defense (LAND81, LAND82, SIDH82, WORM82).

A formal computer security model is a necessary first step in designing and certifying a ccmputer system to process classified data. Several computer security models have been developed to identify what is required to enable multilevel certification of a computer system (LAND81). A similar model is needed to identify what must be achieved to ensure security is not violated when data of various levels of security are processed in a local area computer network.

However, unlike modeling security in single computer systems, modeling security in LANs may take into account certain implementation considerations which may be specific to a particular LAN configuration. These implementation considerations arise due to the distributed nature of LANs, which may be comprised of many heterogenous host computer systems distributed geographically. Therefore, in addition to ensuring security within each host computer, a "global" perspective to analyze the data security requirements within the entire LAN must be considered. Due to the many different potential LAN configurations, specifications, and applications, the development of a single "LAN security model" may prove to be an infeasible solution. Instead, the coordinated development of a "security architecture", which integrates both security policy models and LAN implementation consideration, may result in a more useful analysis tool of the overall LAN security requirements. This thesis addresses the requirements and conceptual design issues of such a LAN security architecture, including a textual definition of a prototype LAN security model.

Computer Networks

A computer network is comprised of individual computer systems with the capability to communicate with each other via some type of communications medium. The individual computers may be large mainframe computer systems, supercomputers, minicomputers, or small microcomputer systems such as a desktop personal computer.

The computers linked by the network may be geographically remote from each other, separated by thousands of miles, and may use a communications link via a satellite orbiting the Earth. Alternatively, the individual computer systems may be in the same room, physically linked by wires.

A local area network (LAN) lies between these two extremes, and is generally defined to cover a geographic area of no more than several square miles. Examples of LAN coverage would be a university campus, a single office building, or a portion of a city. Although a particular LAN may provide service to a specific geographic area, the LAN may contain one or more "gateway" nodes, or interfaces with other computer networks (either LANs or long-haul networks). An example of this would be a LAN with a gateway node to ARPANET (the Defense Advanced Research Projects Agency Network), which is a national long-haul computer network. In this example, the LAN subscribers would also have access to the ARPANET computer resources in addition to the LAN's local computer resources.

Conventional network configuration and analysis considers such parameters as placement of network nodes (network topology), information flow patterns and rates within the network, and average response time to the individual network user (TANE81). This research project extends this parameter list to include data security considerations. The level of data protection and security provided within a network may impact any or all of the above parameters, particularly information flow patterns and overall network throughput and response time.

There are a number of current network architectures (both long-haul and LAN), including ARPANET, Ethernet (a popular LAN which is included in IEEE Standard 802 on

LANs) IBM's Systems Network Architecture (SNA), and Digital Equipment Corporation's Digital Network Architecture, as well as architectures for specialized applications. Although many distinct network implementations have been proposed and designed, an attempt has been made to try to standardize the interfacing of various network components.

Network Protocol Layers

The International Standards Organization (ISO) has proposed an architecture model with the potential for universal networking as a first step toward network protocol standardization (TANE81). This model is called the open systems interconnection (OSI) reference model, and is shown in Figure 1.

Each of the seven protocol layers in the OSI reference model represents a different level of abstraction of the communication between computer systems. The physical layer is concerned with transmitting raw bits over a communications channel, focussing primarily on the design issues dealing with mechanical, electrical, and procedural interfaces to the subnet.

The data link layer takes the raw transmission facility of the physical layer and transforms it into a line that appears free of transmission errors to the network layer. This is accomplished by arranging the input data into data frames, transmitting the frames sequentially, and processing the acknowledgement frames sent back by the receiver.

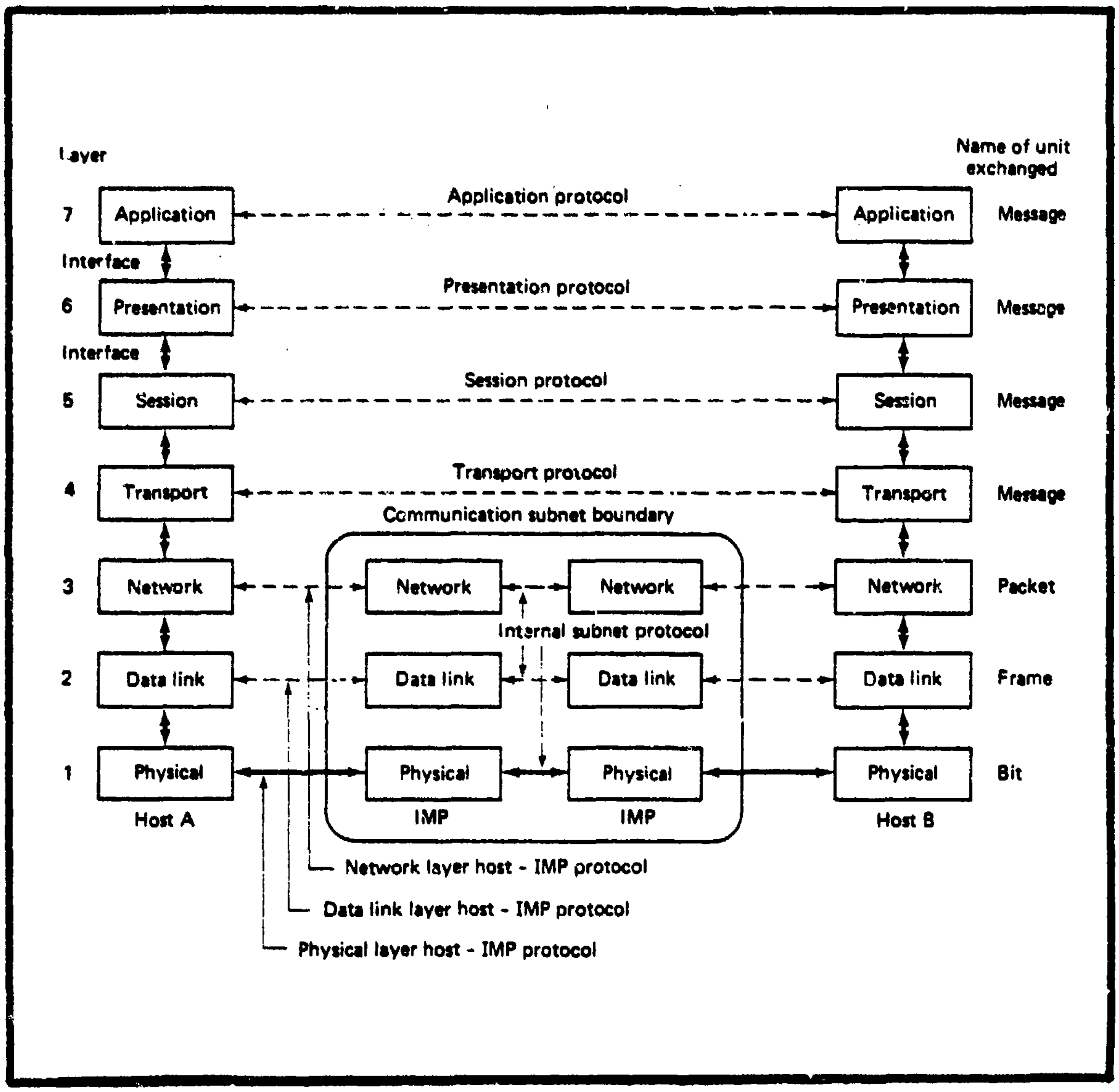

Figure 1:
Open Systems Interconnection (OSI) Reference Model
(TANE81)

The network layer (sometimes called the communications subnet layer) controls the operation of the subnet. This layer basically accepts messages from the source host, converts them into packets of data, and ensures that the packets are properly addressed to the destination computer.

The transport layer (also known as the host-to-host layer) accepts data from the session layer, splits it up into smaller units (if necessary), and passes these to the network layer. The network layer also ensures that the pieces all arrive correctly at the other end.

The session layer provides the user's interface to the network. This layer establishes a connection to another host within the network. A connection between users is usually called a "session".

The presentation layer performs functions that are requested sufficiently often by users to warrant a "library" of routines availible to the user, such as text compression or data encryption (which will be discussed further in Chapter 4).

The application layer is the top level of the protocol abstraction, and is generally concerned with network transparency, or hiding the physical distribution of resources from the user.

Computer networks are designed as a series of protocol layers, with each layer being responsible for some aspect of the network's operation. These protocols serve as the focal points for interfacing one or more computer systems within a computer network.

The impetus for computer networks is to facilitate information exchange among a variety of users, each of whom may require access to common data bases and other computer resources shared within the network. This advantage of allowing each network user access to any of the information contained in the network introduces the problem of protecting sensitive and personal information from disclosure to unauthorized users.

Information Security

With the advent of the "Information Age", the ease of illegally and covertly accessing private (either corporate or government) computer systems and their respective data bases has received much media attention (COMP83). In particular, the need to protect information stored by electronic means has been focused upon. The ever-increasing reliance upon electronic storage of information necessitates the incorporation of security as a primary design consideration, especially in computer systems and networks which process sensitive or personal information. Although there are numerous and various requirements to protect sensitive information, this thesis will consider primarily the area of military security, the structure of which will be described in detail in Chapter two.

Information security is a problem whether we are discussing individual host computers, long-haul computer networks, or LANs. The distributed nature of computer networks complicates the problem of information security. In particular, certain attributes of LANs exacerbate the problem of guaranteeing information security. One such attribute is the network access scheme, dealing with the lower protocol layers of the ISO reference model. A network access scheme at the lower protocol layers specifies how information is to be transmitted between network nodes. One popular implementation of the lower two protocol layers is called "Carrier Sense Multiple Access with Collision Detection" (CSMA/CD).

CSMA/CD is a random-access scheme in which a network node competes with other nodes for use of the network media (multiple access). Before a node can transmit a message, it must first listen to the desired channel to make sure that it is not busy. The node recognizes a busy channel by detecting the presence of a carrier frequency ("carrier sense"). If busy, the node cannot transmit until the channel is clear. Once transmission starts, the node must monitor the channel again to make sure that no other nodes are transmitting on the channel at the same time (collision detection). If messages do collide, the transmission is aborted and the node waits or backs off for a random period of time before it attempts retransmission.

CSMA/CD is an example of a "broadcast" method of communication, where each node in a LAN broadcasts a message to all other nodes. The message contains addressing information to indicate the intended recipient of the message, but all nodes attached to the LAN medium may potentially "eavesdrop" on a message. Unless the contents of the message are protectad somehow (i.e., via data encryption), the potential for an unauthorized listener on the network to intercept sensitive data messages may be great. This is an example of the exploitation of the network protocols to compromise data security.

Computer Security Models

A computer system or network which is to be certified secure or accredited to process classified information must meet certain security-related criteria. To date, the security criteria have been in the form of a formal security model which describes the access to information within a computer system and the flow of information within a computer system (LAND81). Security models will be discussed in detail in Chapters 3 and 4 of this thesis. In Chapter 3, the applicability of past computer security models to LANs will be discussed, emphasizing the need to integrate security policy models with LAN implementation considerations. Chapter 5 presents a textual definition of a prototype LAN security model, including example applications of the model to particular LAN configurations.

Research Objective

The original specification of this research project stated that the objective would be to develop a formal security model for local area networks. In the early stages of research, it became obvious that the development of a formal mathematical model (such as the Bell and LaPadula security model described in BELL73b and BELL74) for LANs was well beyond the scope of a master's thesis project. Instead, the research objective focussed on developing a more informal, pseudo-English, textual security model for LANs, similar to the informal security model proposed for military message systems (MMS) in LAND82. Due to the distributed nature of LANs and the variety of application-specific implementation considerations, a more promising approach to modeling security in LANs appears to be the coordinated development of a "security architecture", which integrates both security policy models and LAN implementation considerations.

Therefore, the ultimate objective of this research project is to identify and analyze the conceptual design requirements of ensuring the security of classified data in a local area computer network. This thesis will analyze the requirements of a local area network computer security model and present a prototype LAN security model, highlighting the need for a "security architecture" approach to modeling security in LANs. This thesis will address what must be achieved to ensure security is not violated when data of various levels of security are processed in a local area network.

Approach and Scope

A secure computer network may only be designed and certified to process classified information after first defining a formal model of the security policy to be enforced by the network. The scope of this thesis, therefore, is to identify and explore the security-specific design issues associated with a local area network. Conceptual design issues for a LAN computer security architecture (which may be applied to existing computer networks or used as a guideline for incorporating security in future local area networks) will be presented, emphasizing the distinction between security policy and LAN implementation considerations.

The net result is to underscore the need for a security architecture which is tailored to a particular LAN application (or class of applications). By carefully integrating security policy issues with LAN implementation issues, the end result should facilitate the verification of a particular LAN's security enforcement properties. Although the development of a formal mathematical model specification (as in BELL73b, BELL74) is beyond the scope of this research project, a textual definition of a LAN security model is presented and discussed.

Organization

This report contains six main chapters followed by a Conclusions and Recommendations chapter. This first chapter provides a brief introduction to security considerations in local area computer networks by discussing computer networks and information security. Further, this first chapter defines the research objective and its associated scope of effort, and outlines the organization of this thesis.

Chapter 2 then presents several important security concepts, including a discussion of military security, potential threats to security, and a description of the four basic modes of computer operation the Department of Defense uses to accredit computer systems processing classified information. Chapter 3 discusses specific security models, emphasizing the difference between the LAN implementation considerations of a secure network and the modeling of the network security policy to be enforced. Next, several approaches and implementation considerations (such as physical security and data encryption) of designing multilevel secure LANs are discussed in Chapter 4, again emphasizing the distinction between the implementation considerations and the security policy model.

Chapter 5 then presents a textual definition of a prototype LAN security model, including a discussion of the application of the model to particular LAN configurations. Chapter 6 further explores the critical design issues of secure communications channels within the network and the inclusion of security in the specification of the network protocols. Chapter 6 also illustrates the interdependance of a security policy model and the various design implementation considerations discussed in earlier chapters. The ultimate goal is to apply knowledge of both security policy models and LAN implementation constraints to meet the objective of processing multilevel secure (MLS) information in a local area network.

Conclusions aud recommendations for further study are presented in Chapter 7, followed by an appendix which documents a particular data security unit available at AFIT for possible future research in the incorporation of data encryption in computer networks.

Summary

The ever-increasing reliance upon electronic storage of information necessitates the incorporation of security as a primary design consideration, especially in computer systems and networks which process sensitive or personal information. Therefore, this research project identifies and analyzes the design requirements of ensuring the security of classified data in a local area network of computers.

II. SECURITY CONCEPTS

Data security in computer networks is becoming increasingly important, owing to the expanding role of distributed computation, distributed databases, and telecommunication applications such as electronic mail and electronic funds transfer. Additionally, the Department of Defense needs to process data at various levels of security while ensuring that unauthorized access to classified information will not occur. Although there are numerous and various requirements to protect information, both corporate and government, this thesis will consider primarily the area of military security.

Hierarchy of Military Security

Military security is necessary due to the existence of information that, if known by an enemy, could potentially damage the national security. The hierarchy of military security recognizes the need for different sensitivity levels, since not all information is equally sensitive to disclosure. The recognized sensitivity levels, in increasing order of impact on national security, are "Unclassified", "Confidential", "Secret", and "Top Secret". Information that has been assigned any of the three levels above "Unclassified" is referred to as "Classified" information.

