AD-A257 626

2

NAVAL POSTGRADUATE SCHOOL

Monterey, California

DTIC
S ELECTE D
DEC 0 1 1992
B

92-30450

THESIS

SECURITY ISSUES
IN THE
DEFENSE DATA NETWORK
by

David Allan Prevost

September, 1992

Thesis Advisor:	Tung Bui
Co- Advisor	Roger Stemp

Approved for public release; distribution is unlimited

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 is unlimited.
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)

6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School	6b. OFFICE SYMBOL *(If applicable)* 55	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c. ADDRESS *(City, State, and ZIP Code)* Monterey, CA 93943-5000		7b. ADDRESS *(City, State, and ZIP Code)* Monterey, CA 93943-5000
8a. NAME OF FUNDING/SPONSORING ORGANIZATION	8b. OFFICE SYMBOL *(If applicable)*	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS *(City, State, and ZIP Code)*		10. SOURCE OF FUNDING NUMBERS

10. SOURCE OF FUNDING NUMBERS

Program Element No.	Project No.	Task No.	Work Unit Accession Number

11. TITLE *(Include Security Classification)*
SECURITY ISSUES IN THE DEFENSE DATA NETWORK

12. PERSONAL AUTHOR(S) Prevost, David Allan

13a. TYPE OF REPORT Master's Thesis	13b. TIME COVERED From To	14. DATE OF REPORT *(year, month, day)* 1992 Septenber	15. PAGE COUNT 99

16. SUPPLEMENTARY NOTATION
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17. COSATI CODES

FIELD	GROUP	SUBGROUP

18. SUBJECT TERMS *(continue on reverse if necessary and identify by block number)*
DDN,Networks,Computers

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

This thesis provides a discussion of the problems associated with networking in the DDN and will help a local administrator of a DDN subnet identify vulnerabilities. Topics such as authentication and access control, communications security, encryption and detection are discussed in order to gain a better understanding of the DDN and what steps can be taken in order to reduce the risks associated with networking. Reccommendations are provided to enable the implementation of an effective program that seeks to reduce these risks to an acceptable level.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED □ SAME AS REPORT □ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION Unclassified	
22a. NAME OF RESPONSIBLE INDIVIDUAL Tung Bui	22b. TELEPHONE *(Include Area code)* 408-646-2630	22c. OFFICE SYMBOL AS/Bd

83 APR edition may be used until exhausted
All other editions are obsolete

Approved for public release; distribution is unlimited.

Security Issues in the Defense Data Network

by

David A. Prevost
Lieutenant, United States Navy
B.A., University of Texas at Dallas, 1986

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
September 1992

Author: David Allan Prevost
David Allan Prevost

Approved by: Tung Bui
Tung Bui, Thesis Advisor

R Stemp
Roger Stemp, Co-Advisor

David R. Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

This thesis provides a discussion of the problems associated with networking in the DDN and will help a local administrator of a DDN subnet identify vulnerabilities. Topics such as authentication and access control, communications security, encryption and detection are discussed in order to gain a better understanding of the DDN and what steps can be taken in order to reduce the risks associated with networking. Recommendations are provided to enable the implementation of an effective program that seeks to reduce these risks to an acceptable level.

Accession For
NTIS GRA&I ☑
DTIC TAB □
Unannounced □
Justification
By
Distribution/
Availability Codes
Dist | Avail and/or Special
A-1

TABLE OF CONTENTS

I. INTRODUCTION

The Defense Data Network is a DOD worldwide collection of computer networks. This integrated telecommunication resource is used by the Department of Defense and its constituents to conduct business, research and related activity on a day-to-day basis and is an invaluable resource to those who have access to it. The Defense Data Network (DDN) is continuously expanding, and as more constituents gain access, the security risk due to exploitation increases. As a result, a major concern of network administrators is the problem of maintaining a safe and secure network. Many attempts to explain the operation and functions of networks are often too technical in nature and do little to help network administrators understand the fundamentals of network security. This understanding is imperative if the DDN is going to continue to provide the Department of Defense (DOD) with an effective networking resource.

A. Scope

The main emphasis of this thesis will concentrate on an analysis of problems associated with maintaining large computer networks and the difficulties associated with security on these networks. Since the DDN is essentially a collection of smaller subnetworks, an analysis of these problems will help enable an understanding of the DDN security problem. Management issues in this paper will address steps system administrators of the Defense Data Network (DDN) can take to insure that all users of the network are authorized for access. This thesis will propose guidelines that administrators may follow in order to ensure that a secure operating environment is available for users of the DDN. Extensive use will be made of the DDN itself in order to obtain security information concerning the network and to have prompt access and response to those involved with network security.

B. Objectives

The objectives of this thesis are the following:

1. What are some of the security problems in large multi-function, multi-user computer networks such as the DDN and how are these problems being addressed?

2. What is the problem of network access and how can we insure that only authorized users have access to the DDN?

3. What are the communications security issues involved and how can we be sure they are properly implemented?

4. How can we detect unauthorized access and what steps can be taken to prevent it from occurring?

5. What are system administrators responsibilities and what should they do in order to ensure the network is secure?

This thesis will help enable a local administrator of a DDN subnet gain an understanding of the problems associated with secure networking as a whole and make him or her aware of the vulnerabilities of networking resources. Current regulatory documentation will be investigated to help identify and determine risk assessment, and help identify the responsibilities of local network administrators.

C. Thesis Organization

The thesis continues with a discussion of networking security issues in general, with an overview of the DDN in particular. Chapter II looks at the communication media of networks as well as the various network topologies used, and provides a brief overview of network protocols.

Chapter III examines the DDN security problem. The types of intrusions are classified and the various points of attack on networks are explained. The types of individuals who intrude on networks and their motives are also analyzed. Chapter IV reviews penetration techniques that are used to gain access to networking resources.

Chapter V examines basic security principles and looks at authentication and access control in computers. Also the topic of multilevel security in networks is briefly discussed. Chapter VI discusses the communications linkages that interconnect networks and the different types of security approaches involved. Trusted hosts and trusted networks are examined as well.

A non-technical analysis of cryptography common in networking is presented in Chapter VII. This includes a look at both link and end-to-end encryption techniques used in networking environments. Chapter VIII looks at techniques used to detect and prevent unauthorized access to networks from taking place. Chapter IX, the final chapter offers conclusions and recommendations that may assist administrative personnel in maintaining a secure and reliable network.

II. INTRODUCTION TO THE DEFENSE DATA NETWORK

The Defense Data Network (DDN) is a large military common-user data communications internetwork operated for the Department of Defense (DOD) by the Defense Network Systems Organization (DNSO) of the Defense Information Systems Agency (DISA)[1]. The DDN is a very large and powerful military network. It can be thought of as an umbrella network composed of several large segments or subnetworks. The unclassified portion of the DDN is a subnet known as the MILNET. The MILNET connects the DDN to an even larger network that includes military contractors, universities, and research centers. This entire collection of interconnected networks is called the "Internet" and its users number in the thousands. With the rapid expansion of the DDN over the last few years, the issue of security has become a topic of growing concern.

A. Network Security

Network security is a complex topic involving not only conventional computer security issues such as authentication and access control measures, physical security, electromagnetic emanation, procedural and personnel security controls but also communications security[2]. The medium used to interconnect computer communications systems represents an additional security dimension that significantly increases the vulnerability of computing resources. The use of encryption in networks, both end-to-end and link level, is just one method used to address network communications security. To maintain the security and integrity of a large network requires a complex combination of policies and technologies. The problems of network security are applicable not only to the DDN and its large infrastructure, but also apply to any networking environment where there is a concern regarding unauthorized access. Networking security issues are not only concerned with hardware and software issues but with the human element as well. What are the types of people who use networks and what are the types of people who abuse it? How penetration of a network is achieved and what measures can be taken to curtail unauthorized activities are just some of the issues that need to be addressed.

There are several trends that emphasize the need to develop network security measures. The increased use of networks to provide remote access to computer facilities, coupled with improved physical security measures at computer sites, makes attacks on networks more attractive to an intruder. The growth in the quantity and value of information made vulnerable by weaknesses in network security further enhances the attractiveness of networks as intruder targets[3]. Computer systems connected by networks are more likely to cooperate in various ways to provide resource sharing for a user community, and in so doing the security of information on a given computer or host may become dependent on the security measures employed by the network and by indifferent hosts. The development of new network technologies has made certain types of attacks on communications systems easier, such as passive wiretapping attacks. Many models and mechanisms developed in the course of research in computer system security are directly applicable to or easily adapted for use in the network environment. This relationship is not one-sided however, since the security mechanisms incorporated in a computer system accessed via a network can be rendered largely ineffective if the network fails to provide a secure communication path between each user and the computer system[4].

B. Networking Communications

The Internet is a method of interconnecting physical networks and allows the computers they reach to interact. A chief advantage of the Internet is that it provides universal interconnection while allowing individual groups to use whatever network hardware is best suited to their needs. There are basically two approaches to network communications: circuit-switched and packet-switched technologies.

1. Circuit-Switched Networks

Circuit-switched networks operate by forming a dedicated connection or circuit between two points. The telephone system is an example of circuit switching technology. One advantage of a circuit-switched network is the fact that once a circuit is established network capacity is not affected by others since the connection is a dedicated link between the two points. A disadvantage is cost: circuit costs are fixed independently of traffic load[5].

2. Packet-Switched Networks

Packet-switched networks, the type most commonly used to connect computers, take an entirely different approach. In a packet-switched network a terminal or source host computer passes a message along with its destination address to the local Packet Switching Node (PSN) computer. The PSN breaks the message into small uniform pieces called packets that are multiplexed onto high capacity intermachine connections. Each packet, which usually contains only a few hundred bytes of data, carries routing information that enables computers on the network to know the packets' correct destination. The packets are passed from PSN to PSN until they reach their destination PSN, where they are reassembled in their original order and delivered. A packet-switched network differs from a circuit-switched network in that no predetermined dedicated path exists for delivery of the data. Each packet takes the best route that it can find at the time, and packets in the message do not necessarily take the same route. Once the packets arrive at the destination PSN, they are reassembled in the correct sequences and delivered to the host as a complete message[6]. The chief advantage of packet-switching is that multiple communications among computers can proceed concurrently; however, the disadvantage is that as network activity increases, a given pair of communicating computers using the network may experience significant increases in response time, and therefore diminished throughput.