In addition to a sensitivity level, a finer degree of classification has been created based on an individuals's "need-to-know". Although this "need-to-know" princip applies to all classified information, in some case information relating to specific subject areas is formally designated as a separate category or "compartment" of information (LAND81). Compartment designations are in addition to the sensitivity level designation. Compartments may overlap, with some information designated as being in two or more compartments. Therefore, a "classification" (also referred to as "security level" or "security partition") consists of both a sensitivity level and a (possibly empty) set of compartments.

This structure of military security is generally modeled as a two-dimensional matrix, or "lattice". One axis may represent the sensitivity levels, and the other axis may represent the compartment(s). Therefore, a particular security partition may be represented in a digital computer as a point or set of points within the lattice. Figure 2 illustrates such a lattice hierarchy, with a global lower bound of "Unclassified - No Categories" and a global upper bound of "Top Secret - All Categories".

Since the purpose of the classification system is to prevent the uncontrolled dissemination of sensitive information, mechanisms are required to ensure that those individuals allowed access to classified information will

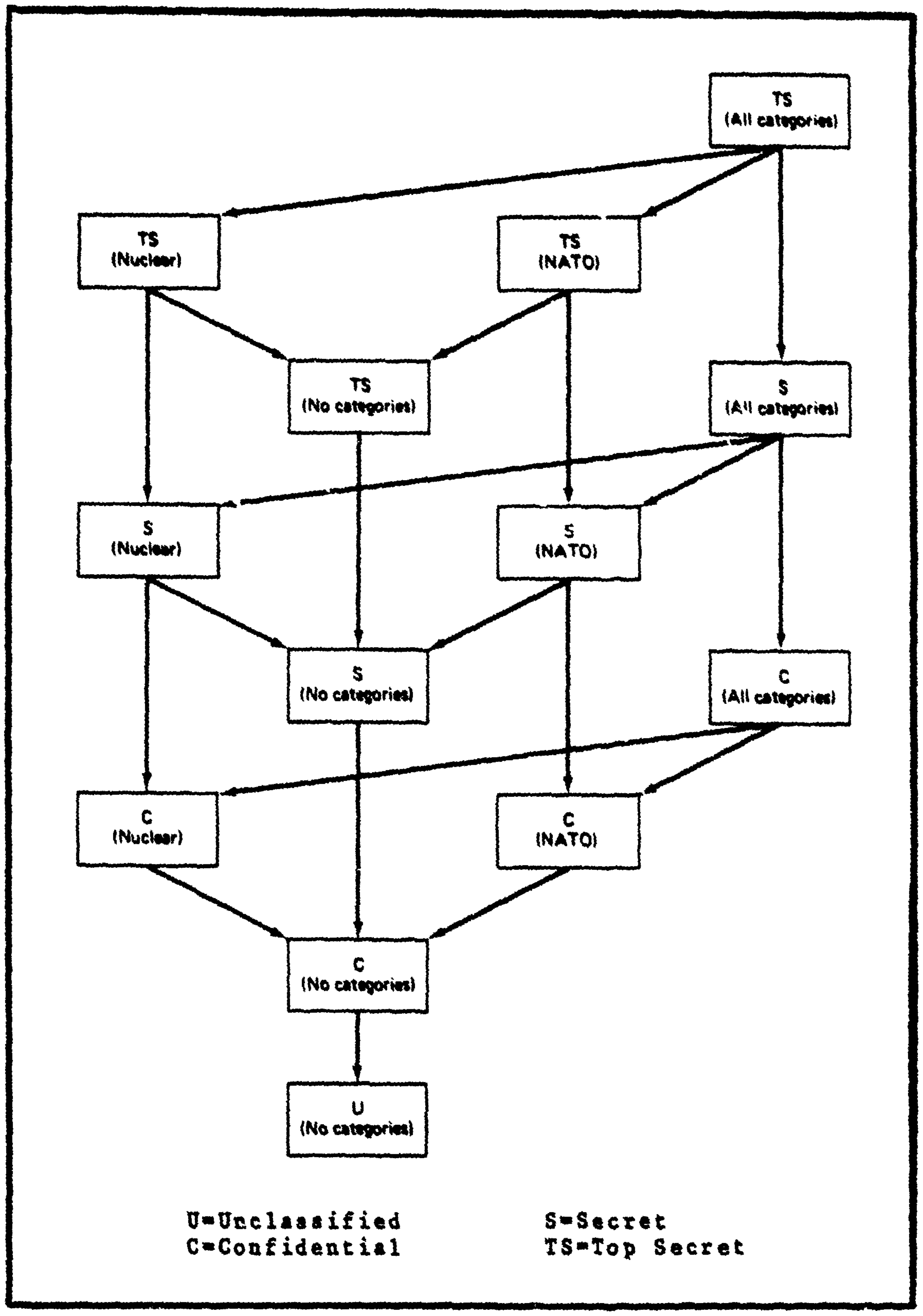

Figure 2 - Example Lattice for Military Classification (KU081)

not distribute it improperly. A security "clearance" may be granted to an individual, indicating that certain formal procedures and investigations have been carried out and that the individual is trustworthy with information up to a certain security level. Therefore, security policy dictates which individuals (based on the individual's security clearance) may have access to certain classified information (based on the security classification of the information). In a computer system or network, the enforcement of a security policy first involves the identification of potential threats to the security of the information contained within the computer or network of computers.

Security Threats

The use of computers to store and modify information may greatly simplify the composition, editing (word processing), distribution (electronic mail), and reading of messages and documents. However, information contained in a computer system must be protected from three primary threats:

1. Unauthorized disclosure of information.
2. Unauthorized modification of information.
3. Unauthorized withholding of information (denial of service).

In the military security system, an individual is authorized to view information classified within his own security clearance (sensitivity level plus need-to-know). The first threat above describes the case where an individual is able to gain access to information classified above his own security clearance level. The second threat arises if an individual, even though he may possess the appropriate security clearance to view a classified document (or to read a file), is able to modify the document (or to write to a file) without possessing the authority to modify it. The third threat depicts a potential situation in which an authorized user with an appropriate security clearance is denied access to a classified document (inadvertently or intentionally). Landwehr also discusses subclasses of these threats along with other threats, noting that most formal security models do not address threats such as wiretapping (LAND81).

Each of these three primary threat areas are further aggravated when computer systems are interconnected via a network such as a LAN. A single computer system may incorporate a centralized "security kernel" or some other single security focal point responsible for enforcing a security policy. A network of computers may or may not contain a centralized security focal point, and the security enforcement mechanisms may themselves become distributed throughout the network. For example, the

CSMA/CD network access protocol (described in Chapter 1) actually broadcasts all network messages to all network subscribers, assuming that only the network node to which the message is addressed will bother to process it. This poses a significant problem in protecting the network messages from unauthorized disclosure to other network subscribers who may not possess the necessary security clearances. Some form of communications security, such as the encryption of the actual data messages within the network, must therefore be an integral part of the network design.

The visibility of all network data traffic to all LAN subscribers poses a significant potential security threat that must be addressed. Some means for separation of network data traffic according to security partitions or even individual sessions must be incorporated into a secure LAN architecture to provide "virtual communication channels" that are secure.

Multilevel Security Considerations

Multilevel security refers to maintaining a separation of data at a wide range of security levels. A realistic operational scenario for a local area computer network required to process classified data indicates the need to simultaneously service users at a variety of security levels while providing full multilevel protection of the data. In contrast, single-level security means that a resource is only allowed to process data at one particular classification level.

At present, the Department of Defense uses four modes of operation to accredit computer systems processing classified information (LAND83):

1. Dedicated: All system equipment is used exclusively by that system, and all users are cleared for and have a need-to-know for all information processed by the computer system.
2. System High: All Equipment is protected in accordance with requirements for the most classified information processed by the system. All users are cleared to that level, but some users may not have a need-to-know for some of the information.
3. Controlled: Some users have neither a security clearance nor a need-to-know for some information processed by the system, but separation of users and classified material is not essentially under operating system control (i.e., manual intervention by a system security officer).
4. Multilevel: Some users have neither a security clearance nor need-to-know for some

> information processed by this system, and separation of personnel and material is accomplished by the operating system and associated system software.

Definitions of these modes are provided in DoD Directive 5200.28 (DOD78). Depending on the operating environment of a LAN, it may need to be accredited for operation in any one of the four modes. Realistically, a LAN will probably need to be accredited for either Controlled Mode or Multilevel Mode, since a variety of users may have access to the LAN and it may be inappropriate or impossible for all LAN users to obtain the highest possible security clearance.

Summary

Data security in computer networks is becoming an increasingly important design issue.. This research focusses upon the military security environment, emphasizing the protection of classified information from unauthorized disclosure. Three primary security threats must be considered, with the added complexity of securing a distributed electronic information media such as a LAN. A means of illustrating the overall approach to security in a complex computer system or network may be embodied as a formal security model of what must be achieved to ensure security policies are not violated. In the next chapter computer security models will be discussed, emphasizing the distinction between security policy models and LAN implementation considerations.

III. COMPUTER SECURITY MODELS

The previous chapter explained various security concepts, including a discussion of military security and information security as it relates to computer systems and networks. The next chapter will offer some insight into the implementation aspects of security in local area networks of computer systems. However, the distinction between a formal security policy model and the actual implementation details of security enforcement mechanisms should be stressed. The transformation from a given security model to an operable, secure computer system or network is, unfortunately, not a well-defined process. In fact, the applicability of computer security models to date has focussed primarily upon a single computer system rather than a network of computers.

Although problems in computer network security are closely paralleled by models and mechanisms developed in the course of research in computer system security, network implementation considerations may introduce some additional complicating factors. For example, security mechanisms incorporated in a single computer system which is accessed via a computer network may be rendered ineffective if the computer network fails to provide a secure communication path between each user and the computer system.

This chapter will discuss computer security models which are in existence today, focussing on the Bell-LaPadula security model and its applicability to modeling security in computer networks. The potential deficiencies of security models as applied to local area computer networks will be presented, highlighting the need to integrate security policy models with LAN implementation considerations to form a security architecture.

Security Models

A computer system or network which is to be certified to process classified information must meet certain security-related criteria, usually in the form of a security model. A system security model defines the security rules or policy that must be enforced by the system implementation.

The "lattice model" of security levels is widely used to represent the structure of military security levels (LAND81, KUO81), as mentioned earlier in Chapter 2. Since a lattice is a finite set of ordered elements, security classifications (which include a sensitivity level and a (possibly empty) set of compartments) may be represented as ordered elements within the lattice.

There are a limited number of security models in existence today, including the UCLA Data Secure Unix model, the Take-Grant model, the High-Water Mark model, and the Bell-LaPadula model (LAND81), the most prominent of which is the Bell-LaPadula model (BELL73a, BELL73b, BELL74). A more recent security model proposed by Landwehr (LAND82) for military message systems (MMS) developed a new approach to defining security models based on the idea that a security model should be derived from a specific application (i.e., the family of military message systems). Both the Bell-LaPadula security model and the MMS security model will be discussed in this chapter.

Bell-LaPadula Security Model

Since the early 1970's the Electronic Systems Division (ESD) of the United States Air Force and the MITRE Corporation have been involved in various projects relating to secure computer systems design and operation. One effort which began in 1972 at MITRE initially produced a mathematical framework and a model by D. Elliott Bell and Leonard J. LaPadula, referred to as the Bell-LaPadula security model. The Bell-LaPadula security model (along with its subsequent refinements) has been widely applied in prototype Department of Defense systems (LAND83). Carl Landwehr presents a detailed accounting of over twenty-five completed and on-going projects to develop secure systems, noting which projects are based upon the Bell-LaPadula model (LAND83).

Bell and LaPadula use finite-state machines and mathematical proofs to formalize their model (BELL73a, BELL73b, BELL74). They first define the various components of the finite-state machine, then formally define what it means for a given state to be secure. Finally, they consider the state transitions that can be allowed so that a secure state can never lead to an insecure state. State representations and transitions rely on the entries in a "access matrix".

Access Matrix

There are three principle components in the access matrix: a set of passive "objects", a set of active "subjects" which may manipulate the objects, and a set of access rules which govern the manipulation of objects by subjects. Each subject has a security "clearance", and each object has a security classification. Each subject also has a "current security level", which may not exceed the subject's clearance.

The access matrix is a rectangular array with one row per subject and one column per object. The entry for a particular row and column reflects the modes of access between the corresponding subject and object. The four modes of access are:

Read-only:	Subject may read the object but cannot modify it
Append:	Subject may write the object but cannot read it
Execute:	Subject may execute the object but

cannot read or write it directly

Read/Write: Subject may both read and write the object

In addition to the four modes of access, a control attribute is defined which allows a subject to pass to other subjects some or all of the access modes it possesses for the controlled object. However, the control attribute itself cannot be passed to other subjects. The control attribute is granted only to the subject that created the object.

Security Properties

In order for a given state to be considered secure, two security properties must hold:

1) Simple Security Property: A subject at a given security level may have read access only to objects at the same or lower security level (referred to as "no read up").

2) *-Property (pronounced "star-property"): No subject may have append access to an object whose security level is not at least the current security level of the subject; no subject has read/write access to an object whose security level is not equal to the current security level of the subject; no subject has read access to an object whose security level is not at most the current security level of the subject.

A set of rules governing the transition from one state to another are required to preserve these two security properties. Bell and LaPadula defined rules to provide the following functions:

A) get (read, append, execute, or read/write) access, to initiate access to an object by a subject in the requested mode;

B) release (read, append, execute, or read/write) access, the inverse of get access;

C) give (read, append, execute, or read/write) access, to allow the controller of an object to extend the designated access to another subject;

D) rescind (read, append, execute, or read/write) access, the inverse of give access;

E) create object, to activate an inactive object or create a new object;

F) delete object, to deactivate an active object;

G) change security level, to allow a subject to alter its current security level.

It is formally, mathematically demonstrated in BELL74 that each of the specified rules preserve both the simple security property and the *-property. One further security principle is called the "tranquility" principle, which asserts that no operation may change the classification of an active object.

Reference Monitor

A reference monitor, as illustrated in Figure 3, utilizes the access matrix to check the validity of a subject's accesses to objects. All accesses to objects are mediated by an enforcement mechanism, the reference monitor, that refers to the data in the access matrix. The reference monitor rejects any accesses (including improper attempts to alter the access matrix data) that are not allowed by the current protection state and rules. To be effective, the reference monitor must be small enough so that its correctness can be proven, and must be tamper proof. The reference monitor is commonly associated with the "security kernel", which is a hardware/software mechanism that implements the reference monitor.

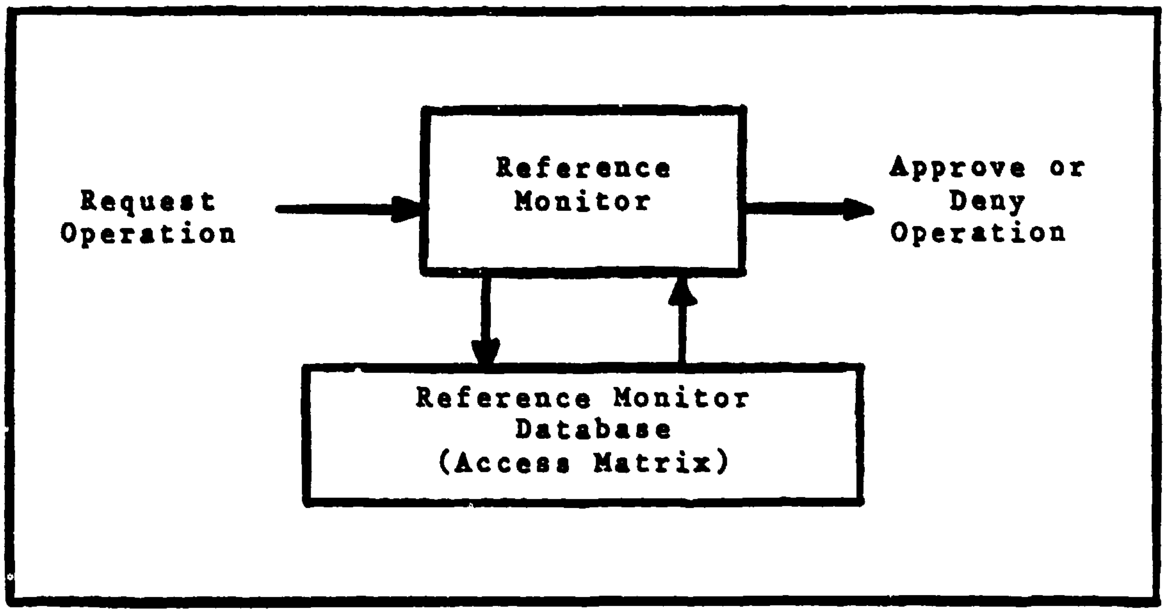
Request Operation
Reference Monitor
Approve or Deny Operation
Reference Monitor Database (Access Matrix)

Figure 3 - Reference Monitor

Security Kernel

A security kernel is actually a hardware/software mechanism that implements a reference monitor (as described above), but the term has also been used to denote all security-relevant system software (AMES83, LAND83). A security kernel may be viewed as the very heart of a shelled operating system (as in the conceptual shelled structure of the UNIX operating system), and is responsible for mediating all references and transactions between subjects and objects to enforce a particular security policy. It is necessary to keep the security kernel as simple as possible to enhance the verification and proof of the kernel's adherence to a security policy.

Actual security kernel implementations usually include one component called the kernel, which enforces a specified set of security rules, and other components called trusted processes. These processes are trusted not to violate security, although they may not be bound to all of the security rules. An example of a trusted process would be a System Security Officer (SSO) performing a process to downgrade or declassify an object or file.

Many projects have sought to demonstrate the practicality of the security kernel approach (AMES83, LAND83, SCHE83). A primary limiting factor on security kernel implementation is the system performance degradation due to the fact that all processes must be mediated through the security kernel.

Military Message Systems

An example of the need to integrate a security model with particular network implementation considerations is given in LAND82, which describes an informal security model for the family of Military Message Systems (MMS). This work at the Naval Research Laboratory (NRL) is investigating the use of application-based security models in the development of military message systems (LAND83). Although the informal model intends to encompass security throughout the MMS family, Landwehr points out that each family member (network node) requires a separate security analysis.

The informal model presented has the same general structure as the Bell-LaPadula security model. However, due to the nature of the data traffic in the MMS family, the Bell-LaPadula concept of an "object" is replaced by an "entity", which is either a "container" or an "object". A container may contain several objects, each of which may have a different security level associated with it. The informal model in LAND82 is comprised of several definitions (clearance, user, container, message, access set, etc.) supplemented by four "security assumptions" and ten "security assertions" (such as "viewing" and "downgrading").

The concept of an "entity" recognizes that in a network the entity may be a host (container) which must be accessed first before you can access an "object". This type of extension to the Bell-LaPadula model by developing a hierarchy of entities may attempt to incorporate the distributed nature of a network into the security model. However, the transformation from such a security model to an actual LAN design may neglect certain other security issues pertinent to LANs, such as communications security and the structure of the network protocols. Since a security model is used to illustrate and verify the security aspects of a computer system or network, this may hinder the verification of the LAN's security properties.

This type of security model considers highly application-specific details to formulate a requirements definition of overall system security. This particular security model illustrates the fact that modeling of security in computer networks needs to include application-specific implementation considerations.

Summary

Security models to date have focussed primarily upon single computer systems as opposed to computer networks. The Bell-LaPadula model provides the basis for modeling security policy, in terms of what relationships and actions may occur among subjects (i.e., users) and objects (i.e., data files) within a computer system. The MMS security model develops the concept that a security model should be derived from a specific application. Although problems in computer network security are closely paralleled by models and mechanisms developed in the course of research of computer systems security, network implementation considerations may introduce some additional complicating factors for ensuring data security. The next chapter will present and discuss some of these important implementation considerations.

IV. SECURE LAN IMPLEMENTATION CONSIDERATIONS

In addition to the more abstract concept of the computer security model, several design and implementation approaches may lend some insight into the actual implementation constraints that security imposes upon a computer network. Several approaches to achieving a multilevel secure local area network are described below, including physical separation of independent LANs (each dedicated to operation at a different, fixed security level), multiplexing security levels in a single LAN, data encryption, and trusted network interface units. A detailed presentation of data encryption and decryption algorithms is beyond the scope of this thesis, but may be found in MEYE82. Rather, an overview of data encryption is presented to illustrate the potential complexity of cryptographic key distribution and management schemes which must be addressed in a LAN implementation.

Security in networks differs in several aspects from security in a centralized computer system. A primary reason is the distributed nature of a LAN (as opposed to the more localized nature of a single computer system) and the complication of establishing and maintaining secure communication channels between LAN subscribers. A second reason is that the network protocols, if not properly designed, can be used by an intruder to gain access to the network data or have it misrouted within the network. In a long-haul type of computer network, the switching nodes and concentrators are distributed physically and may or may not be considered secure.

Physical Security

Physical security refers to the careful control of physical access to or exposure of specific sensitive resources such as classified information. Examples of physical security include safes for storage of classified information, restricted access areas of buildings, and security guards to prevent unauthorized personnel from entering a restricted area. If complete physical security were applied to a computer system or a local area network, all components of the computer system or network would be required to be physically secure. This means that all host processors, data terminals, printers, cables (or other data transmission medium) and all other peripheral equipment must be physically secure. Physical security also includes measures to prevent information from leaving the computer site without proper authorization.

Unfortunately, complete physical security severely constrains an information processing system. For example, complete physical security precludes the connection of such a system to a network where other users are present who may not possess proper authorization to access the classif ed information. Additionally, complete physical security may reduce the chance of compromise, but will not, in a multi-user or multilevel computer network, prevent unauthorized disclosure, modification, addition, or destruction of information, since anyone with access to the network may have access to all the information contained in the network. Therefore, in addition to the traditional concept of physical security and limiting "physical" access to a particular resource, limitation of "electronic" access to a resource must also be taken into account.

Data encryption techniques are an example of limiting the "electronic" access if only authorized personnel possess the decrypting "key" to decipher the information. Encryption will be discussed later in this chapter.

One additional physical security consideration is the prevention of electromagnetic emanation from electronic devices such as computer terminals (also referred to as "Tempest" requirements). With proper equipment, these electromagnetic waves may be received by an enemy and analyzed to reproduce the information from the electromagnetic source. One protective measure is to shield all the electronic components to reduce or eliminate this electromagnetic radiation. This thesis will not go into detail on electromagnetic protective measures, but will assume that appropriate physical security will be provided as specified by the appropriate Department of Defense regulations.

While physical security is still necessary, it must be complemented by certain electronic security measures such as data encryption or "trusted software", each of which will be discussed later in this chapter.

Physically Separate LANs

This approach implements each particular security level as a physically separate local area network, with all data traffic being at the same single security level in each separate LAN. All computers and terminals must be physically protected to the security level of the LAN to which they are connected. This may be a viable approach if only very few distinct security levels need to be processed. For example, certain security partitions (sensitivity level plus compartment set) may be geographically zoned, so separate LANs for each security partition could be a viable solution. However, the duplication of LAN resources may rapidly become cost prohibitive as the number of separate security partitions increases. Another drawback to this approach is the lack of flexibility to the user who needs to frequently access several different levels of classified information.

Multiplexing Security Levels

This approach distinguishes different security levels on a single-network LAN by assigning different channels on a broadband cable (via frequency division multiplexing

(FDM) or time division multiplexing (TDM)) to different security levels. This is a relatively simple approach in terms of off-the-shelf implementability, but constrains the system to a relatively small upper bound on the number of distinct security levels (which may be large when all combinations of compartments are considered). Additionally, this approach requires fixed bandwidth allocation for each security level regardless of relative traffic load and would require complex frequency shifting for fully multilevel operation.

Encryption

When designing a computer network, several sources of data insecurity need to be considered. Prominent among these are spurious message injection, message reception by unauthorized receivers, transmission disruption, and rerouting data to improper nodes. To maintain security against these hazards, a combination of encryption algorithms on the data and appropriate protocols for message exchanges may be employed. These techniques also facilitate the handling of other problems in computer communication networks, such as key distribution, authentication, privacy, digital signatures, network mail, and transaction verification.

Recalling the abstraction of network communications as a layered protocol architecture (as illustrated in Figure 1), data encryption may conceivably be performed in any of the seven protocol layers. Since the network communication media may be easily accessed, there might be a need for encryption on each data link witnin a network, such as encrypting all data at the bottom protocol layers. Alternatively, one can also choose to encrypt data above the network layer, i.e., the host-to-host layer, which constitutes an example of end-to-end encryption. The higher the layer at which encryption is performed, the less the lower layers of the communications subnet (layers 1-3) have to be specially tailored to perform application-specific security tasks. Therefore, the communications subnet layers need not be altered to accomodate secure communuications when encryption is performed at a higher layer. However, data link encryption can mask traffic characteristics, which by itself may be of interest to an unauthorized party. Data traffic characteristics may be readily visible to any potential network intruder if the data packet addressing information is not encrypted. Therefore, a combination of data link and end-to-end encryption techniques may be desirable for a particular network application.

Use of end-to-end encryption (above protocol layer 3) as an approach to secure communications in both wide-area packet-switched networks and in local area networks is currently being researched. This approach requires a key distribution facility (either at each LAN site or possibly at a central facility or network node, called a Key

Distibution Center (KDC)) and encryption/decryption units in each network terminal interface unit. A point-to-point version of end-to-end encryption, known as the "private line interface" (PLI), has been successful in specific applications across wide-area packet-switched networks, and is commonly employed to provide classified communications on the ARPANET (SIDH82b).

There are two basic approaches to encryption. The first requires use of a secret transformation key to encrypt data that is then sent over a public channel. At the receiving station, the same key is used to convert the enciphered data back into the original form (see Figure 4). The transformation key is sent to the authorized receiver over a secure channel and is therefore unavailable to other parties. This method constitutes a private-key cryptosystem (MEYE82).

The second approach is based on the use of separate keys at the transmitting and receiving stations - keys that cannot, in practice, be obtained from each other. Each user keeps one of these two transformations secret and publishes the other, which can then be used to transform data intended for the user. Systems employing this approach are called public-key cryptosystems (DENN83, SMIT83), since the encryption key may be public knowledge but the decryption key is known only to the receiver.

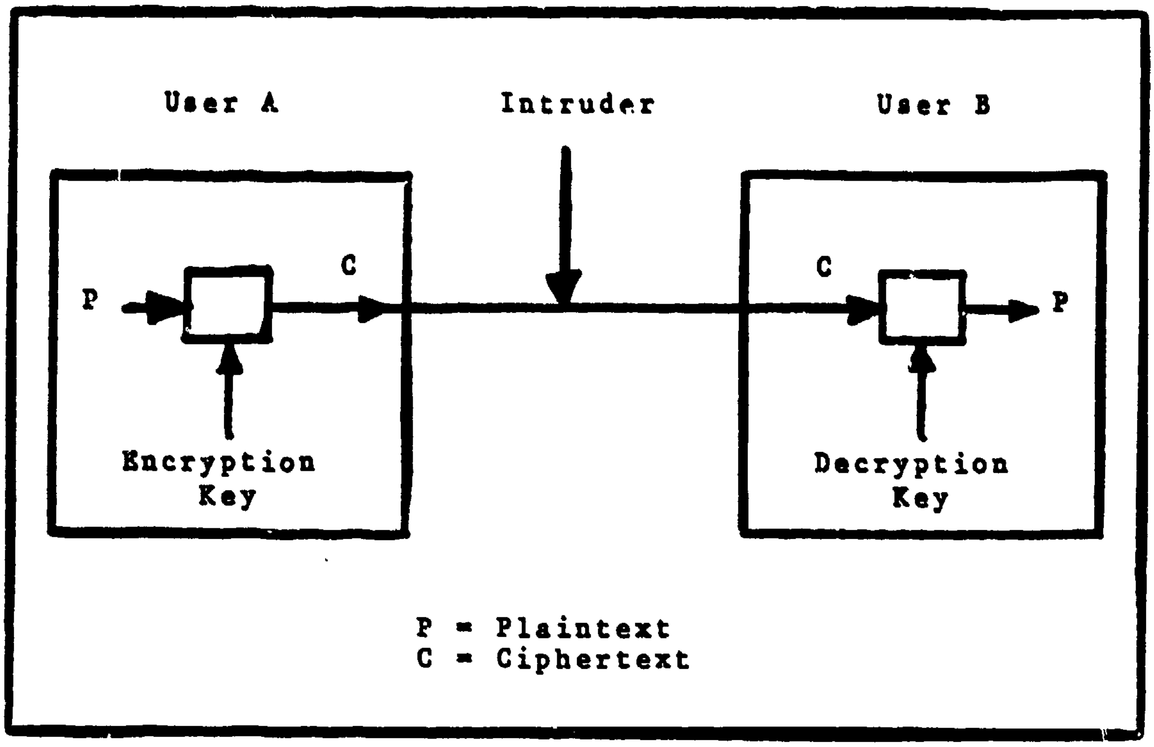

Figure 4 - The Encryption/Decryption Process

Public-key systems have some intrinsic advantages over private-key systems. For example, the public-key method may alleviate problems such as key distribution, secure communication over an insecure channel without exchanging keys, digital signatures, transaction verification, and key exchange. Solving these problems with private-key methods can be cumbersome. To exploit the advantages of public-key systems, more efficient implementation techniques are necessary so that encryption and decryption time can be brought down to acceptable levels. At the same time, better crypto-analysis algorithms may force the use of greater block sizes for a specified level of security (KAK83).

The Data Encryption Standard (DES) of the National Bureau of Standards was adopted for use in the United States in 1977 (MEYE82). This private-key cryptosystem is in use today and has been implemented in hardware as well (COLL79). The major reason for the popularity of the DES is its speed. It takes about 100 milliseconds to implement on an 8-bit microprocessor, and the tima can be brought down to about 5 microseconds on a custom-built LSI (large-scale integration) device (DAVI81). In contrast, with the Rivest-Shamir-Adleman (RSA) algorithm, the most promising public-key system, encryption of 500-bit numbers (a block size necessary for security) using available technology takes about a half second (KAK83). This speed is unacceptable for many applications such as a key-management system, and public-key algorithms are already being used for this purpose.

The size of the encryption or decryption keys varies between different cryptographic codes, but analysis of the relative security of a cryptographic code focusses on the probability of "guessing" or calculating the crypto keys employed. Naturally, the more digits (or bits) in the crypto key, the more difficult it becomes to "crack" the encryption code. As an example, the DES uses an encryption/decryption key size of 64 bits, of which 56 bits are used directly by the cryptographic algorithm and 8 bits are used for error detection. Detailed analysis of the strength of a particular cryptographic code to withstand analytical attack may be found in MEYE82.