C. Network Topology

A single computer system in a network is referred to as a node, and its processor is referred to as a host. The connection between to two hosts is known as a link, and the pattern of links in a network is called the topology of the network[7]. In one commonly used network topology known as a bus, all nodes of the network are connected to a single conductor. The network hosts place messages on the bus and the addressees monitor the bus, taking off messages addressed to them[8]. An alternate method used is known as ring topology. In this topology each network host has two neighbors arranged in a circular pattern. When one host has a message to send, it passes its message to its adjacent neighbor which forwards the message on until the destination host receives the message. The star topology uses a centralized host controller. All nodes wishing to communicate do so through the central host[9]. The central host receives all messages, identifies the addressee, selects the link appropriate for that addressee, and forwards the message[10]. There are several technologies that have emerged to handle data communications. The most prevalent are the Ethernet bus technology and Token Ring technology.

1. Ethernet

Ethernet is the name given to a popular local area packet-switched network technology invented at Xerox in the early 1970's. It uses broadcast bus technology with a best-effort delivery system and distributed access control[11]. In a broadcast bus system all stations share a single communication channel and all transceivers receive every transmission. Ethernet access control is distributed because, unlike some network hardware, there is no central authority granting access. The Ethernet access scheme is called "carrier sense multiple access with collision detect" (CSMA/CD). Multiple machines can access the Ethernet simultaneously and each machine determines whether the transmission path is idle by sensing whether a carrier wave is present. When a host interface unit has a packet to transmit, it listens to the ether to see if a message is being transmitted. When no transmission is sensed, the host interface starts transmitting. If a carrier wave is detected the machine waits a random unit of time before attempting to retransmit the packet.

2. Token Ring

Another commonly used technology is the Token Ring network. It uses a one way ring and uses an access protocol known as token passing. The primary distinguishing feature of token-passing systems is that they achieve fair access by having all machines take turns using the network. At any time, exactly one machine holds a token which grants that machine the right to send a packet. After sending its packet, the machine passes the token to the next machine in sequence, and so on. Thus, when none of the machines has anything to send, they continually pass the token around; when they all have packets to send, they take turns sending them[12].

3. Protocols

There is no predominate technology in use in the DDN. What makes the Internet unique is the ability of the different types of systems to communicate with each other. This is accomplished through the use of protocols. Protocols are to computer communication and networks what programming languages are to computation[13]. Complex data communication systems do not use a single protocol to handle all transmission tasks. Instead, they require a set of cooperative protocols, sometimes called a protocol suite. These different protocols are used to interconnect the different types of systems in use throughout the internet and for the most part are indistinguishable to the network terminal operator who uses the internet.

D. Summary

The DDN is an extremely large network composed of a variety of computing resources for use by DOD and its affiliated organizations. The unclassified portion of DDN is known as the MILNET. These resources are subject to unauthorized access at many different levels and the issue of network security within the DDN is a topic of extreme importance. Many steps can be taken to ensure unauthorized access to the DDN is curtailed. Authentication and access control, communications security and encryption are just a few of the ways in which the integrity of the DDN can be maintained. Networks use a set of conventions called protocols that allow the computers they reach to interact. A variety of topologies have been developed to allow communications between computer systems. A packet-switching technology is used that breaks messages into a series of packets to be transferred along a communications path between different users regardless of the type of architecture and topology of the individual subnets that comprise the Internet and the DDN.

III. DDN SECURITY PROBLEMS

A. General

A computer network is a telecommunications system primarily designed to allow a number of independent devices such as host computers, workstations, terminals and peripherals to communicate with each other. The DDN is essentially a collection of assorted networks all interacting to provide a comprehensive resource of information for the Department of Defense and its associated organizations[14]. As the network has expanded so have the risks associated with maintaining a secure and troublefree network. The points of attack have increased as the network has expanded because potential intruders have obtained a greater understanding of the vulnerabilities associated with the network. Abuse of the network by both authorized and unauthorized persons is a continuous problem in the DDN.

On November 2, 1988 Robert Tappan Morris drastically changed the attitude of network users and administrators concerning networking security. He unleashed his infamous Internet worm which afflicted over 6,000 MILNET and other Internet hosts. The program exploited flaws in utility programs in systems running the UNIX operating system. The flaws allowed the program to break into those machines and copy itself, thus infecting those systems. The incident caused a panic because most of the sites effected were ill prepared for such a massive scale of intrusion[15]. It was fortunate, in a sense, that the attack was unrestrained because it showed the vulnerability of computer networking resources to intrusion.