Key distribution and management may add significant overhead to a network. An example of a DES encryption/decryption device, the CR-200 Data Security Unit, is discussed in Appendix A. The CR-200 unit is available for research projects at the Electrical Engineering Department of the Air Force Institute of Technology. Also, an example of a centralized key distribution and management scheme is given in STEI82, and indicates the level of handshaking necessary between computer systems in one design for a secure network. Key distribution and management schemes may provide the basis for secure communication channels within a LAN.

Digital Signatures

Senders and receivers of sensitive information may require secure means for validating and authenticating the electronic messages they exchange. Validation refers to certification of the contents of a message, and authentication refers to certification of the message's originator. A proposed method to accomplish both functions is the use of a digital signature, which is appended to (or an integral part of) every message (TANE81, KUO81, AKL83). A digital signature is simply a string of 0's and 1's, and may be different for each message sent (unlike a handwritten "analog" signature), which makes a digital signature extremely difficult to duplicate without some private information (AKL83).

Trusted Network Interface Units

The overall objective of a local area network that is simultaneously servicing users at a variety of different security levels is to provide full multilevel protection of the data. Subscribers (host computers or terminals) to a LAN may be limited to operate at a single level of security, or they may be multilevel and trusted to operate at a range of security levels. One approach to ensuring the full multilevel protection of the data on a LAN is to use a "trusted interface unit" (TIU) to enforce security access restrictions to classified data (SIDH82a). All data packets on the LAN medium are plain text (no encryption is performed), and the trusted network interface unit arbitrates all security-related flow of data from the LAN medium to a user terminal or host.

For single-level LAN subscribers, communication is restricted to those at the same security level. This restriction is enforced by the TIU used by each subscriber to interface to the LAN and is based on a security level field in the header of each data packet. The TIU's (not the individual host computers or terminals) are trusted to verify and enforce the security markings in the packets. Similarly for multilevel subscribers (a multilevel secure host computer or terminal), communication is restricted according to the usual security constraints. Security levels are enforced by the TIU for the multilevel host, with the host trusted to choose the specific security level of each packet it transmits. Likewise, the multilevel host is trusted to receive packets at the range of its security levels and to properly protect the data according to the classification in the packet header. Figure 5 shows a simple multilevel LAN with single-level and multilevel subscribers (SIDH82b). This design considers the potential for multilevel host processors, which as of yet may not be proven to be truly multilevel secure. More accurately, the hosts probably operate in a dedicated or system-high mode.

As discussed earlier, appropriate physical security protection requires that the entire LAN medium and all TIU's be physically secured to "system high", the highest security classification to be processed in the LAN. It may be unreasonably costly to protect all TIU's and the entire LAN medium in a network where most of the users are at lower or unclassified security levels.

To alleviate this problem, the simple multilevel LAN is extended to incorporate the concept of physically separate subnetworks whose LAN mediums are each physically protected to some maximum level that may be less than the maximum level of the entire local area network. The subnetworks are connected by "bridges" in such a way that the entire set of subnetworks appear as a single local area network to each TIU and subscriber.

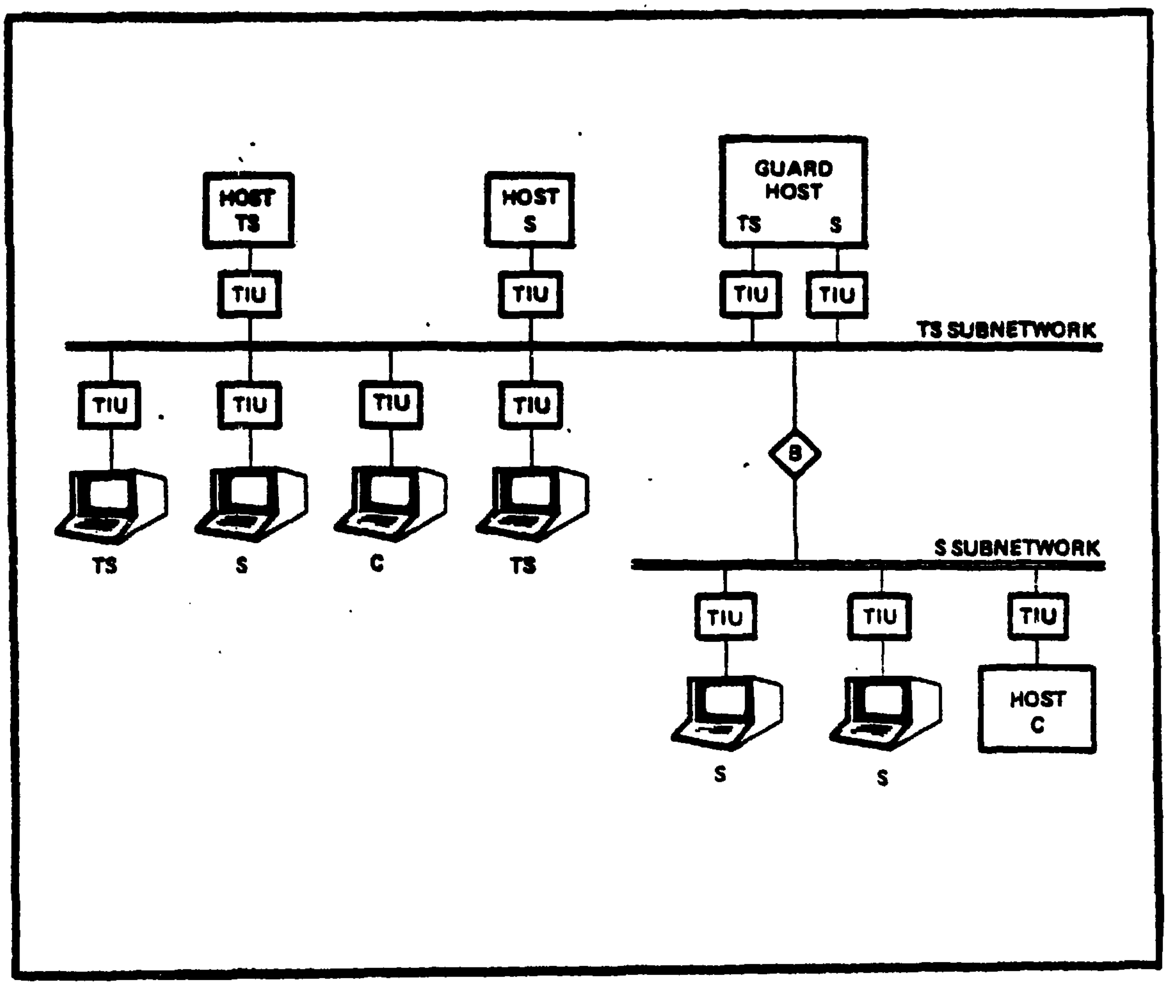

Figure 5 - Simple Multilevel LAN Configuration
(SIDH82b)

An example of a multilevel LAN composed of several subnetworks is shown in Figure 6. Note that data encryption is used only where portions of the LAN medium, TIU-subscriber link, or bridge link must pass through physically unprotected areas. Similar to gateways in wide-area networks, the bridges route packets between LAN subnetworks with identical protocols. They also perform a security check to ensure that information from a high level TIU on one subnetwork does not flow to a lower level subnetwork. Therefore, subnetworks need only be physically protected and trusted to maintain separation of data within the range of levels of subscribers on that subnetwork.

Protocol Modification for Security

As mentioned earlier, the issue of specific network protocols must be addressed in order to incorporate multilevel security. One proposed protocol modification (SIDH82a) is based upon an existing operational protocol, therefore minimizing the modifications to the protocol so as not to seriously affect existing performance studies or implementation techniques. The existing protocol is the "Carrier Sense Multiple Access with Collision Detection" (CSMA/CD) protocol, used by Ethernet, that has been proposed for the IEEE Standard 802.

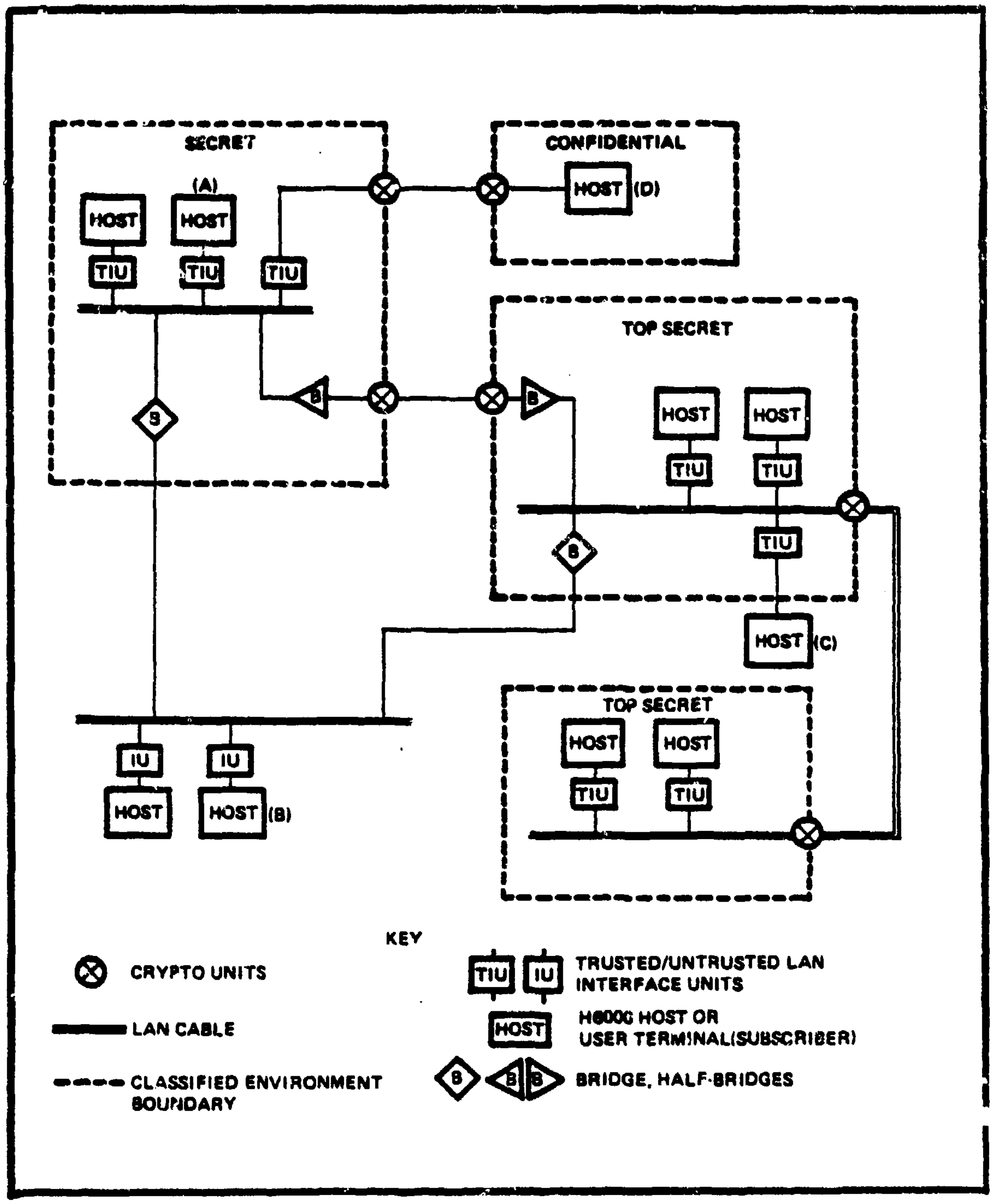

Figure 6 - Multilevel Secure LAN with Subnetworks (SIDH82b)

Figure 7 shows a simplified format of the IEEE 802 CSMA/CD packet along with the modified version for the multilevel secure LAN. Note that the source and destination address fields are subdivided into two components to provide a two-level hierarchical address based on subnetwork number and TIU number. Also, a security level field has been added at the beginning of the data field. The packet and header length are unchanged, and all the CSMA/CD protocol processing logic is unchanged from that in the 802 standard.

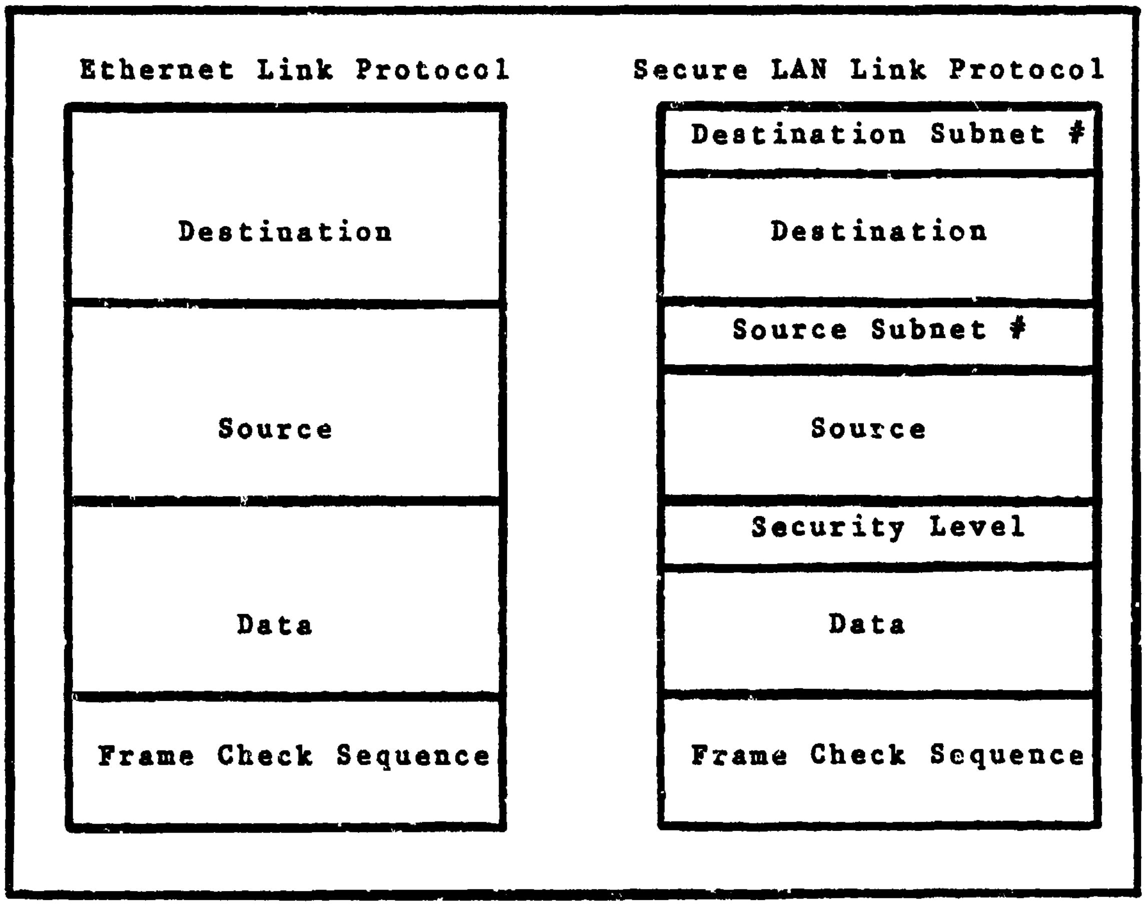

Figure 7 - CSMA/CD Packet Formats (SIDH82a)

A military computer network may use IEEE 802 Standard protocols at the lower protocol layers, but any discussion of protocols should be done in light of Department of Defense standard protocols. The DoD level 4 Standard Transmission Control Protocol (TCP) may be used to maintain the end-to-end integrity of the network (DARP81a). The DoD Standard Internet Protocol (IP) contains both security fields and addressing capabilities for multiple networks (DARP81b). The security implications and provisions of the Internet Protocol are discussed further in Chapter 6.

Trusted Interface Unit

The TIU is responsible for enforcing the security policy based on the security level(s) of its subscriber and the security level of each packet (SIDH82a). The multilevel TIU for a host or terminal will contain fully trusted software. The security processor in such a TIU would only be able to limit communications to the range of levels at which the host or terminal is authorized to operate. The rest of the TIU would have to be trusted to properly identify the security level of the data to the host within that range, so that the host (which is trusted) can make the correct decisions to provide the necessary protection of the multilevel data.

Summary

Enforcing security in a computer network may impose some implementation constraints upon the network. Some implementation approaches (physically separate LANs, multiplexing security levels, trusted network interface units, and data encryption) have intrinsic limitations, but may be well-suited to a specific network application. Data encryption offers some security advantages, but the distribution and management of cryptographic keys could become a cumbersome task in a computer network. The trusted network interface unit approach provides some implementation flexibility and may be adapted to various network applications, but the separation and multilevel protection of the data within a LAN needs to be further addressed.

Each of these MLS LAN approaches involve implementation considerations. In addition to the security policy models described in Chapter 3, a particular LAN application may necessitate unique security-related requirements. Therefore, various LAN implementation considerations need to be integrated with a security policy model to design a "security architecture" for a local area computer network. The next chapter will define a prototype LAN security model upon which a security architecture design may be based.

V. PROTOTYPE LAN SECURITY MODEL

Design and implementation of a secure local area network involves many complex issues, as described in the previous chapters. However, the ultimate objective of system certification to process multilevel classified data relies on the verification of the system's security enforcement policy. As described in Chapter 3, computer security models have served as the fundamental description of how a computer system will address security policy.

The applicability of computer security models to date has focussed primarily upon a single computer system rather than a network of computers. Due to technology trends towards the interconnection of computer systems into computer networks, the resulting impact on information security must be addressed. As illustrated in the previous discussion of the Bell-LaPadula security model in Chapter 3, this model specifies precisely what conditions must be met (in terms of subjects, objects, access modes, and security principles) to assure secure system states. This security model is readily applicable to a single computer system, since the design of a single, centralized security enforcement mechanism (via an access matrix, or reference monitor) is fairly well-specified by the model.

Since the Bell-LaPadula security model applies to single processor hosts and to multiprocessor hosts, how can the Bell-LaPadula model be applied to a LAN? From a global perspective of a LAN as a "virtual machine", the Bell-LaPadula model may be applicable to the security policies which specify which network users (subjects) have access to what network resources (objects). This chapter will present a prototype LAN security model which incorporates the basic structure of the Bell-LaPadula model, yet specifically considers the class of local area computer networks. The prototype model will first be presented and discussed, followed by two examples of how the model would be applied to particular LAN configurations. The incorporation of the LAN security model into a LAN security architecture will then be discussed in Chapter 6.

Model Description

This section provides a textual definition and description of the prototype LAN security model. This model closely parallels the Bell-LaPadula security model (BELL73a, BELL73b, BELL74). The Bell-LaPadula model has already been widely applied in prototype Department of Defense computer systems (LAND83), and is based on formal mathematical proofs. The prototype LAN security model presented in this chapter may therefore be viewed as an extension of the Bell-LaPadula model to incorporate several features of distributed computer networks. One feature that is included is the notion of an "object" being comprised of (potentially many) component "elements" and/or other "objects". Additionally, the LAN security model is based on the underlying assumption of secure communication channels existing within the LAN.

This section will present the prototype LAN security model by explicitly defining its component parts, stating four security assumptions, and then stating eight security assertions which must be demonstrated to hold true for a multilevel secure LAN.

Model Definitions

Entity: An entity is either a subject, an object, or an element.

Subject: A subject is an active user of a computer system or any entity acting on behalf of a user. For example, processes, jobs, and proceduras may all be considered subjects. A subject has a clearance which allows access to objects and elements having classifications which are a subset of the subject´s clearance.

User: A person authorized to use the LAN.

Roles: Certain users may have particular roles to perform, such as downgrading classification levels, distributing objects within the LAN, or releasing objects. To act in a given role, a user must be authorized to perform it. Special roles may be associated with a trusted process or a very limited number of trusted users.

Object: An identifiable resource or data container within a computer system or LAN. Software-created entities such as programs, files, and directories are objects, as well as hardware resources and devices such as memory blocks, disk tracks, tapes, printers, and terminals. An object has a security classification and may contain elements (each with its own classification) and/or other objects.

Element: An element is the smallest unit of information in the system to which a classification is explicitly attached. Therefore, an element contains no other objects or elements, and is not multilevel.

Security Level: In the context of military security modeling, this is the fundamental security attribute of all entities (subjects, objects, and elements) within a computer system or network. The security level (also called security partition) is comprised of a sensitivity level (Unclassified, Confidential, Secret, Top

Secret) and a (possibly null) set of compartments (NATO, NUCLEAR, etc.). Dissemination controls (such as NATO ONLY, NOFORN, or NOCONTRACTOR) may be handled as additional compartment names. The security level is the basis on which all subject-to-object access is determined. A classification represents the security level of an object or element, while a clearance represents the entire set of security levels of a user. A user will operate at a "current security level" which is a subset of the user's clearance.

Current Security Level: The current security level of a subject is that level by which he is currently recognized. A user may possess a clearance to a specific maximum level, but this does not require that he be recognized at this maximum level. Instead, he may choose a lower level (or subset) as his current security level for processing purposes.

Classification: A classification is a designation attached to information entities (objects and elements) that reflects the damage that could be caused by unauthorized disclosure of that information. A classification includes a sensitivity level and compartment set to specify a security level.

Clearance: A clearance represents the degree of trust associated with a subject (user). It is expressed in the same way as classifications are, as a sensitivity level and a compartment set. In a secure LAN, each user will have a clearance, and functions performed by the LAN for that user may check (via an access control matrix) the user's clearance and the classification of objects to be operated on.

Access Modes: "Access" means the ability and the means necessary to store or retreive data, to communicate with (i.e., provide input to or receive output from), or otherwise make use of any resource in a computer system. "Access Control" is a strategy for protecting objects and elements from unauthorized access. Distinct operations are recognized by the protection mechanism as a possible operation on an object. For example, Read, Write, and Append are possible access modes to a file, while Execute is an additional access mode to a program.

Read Access: An access to an object or element permitting only observation with no modification, in accordance with the Simple Security Property (the subject must have a clearance level higher than or equal to the classification level of the object or element).

Append Access: A write operation which does not allow a prior read of the object or element being written, in accordance with the *-Security Property (the subject must be at a current security level lower than or equal to that of the object or element).

Write Access: The union of Read Access and Append Access, when an object or element must be read prior to being written (i.e., modification), in accordance with both the Simple Security Property and the *-Security Property.

Execute Access: An execute access requires that the desired object or element be read by the subject's processing equipment, in accordance with the Simple Security Property.

Delete Access: A delete access is a destructive write process. Since an object or element must normally be viewed (read) prior to deletion (writing), a delete access must behave in accordance with both the Simple Security Property and the *-Security Property (as in the Write Access).

Access Control Matrix: A list or matrix of subjects which are authorized to have a particular access mode(s) to objects or elements within a computer system or network.

Rules of Operation: Functions that may be applied to an entity. Listed below is a core set of operations which need to be incorporated, yet additional operations may be identified for particular LAN applications.

get read: Request read access to an object or element.

get append: Request append access to an object or element.

get execute: Request execute access to an object or element.

get write: Request write access to an object or element.

release: Release accesses currently possessed (read, write, append, execute); the inverse of "get" access.

permit: Permit another subject discretionary access to an object or element.

rescind: Remove or revoke discretionary access privileges (permits) to an object or element.

create: Create a new entity within the LAN.

delete: Remove an existing object or element from the system.

change security level: Allows a subject (user) to alter its current security level.

Simple Security Property: A fundamental security model rule allowing a subject read-access to an object or element only if the security classification of the object or element is the same or less than the current security level of the subject.

*-Security Property: A fundamental security model rule allowing a subject write-access to an object or element only if the security classification of the object or element is the same or higher than the current security level of the subject.

Non-Discretionary Access Controls: Also called mandatory access controls, the aspect of DoD security policy which restricts access on the basis of security levels. To access an item of information, a user must have a clearance level greater than or equal to the classification of the information. Non-Discretionary access controls are embodied in the Simple Security Property of a security model.

Discretionary Access Controls: Access controls to an object or element (in addition to non-discretionary access controls). These are mechanisms that allow each subject, at its own discretion, to decide which of its own access rights are to be given to any other subject on a need-to-know basis for a particular object or element.

Security Assumptions

1. A System Security Officer (SSO) exists and is trusted to properly assign user clearances, roles, and device (objects) classifications. The SSO may have responsibility for the entire LAN, or each LAN host node may have its own SSO.

2. Normal users are expected to properly handle all classified information, using standard DoD procedures. Users are also expected to properly classify all information which they handle, according to DoD security directives.

3. Appropriate network communication protocols exist to ensure secure information transmission within the network. These secure communication channels protect classified data from unauthorized dissemination while providing distinct separation of security levels.

4. Physical security measures to protect particular LAN components (i.e., hosts and terminals) according to DoD regulations are assumed.

Security Assertions

The following assertions are to be demonstrated to hold true for a multilevel secure LAN:

1. Access Control: A user may invoke an operation on an object or element only if there is a corresponding entry in the access control matrix which allows the subject to perform the requested operation on the specified object or element.

2. Clearance Assignment: Only the System Security Officer (SSO) can set the security clearance recorded in the access control matrix for any user.

3. Entity Labeling Requirement: Any entity within the LAN must be labeled with its correct security classification.

4. Classification Hierarchy: The classification of an object is always at least as high as the maximum classification of the objects and/or elements it contains.

5. Classification Preservation: Information removed from or copied from an object or element inherits the classification of that object or element. Similarly, information inserted into an object or element must not be classified at a level above that object or element.

6. Classification Downgrading: No entity classification label can be downgraded except by a user with the role of downgrader.

7. Simple Security Property: A fundamental security model rule allowing a subject read-access to an object or element only if the security classification of the object or element is the same or less than the security clearance of the subject.

8. *-Security Property: A fundamental security model rule allowing a subject write-access to an object or element only if the security classification of the object or element is the same or higher than the security clearance of the subject.

Discussion of the Model

The entities for the model represent the active subjects (users) and passive objects (and elements) within the LAN. Users are "created" by the System Security Officer assigning some form of unique identifier (such as a login name, password, and/or user identification code) to the user. For each type of entity that users may create, an operation or process may be invoked by the user to "create" the new entity, providing the user is authorized to invoke the particular "create" operation requested.

Each user has a security clearance which the SSO will incorporate into the access control matrix. A finer constraint on the user during actual LAN sessions is imposed by the notion of a "current security level". Although a user may possess a very high security clearance, each LAN operation will be associated with a single security partition or subset of the user's maximum clearance. This aids the enforcement of the *-Security Property.

The incorporation of multilevel objects is an extension of the Bell-LaPadula security model's single-level objects, and is similar to the definition of multilevel objects proposed for Military Message Systems (LAND82), as discussed earlier in Chapter 3. For example, a multilevel object may be a large document classified as Top Secret. The document is comprised of individual chapters, sections, and paragraphs, each of which could be labeled with a specific security classification. If each paragraph were labeled with its security classification and treated as an element, the entire Top Secret document (object) would be a collection of many elements at various classification levels. The model requires, however, that the security classification of an object be at least as high as that of the most highly classified element (or object) contained within it. As a further example, the abstract (element) of a technical paper (object) could be unclassified while the remainder of the paper is classified Secret.

A user may refer to another entity within the system by either direct (explicit) reference or indirect (implicit) reference. Entities may have identifiers that allow them to be named directly, such as a command to read a particular data file name (identifier). Alternately, a process acting on behalf of a user may refer to an entity, constituting an indirect reference. From the user's perspective, anything the user can create, display, or modify must be (or be part of) an entity. Assertion 5 stipulates that a part of an object that is removed or modified inherits the classification of the whole object.

When a user invokes an operation on an entity, the user's current security level, user role (such as "downgrader", if appropriate), the appropriate device and entity classifications, and the access control matrix determine whether he can invoke the operation. The implementation of the access control matrix may be centralized at a single "security node" in the LAN, or each host may perform its own access control. The particular implementation should remain transparent to the model.

It is important to pay particular attention to the third security assumption, which assumes secure communication channels exist within the LAN. Although the implementation of these secure communication channels is transparent to this security model, these secure channels are crucial and fundamental to this or any other network security model. This particular design issue will be further discussed in Chapter 6.

Operations are defined in the model which correspond to the user's view of the LAN. Additional model operations may need to be defined for a particular LAN application, and this model is flexible in that respect, as long as the operations are included in the access control matrix. From the user's perspective, the LAN offers functions and services that may be invoked by typing single function keys or strings of characters. In the actual LAN implementation, processes are constrained to invoke only operations that preserve the truth of the model's assertions.

Model Application Scenarios

In order to demonstrate how the prototype LAN security model may be applied to actual local area computer networks, two distinct LAN configurations will be discussed. The first configuration assumes a single security enforcement node within the LAN which is wholly responsible for enforcing the model. The second configuration illustrates the distribution of the security enforcement responsibility to each LAN node.

Single Security Node

Consider first the hypothetical LAN with one of its nodes dedicated to serving as a "security node". The security node arbitrates all subject/object accesses within the entire LAN, so the network topology essentially becomes a "star" topology, as illustrated in Figure 8. This LAN is similar to a single computer system from a security perspective, since there is a single focal point for all security transactions. The security node may be thought of as a "reference monitor" for the LAN, and may contain a security kernel to implement the reference monitor. The security node must also contain a master library and an access control matrix for all LAN system entities (users, files, and devices).

The SSO is responsible for the operation of the security node and for maintaining the access control matrix. All network users, their respective security clearances, and their access rights to the various LAN entities will be recorded in the access control matrix by the SSO. For example, if user "A1" is authorized access only to information contained on host "A", then the security node (via its access control matrix) will ensure that user A1 will not be able to access any entities resident on any host except host "A".