B. Intrusion Classifications

The DDN security problem can be described as the accidental or intentional disclosure, destruction, or modification of information flowing on or accessed through the DDN. Identifying the security problem or threat is a key element in determining the risks involved in the DDN. The problem can be evaluated in several ways. First, there is the unauthorized access of information by either persons or programs that amount to unauthorized use of a network or computer resource without access permission. Such unauthorized access may open the door to other security threats including the use of one computer facility to access other sites on the network[16]. Another problem is the unauthorized disclosure or modification of information. Depending on the sensitivity of the information, disclosure without modification may have more damaging consequences than if the intrusion goes unnoticed. The modification of existing data compromises the integrity of the information in the Internet[17]. Finally there is unauthorized denial of information which is in essence a denial of service to legitimate users of the network. In fact, an entire network may be made unusable by a rogue packet, jamming, or by a disabled network component. (The Morris Worm had all of these characteristics)[18].

C. Attack Points

In evaluating security requirements one must take into consideration the vulnerabilities of individual computers on the network and the network system as a whole. Consideration should be given to the attack points at which these systems are most vulnerable. Potential points of attack are on the hardware, software, and the communications connections between different terminals and hosts. Because of the nature of networking communications, the linkages between different users within the Internet are one of the primary vulnerabilities of networking.

1. Hardware Attacks

Hardware attacks include not only intentional acts such as vandalism and sabotage but natural disasters such as fires and floods. Usually deliberate hardware attacks can be easily prevented by simple physical measures such as locks and secure buildings. In most cases the prevention of hardware attacks on computers can be controlled by simple physical means.

2. Software Attacks

Although software attacks are most often accidental, such as the unintentional deletion of files or programs, we usually associate software attacks with some type of intentional deletion or modification of data (or programs) that render the software unusable, or which violates the integrity of the applications in some way. In network applications these are much more difficult to prevent than in stand alone computer systems. For this reason, stringent security considerations are required to inhibit attacks on software.

3. Interconnections

Of all the attack points, perhaps the most vulnerable are the links that interconnect the different terminals and hosts within the Internet. These connections include terminal-to-network interface connections, terminal-to-terminal interface connections, and terminal-to-host connections. These types of connections make the problem of security in networks much more difficult than the problems associated with stand alone computer security.

D. Network Abusers

Frequently, the weak link in network and computing systems is the people who use them. Individuals who intrude on networks or computer systems in general can be classified in two ways. Those who seek to gain access to the system with the explicit intent of purposely causing damage, or those who accidentally damage resources is some fashion either through unintentional or intentional access.

1. Unintentional Intrusion

Unintentional intrusion may appear to be relatively harmless but the fact is that any unauthorized release, access, or modification of information can have profound repercussions in most circumstances. For example, there are potential legal problems associated with unauthorized disclosure; additionally, the loss of customer goodwill in many business organizations due to disclosure can do much to damage an organizations reputation. The initial damage is still the same regardless of why or how.

2. Intentional Intrusion

Intentional intrusion is a much more serious matter. The problem is more serious not because the damage caused is greater, but because it often involves illegal activity in some manner. According to the FBI each year intentional malicious activity accounts for anywhere from 300 to 500 billion dollars a year in costs[19]. Amateur computer users account for the majority of computer crime committed to date and their activities are expanding every year. Amateurs can be classified as non-computer professionals who are usually tempted by the opportunity to obtain personal profit, revenge against a person or institution, or the challenge.

They usually are not technically sophisticated in their techniques but possess just enough knowledge to cause substantial damage.

Hackers and Crackers are another category of abusers that are usually associated with university or high school students who attempt to access computer facilities for which they are not authorized. While these may not appear to be serious offenders they have caused substantial monetary damages to institutions which they have penetrated. The term *Hackers* is usually associated (by the news media) with innocent intruders who, in many cases may actually enhance technological innovation through their ability to continuously penetrate existing systems. *Crackers*, on the other hand, are those who penetrate systems with the direct intent of causing damage. *Career Criminals* are computer professionals who engage in computer crime knowing the full implications of their transgressions. They actively seek out targets and attack them in order to realize some type of gain at the expense of those they have attacked. It is often difficult to apprehend career criminals because their computer expertise often allows them to manipulate the system undetected. Even when they are apprehended it is difficult to prosecute them because there is a lack of precise legal definitions as to what constitutes computer crimes. Organizations often choose not to prosecute those involved in computer crimes because of the difficulty and costs associated with prosecution in addition to the potential loss of public confidence in the victim organization.

E. Summary

The threat to the DDN and to the Internet in general can be viewed as the unauthorized access of information, unauthorized disclosure or modification of information, and unauthorized denial of information. As the DDN has expanded the threat to Internet resources has expanded with it. In assessing these threats we can evaluate software, hardware, and the communications medium that interconnect the network as potential points of attack and we can take steps to reduce these vulnerabilities. The identification of the types of individuals who may possibly intrude on the DDN is important for taking security precautions against potential violations. Charles Pfleegers' book "Security in Computing" and the "DDN New Users Guide" by Barbara Varallo are excellent sources that discuss these topics. In Chapter IX, I have proposed several recommendations to help network administrators reduce the threat due to these vulnerabilities.