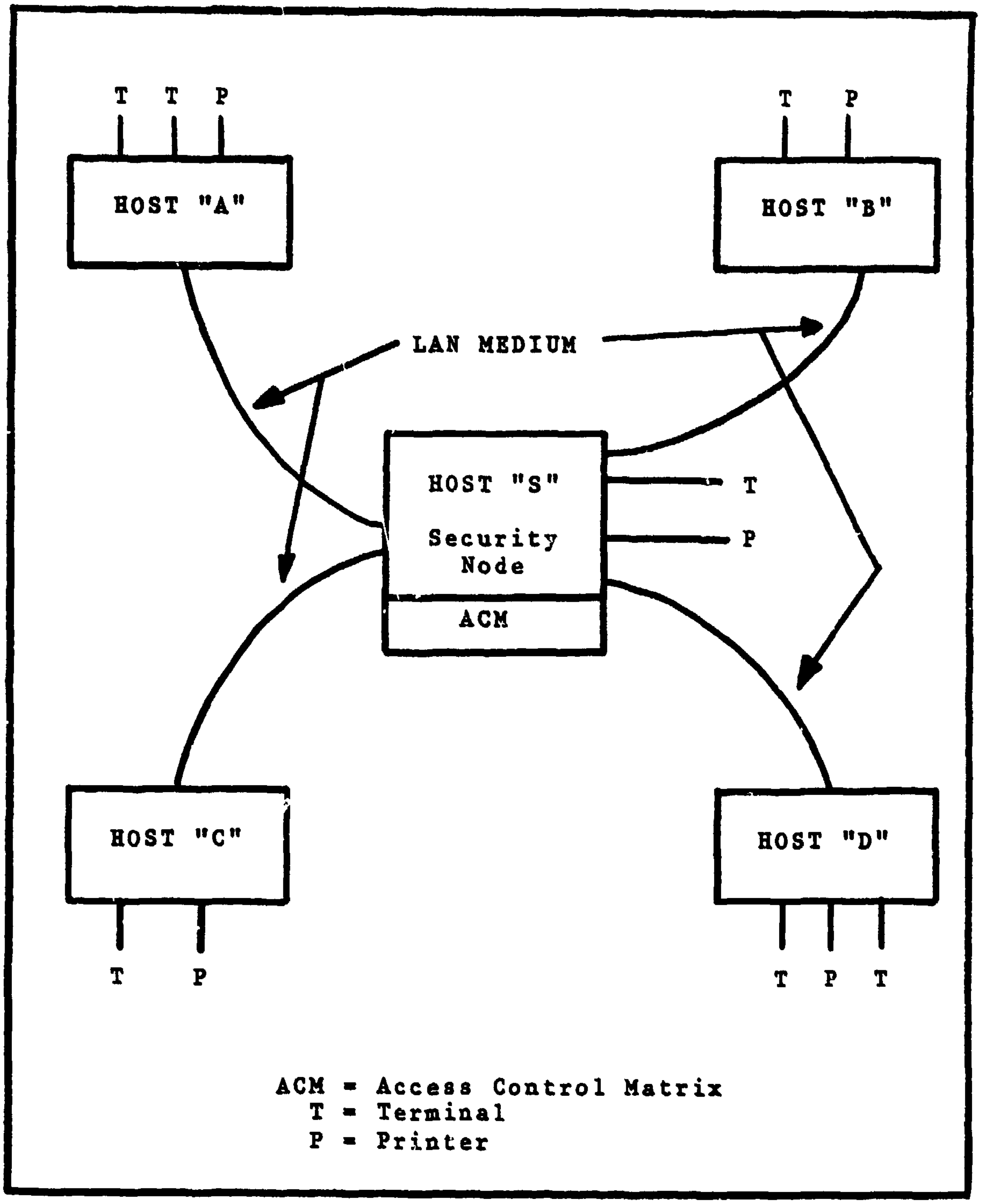

Figure 8 - Secure LAN with Single Security Node

By defining the multilevel object entity within the model, a hierarchy of object entities may be created (similar to the tree structure of files and directories in the UNIX operating system (RUSH83)). For example, the network in Figure 8 could be modeled as four primary multilevel objects corresponding to the four host computers. Each of these primary objects would contain other objects, such as data files and devices. The hierarchical structure may therefore be decomposed down to its individual, single security level elements. Note that this hierarchy may also account for the security processing mode (Controlled, System High, Dedicated, or Multilevel) of each host.

This LAN configuration has the advantage of centralizing the accountability for security-related transactions described in the LAN security model. Some applications may necessitate such a single security control point for accountability purposes, such as the generation of audit trails to keep a log of all security transactions within the system. One potential disadvantage to this configuration is the added "overhead" since each network transmission must be routed first through the security node for processing and access control enforcement. This added overhead may degrade the throughput of the network and adversely affect other performance parameters such as response time. Another potential disadvantage is that the access control matrix must be cognizant of all entities within the entire network, including master libraries of all objects and elements. In a large, complex LAN with many hosts, the access control matrix could be quite large and difficult to manage.

Multiple Security Nodes

As an alternate example, consider the LAN illustrated in Figure 9. Instead of a single security node, each host subscriber to the LAN performs its own security arbitration and access controls. In this case, the LAN security model could be applied to each individual host within the LAN.

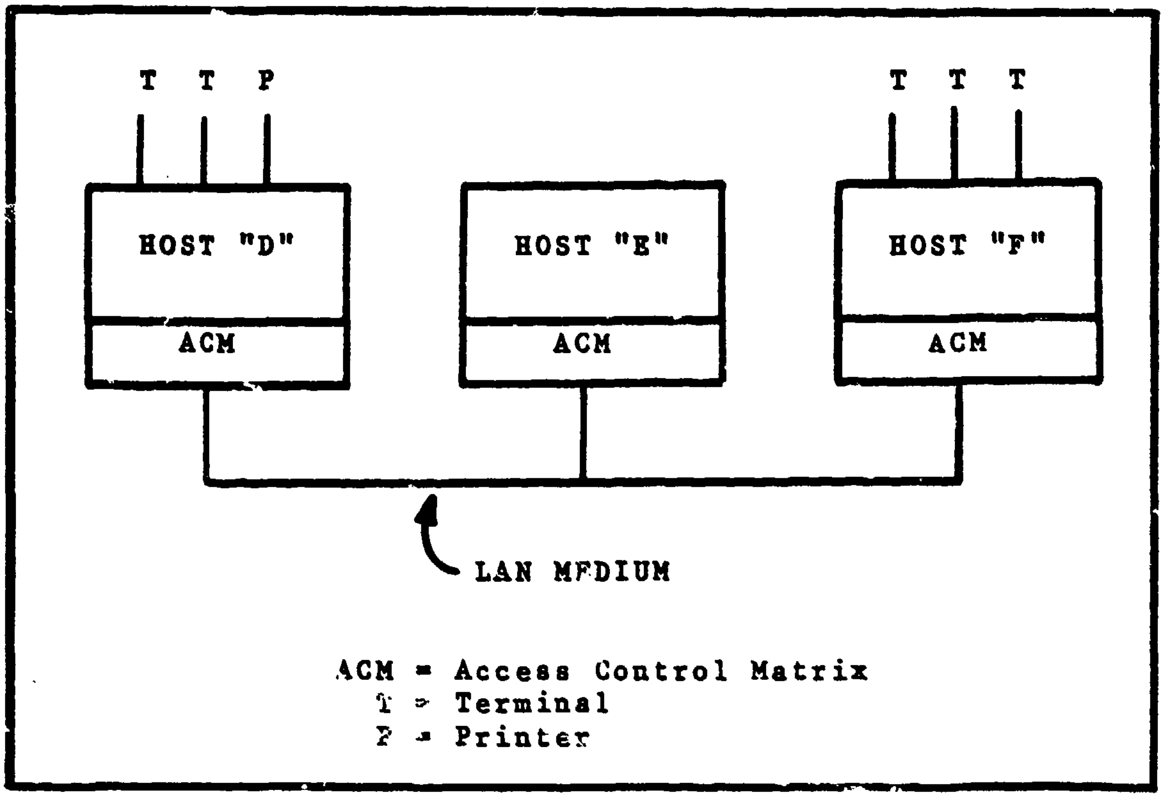

Figure 9 - Secure LAN with Multiple Security Nodes

The hierarchy of entities may be created, as discussed in the single security node example. However, now each LAN node is responsible for access control arbitration of all entities it contains. Each host may have its own SSO to assign user clearances and maintain the access control matrix. Since each node requires its own access control matrix and SSO, the LAN security model may be applied to each node in the LAN. For example, if user "D1" resident on host "D" requests to read a data file named E-FILE on host "E", the access control matrix in host "D" may first check to see if user "D1" is authorized access to host "E" (an object). Note that host D's access control matrix requires no knowledge of the data file "E-FILE", or any of the objects contained within any other host. Once user "D1's" request arrives at host E, host E's access control matrix will determine whether user D1 is authorized to read the data file "E-FILE".

A primary advantage of this LAN configuration is the capability of each LAN subscriber to control its own resources. This may be particularly appropriate when only minimal and infrequent transactions occur between LAN hosts, yet the capability to communicate is still required. A potential disadvantage of this configuration is the large number of separate access control matrices and SSO's (although perhaps a single SSO could service all LAN hosts). Finally, the LAN designer must be aware that individual analysis and security modeling of each LAN node may be naive to the aggregate security structure of the entire LAN.

Summary

Computer security models have served as the fundamental description of how a computer system enforces security policy. This chapter has presented a prototype LAN security model which specifies what must be achieved to ensure the multilevel secure protection and separation of classified data in a LAN. The model closely parallels the Bell-LaPadula security model, which has been applied to a variety of DoD computer systems. The LAN security model presented incorporates the concept of multilevel objects and relies on the assumption of secure communication channels within the LAN. The next chapter will address the relationship between the LAN security model and certain other design issues associated with developing a "security architecture" for a LAN.

VI. SECURE LAN COMMUNICATION CHANNELS

Most security models to date have narrowly focussed upon two fundamental concepts. First, they have concentrated solely upon a single, stand-alone computer system in which a single, centralized operating system is assumed to encompass a security kernel (or other similar mechanism) to enforce a particular security policy. Secondly, these models strictly address security policy, regardless of implementation considerations.

The term "model" implies that a security model should be generic enough to apply to a variety of applications, which may not be feasible to accomplish for the entire class of potential LAN configurations. While the basic security policy concepts intrinsic to the model still apply to the LAN, particular LAN components and features (such as bridges, gateways, secure communication channels, and network protocols) do not fit neatly into the model. This necessitates the integration of the LAN security model with some of the application details of a LAN configuration to properly describe the security-relevant behavior of a LAN, resulting in a security architecture.

The implications of applying the prototype LAN security model presented in Chapter 5 to a LAN (or even a generalized computer network) leaves some security design issues unaddressed. These topics involve the consideration of various implementation constraints introduced in computer networks. In addition to the previously discussed "conventional" physical, electromagnetic emanation, and personnel security controls, the complex topic of computer network security involves communication security, network protocols, and user authentication techniques. For example, the prototype LAN security model explicitly assumes the existence of secure communication channels within the LAN.

User authentication refers to the problem of positively identifying the user(s) of a communications media, especially when the two ends of a communications channel are remote from each other. Research on user authentication techniques and schemes involves communications security, data encryption, digital signatures, and protocol specification techniques. Although user authentication is a necessary component of a secure system, it is an implementation detail that will be will be assumed for the purposes of this thesis.

The design issues concerning communications security and network protocols will be discussed in this chapter, since the prototype LAN security model presented in Chapter 5 depends upon the establishment of secure communication channels within the LAN.

Communications Security

Even if a network is comprised solely of proven, secure computer systems, the security mechanisms in the network must account for the possibility that individual components of the network could be subverted, thus violating some of the premises upon which a secure system proof may be based. In the case of a packet-switched or packet broadcast network, the actual communication media may be quite vulnerable to wiretapping or other subversion, especially in the case of a long-haul computer network utilizing satellite channels. Landwehr notes that most formal security models do not address threats such as wiretapping (LAND81).

Communication security must be a prime consideration in a multilevel LAN because 1) data of many different classification levels may appear on the communication media, and 2) even if the LAN media is physically secure, the LAN quite likely will interface with another network (through a gateway node) which may or may not contain a physically secure communications media. Both "user ends" of a network connection are assumed to terminate in secure areas, but the remainder of the connection may be subject to physical attack such as active or passive wiretapping.

The best available technology for providing communications security appears to be data encryption (TANE81, KUO81, MEYE82). Data encryption may be at the end-to-end level, at the data link level, or potentially at any protocol layer (or combinations of layers) in the ISO reference model discussed in Chapter 1. Some form of end-to-end encryption appears desirable because, depending on the key management scheme, user authentication may be enhanced and additional separation of "logical channels" within the network may be obtained.

If data encryption is performed at a high protocol layer (above layer 4), it is then "transparent" to the lower protocol layers. The lower protocol layers are responsible only for routing the data traffic between the source and destination network nodes, so data encryption performed at a higher layer doesn´t adversely impact the lower protocol layers. However, the packet addressing information that is appended by the lower protocol layers is plainly visible to an intruder, and may provide useful information in the form of traffic analysis.

Alternatively, if the packets are encrypted at a low protocol layer, then even the addressing information is encrypted on the LAN medium, hampering a potential intruder´s traffic analysis capability. In a broadcast LAN, however, each node must then decipher all data packets to determine the addressing information, which may constrain the throughput of the network.

Therefore, depending on the particular LAN evironment and threat assessment, a combination of high-level and low-level encryption may be appropriate. Note that the encryption algorithm itself may impose performance limitations on the LAN. If a particular encryption algorithm depends on past data values to decipher current data values, a single lost data packet may necessitate the retransmission of the entire message.

Network Protocols

The specification of the various network protocol layers (described in Chapter 1) affects the security behavior of a LAN. Computer communication protocols are very important components of computer networks. They are a set of rules which govern the interaction among network components and an orderly transfer of data among them. The correct specification and operation of the protocols is essential for the successful operation of a computer network communication system (SUNS79, SIDH82c).

One example was given in Chapter 4 of a simple modification of the lower two protocol layers of a CSMA/CD data packet by adding a packet header to indicate the security level of the data contained in the packet. Similarly, the Department of Defense Standard Internet Protocol (IP) header incorporates a security field (DARP81b). The DoD Standard Transport Control Protocol (TCP) makes use of the IP type of service field and security option to provide precedence and security on a per connection (session) basis to TCP users (DARP81a). Not all TCP modules will necessarily function in a multilevel secure environment; some may be limited to unclassified use only, and others may operate at only one security level and compartment. Consequently, some TCP implementations and services to users may be limited to a subset of the multilevel secure case.

TCP modules which operate in a multilevel secure environment must properly mark outgoing segments with the security, compartment, and precedence. Such TCP modules must also provide to their users or higher level protocols (such as Telnet or THP) and interface to allow them to specify the desired security level, compartment, and precedence of connections.

The IP packet header format's security option field provides a way for hosts to send security, compartmentation, handling restrictions, and transmission control code (TCC, for closed user groups) parameters. The security field (S Field) of the header specifies one of sixteen security levels (i.e., Unclassified, Confidential, Secret, Top Secret), eight of which are reserved for future use. The compartment field (C Field) contains all zeros if the information transmitted is not compartmented. Other values for the compartment field may be obtained from the Defense Intelligence Agency (DIA). The handling restrictions field (H Field) may contain alphanumeric digraphs to represent the values for the control and release markings defined in the Defense Intelligence Agency Manual DIAM 65-19, "Standard Security Markings". Finally, the transmission control code field (TCC Field) provides a means to segregate traffic and define controlled communities of interest among network subscribers.

Network protocols such as TCP-IP may enhance the security aspects of a LAN, but all the protocol header information may be rendered useless if the actual data within a packet is transmitted as plain text. Therefore, a combination of data encryption and network protocols with security features may be a feasible approach to protecting sensitive data via secure communication channels.

Summary

Due to the distributed nature of local area computer networks and the lack of a network operating system, no centralized focal point may exist in a LAN to serve as a security enforcement mechanism. The complex topic of computer network security involves communcations security, data encryption techniques, network protocols, and key distribution schemes. These security aspects, which may differ from LAN to LAN depending on configuration and application, need to be integrated with a security policy model such as the prototype LAN security model to form a security architecture.

VII. CONCLUSIONS AND RECOMMENDATIONS

Processing of various levels of classified information in a local area network of computers requires strict attention to both physical and electronic security protection measures to prevent unauthorized access to sensitive information. Due to their distributed nature, LAN's involve several security issues that are distinct from issues concerning just multilevel secure computer systems. In particular, the establishment of secure communication channels between LAN subscribers and the associated separation and protection of data classified at different security levels must be addressed. Some combination of the techniques presented in this paper (data encryption, physical security, and trusted software) must be integrated with a security policy model (such as the prototype LAN security model) into a cohesive design of a "security architecture" that will provide full multilevel protection of the LAN resources.

Conclusions

Past computer security models have focussed upon modeling security in a single computer system (BELL73a, BELL73b, BELL74, LAND81). The state of the art in data communications technology is aimed towards complex networks of computer systems, interconnected by a variety of media and accessible to a variety of users. Modeling security in LANs is not as straightforward as in single computer systems. Since different LAN applications may contain a completely different structure of security enforcement mechanisms, a single "LAN security model" may not be an appropriate (or even useful) entity if used for all LANs. Therefore, computer security models developed for single computer systems need to be expanded to incorporate the distributed nature of present and future computer networks, both local area networks and long-haul networks.

This thesis has presented both a prototype LAN security model and a discussion of application-specific secure LAN design issues. These LAN implementation considerations must be integrated with a security policy model to produce a "security architecture". There are two primary implications for modeling security in local area computer networks:

1) Due to the distributed nature of the network itself, certain aspects of a security model may similarly be distributed to accurately model the various security enforcement mechanisms in a computer network.

2) Modeling of security in computer networks may involve or depend upon implementation considerations, such as:

   a) How and where data encryption and decryption are to be performed, and the consequenses of the associated cryptographic key distribution and management system

b) Physical topology of the network and its associated interface mechanisms

c) User identification/authentication and data access authorization schemes

d) Formal specification of network protocols to establish secure communication channels

The necessity of a comprehensive security architecture for a particular LAN increases as the complexity of the secure systems escalate. As computer technology transitions from single, stand-alone computer systems to complex networks of many computers and peripherals, the rigorous enforcement of security policies demands the existence of and adherence to a model of security policy as well as application-specific security considerations in a local area computer network.

Recommendations for Further Study

Many of the issues raised and implementation considerations discussed in this thesis are still quite theoretical in nature, and great potential exists for further study. Categories that require further research include user identification and user authentication schemes, the analysis of mandatory versus discretionary access controls, and the generation of audit trails within a LAN. In particular, the following would prove to be excellent and relevant research topics that need to be addressed in the field of computer network security:

1. The distribution and management of encryption and decryption keys will certainly add "overhead" to any computer network's information processing capability. An analysis of the extent of this overhead associated strictly with security enforcement is necessary to quantify the security-specific throughput constraints imposed on a computer network.

2. Development of a LAN security architecture, tailored to a specific LAN application, including both a security policy model such as the prototype LAN security model and implementation constraints.

3. The CR-200 Data Encryption Unit, described in Appendix A, could form the nucleus of a prototype "Trusted Interface Unit", perhaps implementable on the AFIT Digital Engineering Laboratory's LSI-11 computer network.

4. The mathematical formalization of the prototype LAN security model, perhaps tailored to a specific LAN application.

Summary

Security has been an overlooked issue in the design, analysis, and implementation of many computer systems and networks, particularlv in the private corporate sector. In fact, the U.S. Department of Commerce's NBS Special Publication 500-96, "The Selection of Local Area Networks" (ROSE82) devotes only a single paragraph to security and privacy, only to mention that "Security considerations include security, access authorization, and encryption." The Department of Defense and the intelligence communities have been the driving force behind provably secure computer systems and networks, because national security is a primary objective.

Security and privacy issues need to be addressed at the very earliest point in the definition of user requirements in the baselining of all future computer systems and networks. Otherwise, the growing computer literacy in our highly technological society may exploit the drastic weaknesses in the privacy and security of computer systems and networks.

BIBLIOGRAPHY

AKL83 Akl, Selim G. "Digital Signatures: A Tutorial Survey," Computer, Vol 16, No 2; pp 15 - 24; February 1983.

ALLA82 Allan, Roger. "Designer's Reference: Computer Standards." Electronic Design, Vol 30, No 26; 23 December 1982; pp 107-112.

AMES83 Ames, Stanley R. et al. "Security Kernel Design and Implementation: An Introduction," Computer, Vol 16, No 7; pp 14-22; July 1983.

AXNE83 Axner, David H. "Protocol Converters are Compatible Bridges to Future", Telecommunications Products and Technology, Vol 1, No 4, pp 1 & 25-28; October 1983.

BELL73a Bell, Elliott D. and Leonard J. LaPadula. Secure Computer Systems: Mathematical Foundations. ESD-TR-73-278, Vol I; MTR-2547, Vol I; (AD 770 768) November 1973.

BELL73b Bell, Elliott D. and Leonard J. Lapadula. Secure Computer Systems: A Mathematical Model. ESD-TR-73-278, Vol II; MTR-2547, Vol II; (AD 771 543) November 1973.

BELL74 Bell, Elliott D. and Leonard J. Lapadula. Secure Computer Systems: A Refinement of the Mathematical Model. ESD-TR-73-278, Vol III; MTR-2547, Vol III; (AD 780 528) April 1974.

BELL75 Bell, Elliott D. and E. L. Burke. A Software Validation Technique for Certification: The Methodology. ESD-TR-75-54; MTR-2932, Vol 1; (AD A 009 849) April 1975.

BIBA77 Biba, K. J. Integrity Considerations for Secure Computer Systems. ESD-TR-76-372; MTR-3153, Rev 1; (AD A039 324); April 1977.

BOCH79 Bochmann, Gregor V. and Tankoano Joachim. "Development and Structure of an X.25 Implementation". IEEE Transactions on Software Engineering, Vol. SE-5, No 5, pp 429-439; September 1979.

CHEH81 Cheheyl, Maureen H. et al. "Verifying Security," ACM Computing Surveys, Vol 13, No 3; pp 279-340 September 1981.

COLL79 "User's Guide to the Collins CR-200/220 Data Security Unit"; Collins Telecommunications Products Division, Rockwell International, Cedar Rapids, Iowa; October 1979.

COMP83 "Computer Break-in Charged". Associated Press (Los Angeles); The Journal-Herald (Newspaper); Dayton, Ohio; 3 November 1983; p 22.

DARP81a DoD Standard Transmission Control Protocol, Defense Advanced Research Projects Agency (DARPA) (Prepared by the Information Sciences Institute, University of Southern California); Arlington, VA September 1981.

DARP81b DoD Standard Internet Protocol, Defense Advanced Research Projects Agency (DARPA) (Prepared by the Information Sciences Institute, University of Southern California); Arlington, VA; September 1981.

DAVI81 Davies, Donald W. Tutorial: The Security of Data in Networks. IEEE Computer Society Press; Los Angeles; 1981.

DAVI83 Davies, Donald W. "Applying the RSA Digital Signature to Electronic Mail," Computer, Vol 16, No 2; pp 55-62; February 1983.

DEMI83 DeMillo, Richard and Michael Merritt. "Protocols for Data Security," Computer, Vol 16, No 2; pp 39-50; February 1983.

DENN83 Denning, Dorothy E. "Protecting Public Keys and Signature Keys," Computer, Vol 16, No 2; pp 27-35 February 1983.

DOD78 DoD Directive 5200.28 of 18 December 1972, First Amendment, Change 2, 29 April 1978.

FRAI83 Fraim, Lester J. "Scomp: A Solution to the Multilevel Security Problem," Computer, Vol 16, No 7; pp 26-34; July 1983.

FURT78 Furtek, Frederick C. A Validation Technique for Computer Security Based on the Theory of Constraints. ESD-TR-78-182; MTR-3661 (AD A065 111); December 1978.

GOOD82 Good, Donald I. "The Proof of a Distributed System in Gypsy"; Institute for Computing Science, University of Texas at Austin; Technical Report No 30; September 1982.

ISO82 "Information Processing Systems - Open Systems Interconnection - Basic Reference Model"; International Organization for Standardization, Draft International Standard ISO/DIS 7498; April 1982.

KAK83 Kak, Subhash C. "Data Security in Computer Networks," Computer, Vol 16, No 2; pp 8-10; February 1983.

KENT76 Kent, Stephen T. Encryption-Based Protection Protocols for Interactive User-Computer Communication; MIT Master's Thesis; (AD A026 911); May 1976.

KENT80 Kent, Stephen T. Protecting Externally Supplied Software in Small Computers. MIT Doctoral Dissertation; MIT/LCS/TR-255; (AD A104 678); May 1981.

KLEI76 Kleinrock, Leonard. Queueing Systems. John Wiley and Sons, New York; 1976.

KUO81 Kuo, Franklin F. (Editor). Protocols and Techniques for Data Communication Networks. Prentice-Hall; Englewood Cliffs, NJ; 1981.

LAND81 Landwehr, Carl E. "Formal Models for Computer Security," ACM Computing Surveys, Vol 13, No 3; pp 247-278; September 1981.

LAND82 Landwehr, Carl E. and C. L. Heitmeyer. Military Message Systems: Requirements and Security Model. NRL Memorandum Report 4925; September, 1982.

LAND83 Landwehr, Carl E. "The Best Available Technologies for Computer Security," Computer, Vol 16, No 7; pp 86-100; July 1983.

MEYE82 Meyer, Carl H. and Stephen M. Matyas. Cryptography: A New Dimension in Computer Data Security John Wiley and Sons; New York; 1982.

POPE73 Popek, Gerald J. Access Control Models; ESD-TR-73-106; (AD 761 807); February 1973.

REED82 Reed, William P. The Analysis and Design of a Computer Security/Recovery System for a Relational Database Management System; Master's Thesis; Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio; December 1982.

RAUC83 Rauch-Hindin, Wendy B. "Special Series on System Integration: Upper-Level Network Protocols"; Electronic Design, Vol 31, No 5; 3 March 1983; pp 180-194.

RIVE78 Rivest, R.L., A. Shamir and L. Adleman. "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communications of the ACM, Vol 21 No 2, p 120; February 1978.

ROSE82 Rosenthal, Robert (Editor). The Selection of Local Area Computer Networks. National Bureau of Standards (NBS) Special Publication 500-96; Washington, D.C.; November 1982.

RUSH83 Rushby, John and Brian Randell. "A Distributed Secure System," Computer, Vol 16, No 7; pp 55-67 July 1983.

SAUE81 Sauer, Charles H. and K. Mani Chandi. Computer Systems Performance Modeling. Prentice-Hall, Englewood Cliffs, New Jersey; 1981.

SCHA83 Schanning, Brian. "Securing Data Inexpensively Via Public Keys"; Computer Design, Vol 22, No 4; 5 April 1983; pp 105-108.

SCHE83 Schell, Roger R. "A Security Kernel for a Multiprocessor Microcomputer," Computer, Vol 16, No 7; pp 47-53; July 1983.

SIDH82a Sidhu, Deepinder P., and Morrie Gasser. "A Multilevel Secure Local Area Network"; Proceedings of the 1982 Symposium on Security and Privacy; IEEE Computer Society; April, 1982.

SIDH82b Sidhu, Deepinder P., and Morrie Gasser. "Design for a Multilevel Secure Local Area Network"; MITRE Report Number MTR8702; MITRE Corporation; Bedford, MA; March, 1982.

SIDH82c Sidhu, Deepinder P. "Protocol Design Rules"; Protocol Specification, Testing, and Verification (Proceedings of the 2nd International Workshop on Protocol Specification, Testing, and Verification) North-Holland Publishing Company, 1982; pp 283 - 300.

SMIT83 Smith, John. "Public Key Cryptography," Byte, Vol 8, No 1, pp 198-218; January 1983.

STEI82 Steinmetz, Jay S. "A Secure Computer Network"; Master's Thesis; Air Force Institute of Technology, Wright-Patterson Air Force Base, OH; November 1982.

SUNS79 Sunshine, Carl A. Formal Methods for Communication Protocol Specification and Verification. N-1429-ARPA/NBS; (AD A083 263); November 1979.

TANE81 Tanenbaum, Andrew S. Computer Networks; Prentice-Hall; Englewood Cliffs, NJ; 1981.

VOYD81 Voydock, Victor L. and Stephen T. Kent. "Security in Higher Level Protocols: Alternatives and Recommendations"; National Bureau of Standards Report Number ICST/HLNP-81-19; September, 1981.

WALT74 Walter, K. G., et. al. Primitive Models for Computer Security; ESD-TR-74-117; (AD 778 467); January 1974.

WALT75 Walter, K. G., et. al. Initial Structured Specifications for an Uncompromisable Computer Security System; ESD-TR-75-82; (AD A022 490); July 1975.

WORM82 Wormington, T. D. and C. E. Giesler. Secure DBMS. RADC-TR-81-394; February 1982.

APPENDIX A

CR-200 DATA SECURITY UNIT

The AFIT Electrical Engineering Department has one CR-200 Data Security Unit, which is manufactured by Collins Telecommunications, a division of Rockwell International. The CR-200 is a stand-alone data encryption/decryption device for use in new or existing data communications systems to protect data in transit. This unit utilizes a single MOS/LSI implementation of the National Bureau of Standards′ Data Encryption Standard (DES) algcrithm as specified in Federal Information Processing Standards Publication (FIPS Pub) 46. The DES initialization and modes of operation are as specified in Federal Standard 1026. The cipher feedback mode is used for data encryption and decryption while the block mode is used for encryption and decryption of key variables.

The data encryption process occurs when the CR-200 receives clear text from the data terminal equipment (DTE) and outputs this data as ciphered text to the data communications equipment (DCE). In the decryption mode, the ciphered text from the DCE is decrypted and output to the DTE as clear text (see Figure 10). The CR-200 contains its own power supply, an input/output circuit card, a CPU/DES circuit card, and a circuit card that contains the keypad and front panel lamps.

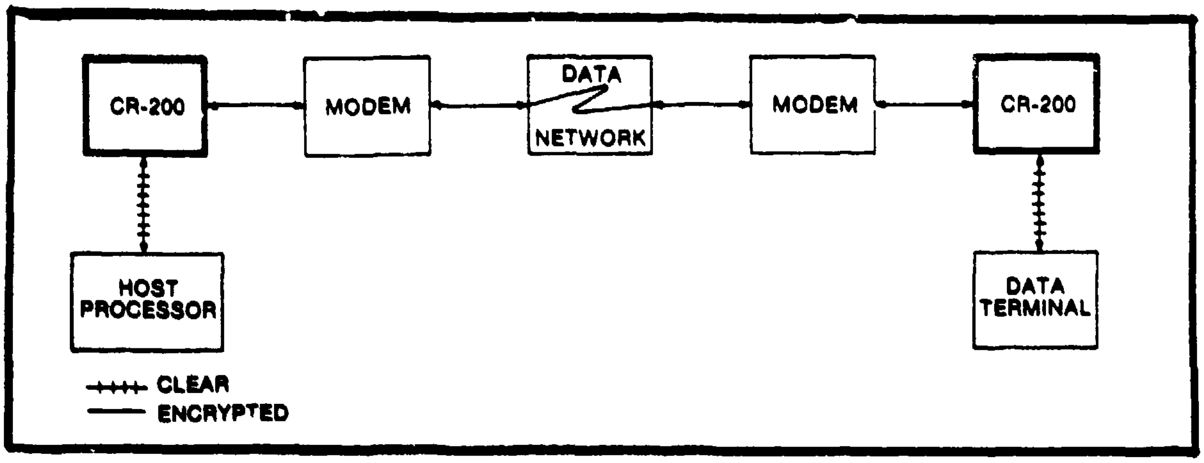

Figure 10 - CR-200 Single Link Encryption Configuration (COLL79)

CR-200 Operating Features

The CR-200 Data Security Unit can be applied to data networks operating full or half duplex, asynchronously or synchronously at data rates up to 9600 bits per second. Two major categories of protocols are supported - the Asynchronous Start-Stop and character-oriented synchronous (BISYNC and similar protocols). Extensive self-test capability is incorporated into the CR-200 to simplify system maintenance and fault isolation.