IV. NETWORK PENETRATION

A. Introduction

In evaluating the security relationships between different hosts on the Internet one must consider the various penetration techniques that intruders use to access computer networks. The techniques used for penetration are closely associated with the computer or networking systems vulnerabilities. Therefore, successful prevention requires the identification of these vulnerabilities. Through analyzing a systems protection mechanisms, how they function, and their deficiencies, consideration can be given to how such mechanisms can be circumvented, nullified, or deceived. A particular type of technique may be used to exploit more than one vulnerability, and a vulnerability may be exploited by more than one technique. Some penetration techniques leave signatures (residual traces) and others do not. Such signatures, their detection, and analysis, are fundamental to threat monitoring and security auditing. Many of these techniques can be categorized by the types of activity they involve and the system vulnerabilities they exploit.

B. Viruses and Worms

By far the most common type of penetration is the use of what are called viruses not to be confused with a worm. Confusion as to whether a rogue program is a worm or a virus is due to a subtle difference in their behavior. A viral program, or virus, is a piece of code that attaches itself to other programs (hosts), including operating system files; however, it cannot run independently. It requires that its host program be executed in order to activate the viral code segment. A worm is a fully functional, independent program that can run by itself and propagate a fully working version of itself to other machines. It is derived from the word tapeworm, a parasitic organism that lives inside a host and saps its resources to maintain itself[20]. Precautions must be taken to inhibit both types of these attacks.

C. Finger Programs

One type of penetration technique exploits a system utility known as the "finger program". This program is a utility on Unix based computer systems that allows users to obtain information about other users. It is generally used to identify the full name or login name of a user, determines whether or not the user is currently logged in, and then obtains other information about other users. This program can be exploited by an intruder to obtain critical information necessary to access the system.

Another type of attack is through the exploitation of the electronic mail utility found on most systems. The Morris worm took advantage of a little known debugging access (trapdoor) in the utility that allowed testers to verify that mail was arriving at a particular site without the need to activate address resolution routines.

Potential intruders can also take advantage of sloppy administrative techniques. Many system services have configuration and command files owned by a common user identification number. In other words, systems that have services such as electronic mail, finger utilities, file transfer protocol (FTP) and others, all use the same user identification number to utilize these services. The simple process of assigning different user identification numbers could help reduce the vulnerabilities of penetration.

D. Passwords

One of the most well-known penetration techniques is to attempt to discover authorized user passwords. The attacker accomplishes this by using a list of possible passwords and comparing them against the actual passwords. The security of the password is provided in large part by the prohibitive effort of trying all combinations of letters. Unfortunately, as machines get faster, the cost of such attempts decreases. Potential intruders may utilize what is known as "cracker" programs in order to exploit poor password selections. These programs systematically try all possible password combinations that are in a file. The file may consist of all the words in a dictionary or a carefully constructed set of possible passwords based on some personal knowledge of the user.

E. Browsing

Browsing allows an individual to gain unauthorized access to a users files by exploiting vulnerabilities in the file access control mechanisms in the operating system. Browsing requires an understanding of the general system specific naming convention of computer files. Unauthorized system users can use this technique numerous times to browse through all the files looking for classified or sensitive information. This technique is not generally possible when the files are protected by passwords or other security precautions.

F. Masquerading

Gaining unauthorized access to a system by assuming the identity of another authorized user is called masquerading. The success of this technique stems from a computer system's inability to establish a user's identity other than through symbolic identifiers. The easiest method of masquerading is to obtain the password and other identifiers of an authorized user from some report or document that was carelessly left exposed. This situation is most likely to occur in installations that support remote terminals where no option exists to have such identifiers suppressed by the terminal during the log on procedure. Even when a terminal does possess suppression capabilities which overtypes these identifiers before or after their printing, it may still be possible to obtain the identifiers. A more sophisticated technique for gaining access to an authorized user's identifiers is to wiretap the terminal and intercept the identifiers when they are transmitted in the clear over communication lines[21]. A much less sophisticated, but very common technique, is to look over someones' shoulder as they are entering their password on a terminal or when they are writing it down to keep from forgetting it. Regardless of how the intruder gains access to the system the damage can be the same.

G. Scavenging

This penetration technique exploits the vulnerability of unerased residual data. Both primary and secondary storage media used for processing information may continue to retain information after it has been released for reallocation to another user or program. The latter may then scavenge the information by reading the storage media before making any other use of it[22].

H. Unknown System State Exploitation

This method takes advantage of certain conditions that occur after a partial or total system crash. For example, some user files may remain open without an end-of-file indication. Another individual or program may then obtain unauthorized access to other files by reading beyond that indicator when the system resumes operation.

I. Asynchronous Interrupt

This technique exploits system vulnerabilities arising from deficiencies in the interrupt management facilities of an operating system. If a processor suspends execution of a protection mechanism to process an interrupt and is then erroneously returned to a user program without completing the security check then the protection has been circumvented[23].

J. Spoofing

Spoofing exploits the inability of remote users to verify that they are actually communicating with the intended system rather than some masquerading system. This deception, also known as a "Mockingbird Attack," can be perpetrated by intercepting the terminals communication lines and providing system-like responses to the user. A variation of spoofing is the use of an application program to provide responses similar to the operating system, so the operator will unknowingly provide the passwords to an application program and not to the operating system[24].

K. Trojan Horse

In this technique computer processing is covertly altered by either modifying existing program instructions or inserting new instructions. Once this has been accomplished, whenever the altered processes are used the perpetrator will automatically benefit from unauthorized functions performed in addition to the routine output. This modification is usually done by hiding secret instructions in either the original source-code or the machine-code version of a lengthy program. Even harder to detect is the alteration of the operating and utility system programs so that they make only temporary changes in the target program as it is executing. The hardware version of the Trojan Horse technique is relatively rare. However, the replacement of valid micro-chips with slightly altered counterfeit chips is entirely possible and would is extremely hard to detect. In either the software or hardware Trojan Horse method, only someone with access to a program or the computer system could become a perpetrator.

L. Clandestine Machine Code Change

This technique is closely related to the Trojan Horse technique. It allows system programmers to insert code into the system that creates trapdoors. At specific times based on certain combinations, these trapdoors can be activated by an intruder through the user's program. Individuals who initially design the system, contract maintenance personnel who fix the system, or people who are able to gain access to the supervisory state also have this opportunity. The technique could be as simple as users stealing job card information on work that has already gone through the system. They then resubmit this information to the system on their own job cards along with another program[25].

M. Summary

Understanding the way an unauthorized intruder attempts to gain access to a network system is important in preventing unauthorized and potentially harmful exploitation. The types of techniques used are closely related to the type of networking system employed. By analyzing these techniques and exploiting their vulnerabilities the integrity of a networking communications system can be maintained.

V. NETWORK SECURITY

A. Security Principles

Network security can be defined as the protection of network resources against unauthorized disclosure, modification, utilization, restriction, or destruction. When evaluating security in the DDN we can consider three fundamentally important areas:

1. The physical security of the computer systems and the network as a whole.
2. Access to the resources of the network.
3. Communications security of the medium of information transfer.

B. *Physical Security*

Certainly one of the most fundamental aspects of security, and one of the most easily understood, is physical security. Physical security includes the facilities that house the computers, hosts, and other peripheral devices as well as the remote terminals that comprise the network. Another way to describe it is the external protection provided for the computer system. This physical protection also includes controlling the dangers due to natural disasters such as fire, floods, storms and other unscheduled contingencies. Protection against physical entry by prospective intruders must be maintained in order to ensure a secure system and as a result, physical security considerations are often one of the most easily addressed of all security precautions.

C. Authentication and Access Controls

The most challenging security consideration in networks is the problem of authentication and access control. Although authentication and access control mechanisms are logically and functionally separate, they are related in that the decisions made by access control mechanisms are based on information supplied by authentication mechanisms. Both types of mechanisms are, in turn, dependent on communications security measures since violations of communications security can result in circumvention of the security policies implemented by the authentication and access control mechanisms. Authentication and access control mechanisms have been studied extensively in the context of individual computer systems, and many of the techniques and much of the terminology developed in that context are applicable in a network environment as well. However, the desire to provide flexible and controlled sharing of resources in networks introduces the need for additional authentication and access control techniques[26]. In a security context, the term authentication applies to procedures for verifying the claimed identity of a user, whether this user is embodied as an individual, a terminal, or a network. A variety of techniques have been developed for personal identification including various password schemes, the use of badges and keys, and physical characteristic measurements such as fingerprints, voice prints, and retinal scans.

1. Passwords

The most common type of authentication mechanism is the use of passwords. One of the easiest ways an intruder can get into a system is by breaking into someone's account. This is usually easy to do, since many systems have old accounts whose users have left the organization or accounts with easy to guess passwords. If an intruder can discover a user's password he or she can log in to the system and operate with all the capabilities of that user. If the password obtained is that of a system administrator then the intruder will have read and write access to most every file on the system, or to put it another way, he will have administrative capabilities on that network. For this reason, choosing secure passwords is very important.

One of the most significant problems with password authentication systems is that users often choose very poor passwords. Experiments have been conducted to determine typical user's habits in the choice of passwords. In a collection of 3,289 passwords, 16% of them contained three characters or less, and an astonishing 86% were those which could generally be described as insecure[27]. Additional on. Next, the worm tried each word present in an internal dictionary of 432 words. When all else failed, the worm tried going through the system dictionary, trying each word. The password selection criteria discussed above successfully guard against all three of these strategies[30]. Appendix A provides guidelines to follow when selecting passwords.

2. Token-Smart Cards

A means of authentication that is becoming quite popular is the use of token or smart cards. Anyone that has used an automated teller machine is familiar with the token card. Credit type cards with magnetic strips contain information that permit access to the system. Simple reading mechanisms can be built into the computer systems without great expense. The problem with the use of this type of mechanism is the cards can easily be lost or stolen. Theft may even be unnecessary, since credit cards may be readily duplicated, including the magnetic strip with its coded information. A modification of the token card is the smart card. It is similar to the token card except it has an embedded microprocessor. A smart card is not just a passive container of data. It can actually perform computations, such as computing the response function of a challenge response system, or providing public key encryption services. Since the smart card can be configured with a local challenge and response system, the fact that it is stolen by an intruder does not necessarily mean that he or she can gain access. The proper response to the challenge query must still be known. The smart card is a much more secure means of access than the token card since access can not be obtained if the card is lost or stolen. This avoids a characteristic problem of token systems in which a user must possess something to gain access that may be lost or stolen.