Internal storage for a total of five key variables is included. A battery backup for the key variable memory assures that the keys will not be lost during a power failure or when the unit is powered down. A special interlock destroys all key variables if the front cover is opened. Key variables may be loaded from the front panel key pad of the CR-200 or down-line loaded by means of "rekey messages" that are recognized and intercepted by the unit. Dual lock protection is provided for front panel entry.

CR-200 System Applications

Many configurations of data communication networks may utilize the CR-200. The least complex application is the encryption of a single host processor-to-data terminal link, referred to as the single-link encryption configuration, and is illustrated in Figure 10. One unit is inserted between the host and its associated modem, and a seocnd unit is inserted between the data terminal and its associated modem.

Another application simply extends the point-to-point case to include multiple terminals, all being serviced by a single host computer. This is referred to as the multidrop encryption configuration and involves the encryption of a host processor-to-multidrop terminal link (see Figure 11).

A third potential application of the CR-200 is in message-switched systems. The CR-200 is connected between each data terminal and the switched data network (see Figure 12). Since message-switched applications often utilize certain characters (which must not appear in the normal data traffic) to control the switch network, the CR-200 may be optioned (specified at time of order from Collins) to remove any such characters from the cipher text.

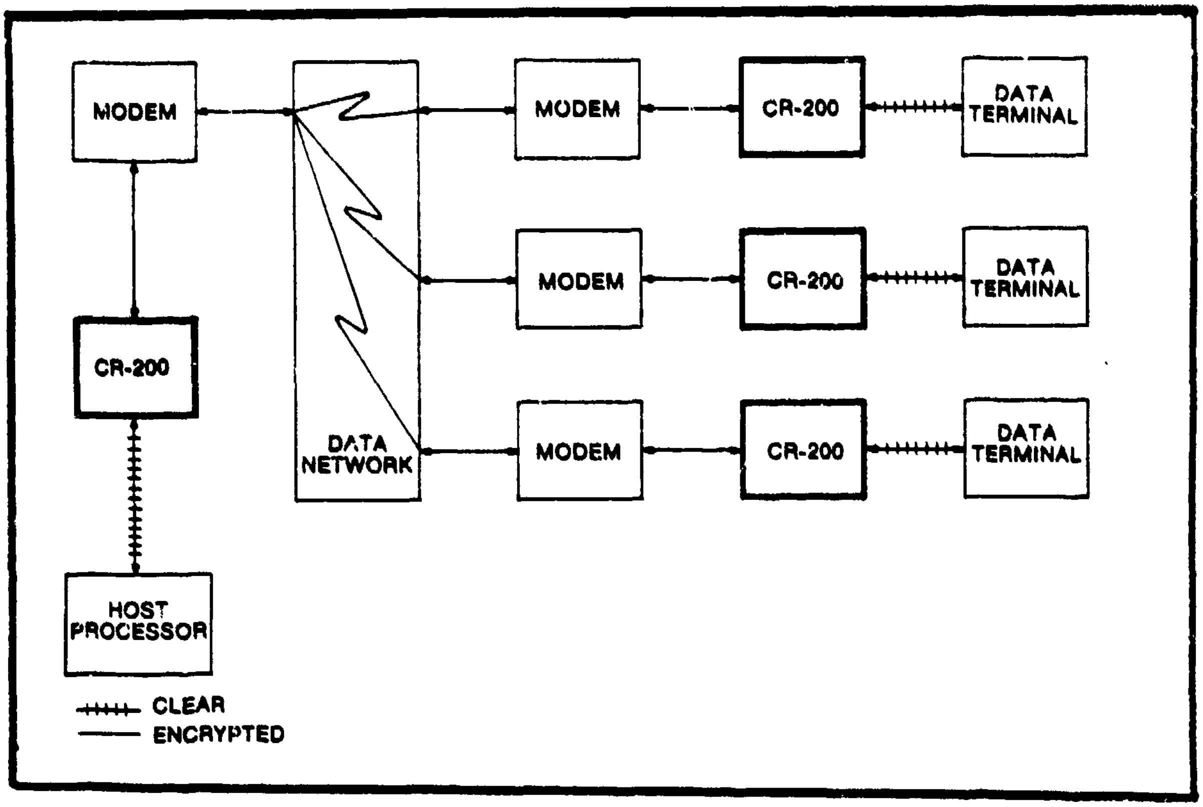

Figure 11 - CR-200 Multidrop Encryption Configuration (COLL79)

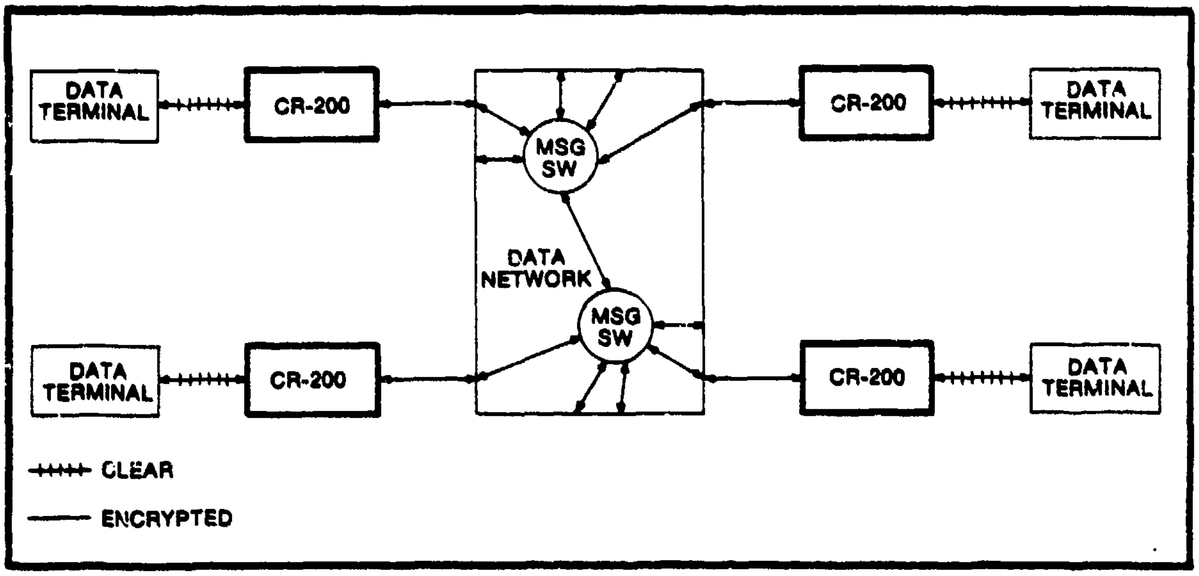

Figure 12 - CR-200 Message Switched Network Configuration (COLL79)

Key Management in the CR-200

Since the DES algorithm is public information, the entire security of DES-based encryptors resides in keeping the key variables secret (the key variable is a 56-bit number that controls the DES encryption/decryption operation). There are two basic threats to keeping the key-variable secret:

1) Unauthorized access to the key-variable generation, distribution, or storage process, and
2) Analysis of sufficient encrypted data to determine the key variable.

The strength of the DES algorithm makes the second threat a very expensive and time-consuming process involving trial and error of over 10^{16} key variables. By changing the key variable periodically, this process can be made prohibitively expensive or time consuming. A process inexpensive enough would take so long that the information encrypted in the particular key variable is no longer valuable by the time the key variable is determined. However, changing the key variable often increases the first threat by increasing the number of key generation, distribution, and storage processes which require protection. To ease this problem, the CR-200 employs a master/secondary key arrangement.

The master key (also called the key encrypting key "KEK") is used to encrypt secondary keys and becomes the only key variable that must be distributed and stored in a secure manner. By limiting its use to a relatively infrequent encryption of secondary keys, which are themselves pseudorandom numbers, the threat of determining the master key by analysis is all but eliminated. Since the analysis threat is low, the master key life is long (several years, for example) and there are few generation and distribution processes to protect.

The secondary key (also called the data encrypting key "DEK") is used to encrypt the actual data and is changed more frequently than the master key (daily, weekly, or monthly, for example). If it is encrypted before distribution and storage, these processes need not be secure. For example, the encrypted secondary keys could be distributed by telephone or mail without regard to who may have access to them during distribution. As long as the master key is unavailable to unauthorized persons, the encrypted secondary keys are secure.

The CR-200 has the capability to store and use five keys. A single master key, which may be entered only through the CR-200's front panel key pad, is used only to encipher new secondary keys. Four secondary keys, used to encrypt data traffic, may be stored in the unit, all of which may be down-line loaded through the network using a "rekey message".

A normal scenario of operation includes each CR-200 crypto unit in the data network having a unique master key. Each secondary key would be related to a message or group of messages and would normally be loaded through the network.

One use for the multiple secondary key storage is with multidrop network links. The units associated with the data terminals may use different secondary keys, and the unit associated with the host may store up to four of these secondary keys. As the host polls the different data terminals, it is not necessary to reload any secondary keys. Only a short command to change keys needs to be sent to the encryptor associated with the host.

Remote loading of secondary key variables (down-line loading) is accomplished by passing special "rekey" messages to the unit. These messages may originate from a data terminal keyboard or a processor that is part of the data network.

The Session Key

One interesting option available on the CR-200 is the capability to establish a "session key". The session key is a key variable that is generated by the transmitting unit, automatically loaded down-line to the receiving unit, and used for a single communication session. Once the interactive session has terminated, the key expires and any subsequent communication requires a new session key. This session key mode of operation is an option enabled by a hardware strap within the CR-200 unit. The session key is generated by a pseudorandom generator within the unit and is encrypted in the secondary key before being down-line loaded. When the session key option is enabled, the only use of the secondary key is to encrypt the session key. Thus, the useful life of a secondary key is greatly increased and the key distribution requirements are significantly reduced. The session key option is available only with asynchronous protocol units.

CR-200 Implementation Constraints in a LAN

The CR-200 Data Security Unit is intended primarily for encrypting data links between a host computer and its associated terminal(s). Such data links are usually connected to actual hardware I/O ports on the host computer, so terminal addressing from the host is not included in the data to be transmitted. Rather, the terminal addressing is accomplished by the host computer selecting the appropriate input/output port corresponding to the desired terminal.

This poses a problem for using the CR-200 in a local area computer network environment where there is no central host computer to manage the node-to-node addressing protocol. Since the CR-200 basically encrypts a stream of raw data for transmission, some means for adding appropriate header messages and packetising the data into a standard format such as the X.25 standard packet formats. The actual data intended for transmission in a local area network must be properly packaged into individual packets, each of which must contain network control parameters such as destination and source addressing information for connection management.

VITA

Wesley Allan Ballenger, Jr. was born on 22 March 1958 in Alexandria, Virginia. He attended Robert E. Lee High School in Staunton, Virginia until his Senior year, during which he attended Loudoun Valley High School in Purcellville, Virginia. Upon graduation from Loudoun Valley in 1976, he attended the University of Virginia School of Engineering and Applied Science in Charlottesville, Virginia, majoring in Electrical Engineering. There he accepted a three-year U. S. Air Force ROTC scholarship, graduating in May 1980 with a Bachelor of Science in Electrical Engineering.

Allan entered active duty in September 1980, and was assigned to the Air Force Wright Aeronautical Laboratories' Flight Dynamics Laboratory at Wright-Patterson AFB, Ohio. His primary job responsibility involved the development of multi-microprocessor flight control architectures for advanced digital avionics systems. In Spring of 1982 he was selected to attend the Air Force Institute of Technology to pursue a Master of Science in Electrical Engineering. He is a member of Eta Kappa Nu, Tau Beta Pi, and the Trigon Engineering Society.

Permanent Address: Box 124
Lincoln, VA 22078

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION
Unclassified

1b. RESTRICTIVE MARKINGS

2a. SECURITY CLASSIFICATION AUTHORITY

2b. DECLASSIFICATION/DOWNGRADING SCHEDULE

3. DISTRIBUTION/AVAILABILITY OF REPORT
Approved for Public Release;
Distribution Unlimited

4. PERFORMING ORGANIZATION REPORT NUMBER(S)
AFIT/GE/EE/83D-10

5. MONITORING ORGANIZATION REPORT NUMBER(S)

6a. NAME OF PERFORMING ORGANIZATION
Air Force Institute of Technology

6b. OFFICE SYMBOL *(If applicable)*
AFIT/EN

7a. NAME OF MONITORING ORGANIZATION

6c. ADDRESS *(City, State and ZIP Code)*
Wright-Patterson AFB, Ohio 45433

7b. ADDRESS *(City, State and ZIP Code)*

8a. NAME OF FUNDING/SPONSORING ORGANIZATION
Rome Air Development Center

8b. OFFICE SYMBOL *(If applicable)*
RADC/COTD

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c. ADDRESS *(City, State and ZIP Code)*
Griffiss AFB, New York 13441

10. SOURCE OF FUNDING NOS.

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT NO.

11. TITLE *(Include Security Classification)*
MODELING SECURITY IN LOCAL AREA NETWORKS

12. PERSONAL AUTHOR(S)
Wesley Allan Ballenger, Jr.

13a. TYPE OF REPORT
Master's Thesis

13b. TIME COVERED
FROM Feb 83 TO Dec 83

14. DATE OF REPORT *(Yr., Mo., Day)*
1983 December 16

15. PAGE COUNT
108

16. SUPPLEMENTARY NOTATION

7 Feb 84

Lynn Wolaver
LYNN E. WOLAVER
Dean for Research and Professional Development
Air Force Institute of Technology (ATC)
Wright-Patterson AFB OH 45433

17. COSATI CODES

FIELD	GROUP	SUB. GR.
9	2	

18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*

Security Models	Secure Communication
Computer Security	Local Area Network
Computer Network	Information Security

19. ABSTRACT *(Continue on reverse if necessary and identify by block number)*

The Department of Defense needs to process Data at various levels of security in Local Area Networks (LAN) of computer systems. A formal computer network security model is a necessary first step in certifying a computer system to process classified data. Several computer security models have been developed to identify what is required to enable multi-level certification of a computer system, and a similar model is needed for LANs.

The primary objective of this research project is to analyze the requirements of a LAN security model. Conceptual design issues of LAN security modeling are presented in this thesis to identify what must be achieved to ensure security is not violated when data of various levels of security are processed in a local area network.

Due to their distributed nature, LANs involve several security issues not addressed in security models (such as the Bell-LaPadula security model) developed for single computer systems. Therefore, modeling of security in LANs and computer networks must be complemented

(Continued on Reverse)

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT
UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. □ DTIC USERS □

21. ABSTRACT SECURITY CLASSIFICATION
Unclassified

22a. NAME OF RESPONSIBLE INDIVIDUAL
Walter D. Seward, Major, USAF

22b. TELEPHONE NUMBER *(Include Area Code)*
(513) 255-3450

22c. OFFICE SYMBOL
AFIT/ENG

EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

Block 19 Continued:

with LAN application and implementation considerations, primarily associated with secure communications channels between LAN subscribers.

This thesis analyzes the security requirements of a local area computer network, highlighting the need for a "security architecture" approach to modeling security in LANs. A textual definition of a prototype LAN security model is presented, and the model's application to hypothetical LAN configurations is discussed.