D. Physical Characteristics Access Control

The problem with using information such as passwords for authentication is the information that grants access to the network, the password, may become known to another person. Items such as tokens, smart cards or other physical devices that grant access may be stolen or duplicated. Authentication mechanisms have been developed in recent years that use the personal physical characteristics of authorized users to grant access. These devices include finger print and voice print analysis, as well as retinal scans. A device for the verification of a person's identity compares a measured set of electronic data, representing a characteristic of someone claiming to be authorized to use the system, with a set of stored data taken from the authorized person. However, it is sometimes difficult, when working with body measurements and other human processes, such as speech or writing, to establish accurate reference points and obtain repeatable registration for the measurement and matching of patterns[31].

1. Fingerprints

Matching fingerprints is a useful technique which can be performed either at the local or host site, or by reading the prints locally and making a comparison by means of a computer at a remote site. The fingerprints are electronically scanned either through a lighted prism or by reading a sensitized card on which they have been placed[32]. In a self contained system, the image is compared with one stored to produce a signal showing the degree of similarity between the two prints. If the similarity is acceptable, the person is cleared. Acceptance or rejection by most identification devices may be signaled by a light or by a readout on a video display terminal. A more complex verification method requires transmission of fingerprint signals to a remote computer, either the host itself, or a computer at the network control center. This does away with storing the file of prints locally, and so reduces the chance of an intruder gaining access by tampering with the local device[33]. One of the primary advantages of using fingerprints and other authentication control mechanisms that use physical characteristics is the medium to gain access, in this case the fingerprints, cannot be lost or stolen. Although the use of fingerprints is a more secure access control mechanism than passwords, it is possible for a sophisticated intruder to duplicate fingerprints.

2. Voice Recognition Systems

One type of access control mechanism that can be used is voice recognition systems. A computer can analyze digitized voice signals accurately enough to distinguish one voice from another, and to verify a speaker's identity. One such computerized voice verification system is first trained with a vocabulary of selected words. The person seeking access to the system enters a claimed identity by keyboard to retrieve a reference profile. The system then generates a phrase from the vocabulary and presents this phrase to the person over a loudspeaker using prerecorded or synthesized speech[34]. The person repeats the phrase into a microphone which transmits the signals to digitizing circuits and then to the computer. The computer then locates specific parts of speech waveforms and matches them against the appropriate reference profiles. If they match within a specified tolerance, the person's identity is considered verified, otherwise he or she is rejected. The reason for using several words from a larger vocabulary is to prevent an imposter from using a recording of an authorized person's voice. Even if the imposter had a recording of the vocabulary as spoken by an authorized user, it would be quite difficult to pick out the designated words and play them into the microphone in the short time available. There is considerable controversy regarding the possibility of recognizing speakers over ordinary telephone circuits, due to noise and loss of fidelity. The quality of these circuits also varies considerably from one connection to another. It is possible to digitize the voice at the source so that it may be transmitted without distortion. This would require special equipment for digitizing and buffering the spoken phrases, and would probably increase transmission time considerably, since high-fidelity speech has a higher information content than that transmitted by telephone lines[35]. It is for this reason that voice recognition systems are not considered practical alternatives for access when used in a networking environment.

3. Retinal Scanners

The most secure means of authentication is the use of retinal scanners. Each person's eyes have a distinct pattern of blood vessels that are unique to that person, much like fingerprints. The information that maps the eye is digitized and recorded. To gain access a person's eyes are scanned and the information is compared with the recorded information. The use of retinal scanners is extremely secure but also very expensive to implement. It is usually used for extremely sensitive access requirements. The use of retinal scanners to gain access to a network is very rare, much like the use of fingerprints.

E. Multilevel Security

The techniques discussed so far, have been concerned primarily with security as it relates to the individual user. A somewhat different, but widely applicable requirement, is to protect data or resources on the basis of levels of security[36]. This is commonly found in the military, where information can be unclassified, confidential, secret, top secret, or beyond. The concept of multilevel security is applicable in other areas where information can be organized into categories and users can be granted clearances to access certain categories of data. For example, the highest level of security might be for strategic planning documents and data, accessible by only high level personnel and their staff. Next might come sensitive financial and personnel data, accessible only by administration personnel.

When multiple categories or levels of data are defined, the requirement is referred to as one of multilevel security. The requirement, which is based on current finite state security models, is in two parts and can be simply stated as follows: A multilevel secure system must enforce[37] no read up, that is a subject can only read an object of a less or equal security level. It must also enforce no write down, a subject can only write into an object of greater or equal security level. These two rules, if properly enforced, provide multilevel security, however, the overhead required to implement a multilevel security apparatus is significant, and the restrictions they impose create additional problems in a distributed environment.

F. Summary

The large number of people who have access to data networks creates significant concern over the need to accurately verify their identities. Intruders continue to gain unauthorized access to networks and are causing widespread damage to computing resources. This problem has become especially acute since the incorporation of many smaller subnets into the Internet do not provide adequate security measures. The increased demand for security has produced a variety of protective devices that verify the identity of a person at the terminal before allowing that individual access to the network. These authentication and access control mechanisms include physical security measures, as well as other techniques such as passwords, token keys or identification cards. Personal characteristics mechanisms such as handwriting, fingerprints, and voice patterns are becoming more and more common in order to neutralize potential attackers. Chapter IX provides guidelines to help determine the appropriate types of authentication and access mechanisms for networks.

VI. COMMUNICATIONS SECURITY

A. Security Approaches

There are two basic approaches to considerations of communications security. These are link-level and end-to-end level security measures. The former independently protects messages on each of the communications links, while the latter provides continuous protection for each message from its source to its destination. When evaluating these two approaches one must look at the communication medium used at various links in the network and their susceptibility to attack. The use of trusted hosts and trusted networks ensure the integrity of link-level and end-to-end systems.

1. Link-Oriented

Link-oriented protection provides security for messages passing over an individual communications link between two nodes independent of the ultimate source and destination of the messages. The underlying assumption in providing protection of this sort is that it is much easier to attack the communications link, rather than the nodes themselves. However, often it may not be possible or economically feasible to physically secure nodes in a network as readily as in the terminal and host nodes. Yet, subversion of one of the packet switching nodes results in exposure of all the message traffic passing through that node, despite the physical security precautions in effect at the source and destination. If the only unsecured communication link in a network occur within the communication subnet, link-oriented measures have an advantage, in that they can provide a transparent form of communication security for the hosts attached to the network. If only some of the communication links between terminals and hosts need to be protected, security measures for these links can be implemented without affecting the other hosts on the network[38].

2. End-to-End Oriented

Rather than viewing a network as a collection of nodes joined by communication links, each of which can be independently protected, one can view a network as a medium for transporting messages in secure fashion from source to destination. From this perspective, end-to-end security measures protect messages in transit between source and destination nodes in such a way that the subversion of any of the communication links between the source and destination does not result in exposure of message traffic[39]. There is some flexibility in defining the points at which end-to-end security measures are implemented: from host to host, from terminal to terminal or service host, or from terminal to process on a service host. By extending the domain of end-to-end security measures, more of the communication path between a user and his application, or between a pair of users, is protected. However, as the domain of such measures is extended, the range of hardware and software that must interface with these measures may increase[40]. Since end-to-end security measures usually extend beyond the communication subnet, these measures sometimes require a greater degree of standardization of interfaces and protocols for subscribers to the network. However, such standardization is already coming about for technical, economic, and political reasons. A major advantage of end-to-end security measures is individual users and hosts can elect to employ them without affecting other users and hosts, and thus the cost of employing such measures can be more accurately apportioned. Moreover, these measures can be employed not only in packet-switched networks, but also in packet broadcast networks, where link-oriented measures are often not applicable.

3. Connections Oriented

In many applications, a communication network is viewed as providing its users with a medium for establishing connections or virtual circuits from source to destination. This view suggests that security services be connection-oriented. Thus, connection-oriented security measures constitute a refinement of end-to-end measures[41]. As is the case with end-to-end security measures, there is considerable flexibility in choosing the points that are to act as the ends of the connection for security purposes. Connection-oriented security measures not only protect that portion of a communication path that lies between the security-defined ends of the connection, but also significantly reduce the probability of undetected cross-talk, whether induced by hardware or software, over that interval[42]. In the case of a full-duplex connection between a terminal and a process on a service host, the connection is composed of two independent simplex channels. In many applications, the connection exists for the duration of a single log-in session. Both the terminals and the host are assumed to reside in secure areas while the remainder of the network may be subject to exploitation. A terminal may, at different times, be used by various individuals over a range of authorization levels. The host provides services to a diverse user community, not all of whose members employ communications security measures. An intruder, represented by a computer under hostile control, is assumed to be situated in the communications path between the host and the terminal. Thus all messages transmitted on the connection must pass through the intruder. In many respects, connection-oriented measures provide the greatest degree of communications security and they are applicable in a wide variety of environments.

Although both link-criented and connection-oriented security measures have advantages and disadvantages peculiar to themselves, connection-oriented security measures generally afford greater overall protection in a wide range of environments and are more naturally suited to a user's perceptions of his or her own security requirements. This stems from the fact that connection-oriented measures rely on the security of equipment only at the source and destination of a connection, while link-oriented measures may require that each node in the communication subnet be secure. However, there are situations where both types of measures can be useful and can be employed to provide an economic level of protection that is higher than which could be achieved using either class of measure alone.

B. Attack Classifications

We can classify types of attacks that might be mounted by an intruder. If an intruder can position himself at some point in the network through which information must pass he or she will be able to conduct both active and passive attacks. For example, in an internetwork environment, the intruder could take the form of a gateway in some intermediate network that provides the only communication path between two processes that are at the ends of the connection of interest.

1. Passive Attacks

In passive wiretapping, the intruder merely observes messages passing on a connection without interfering with their flow. Intruder observation of the data in a message can be termed "release of message contents", and is the most fundamental type of passive wiretapping[43]. The intruder can also observe portions of the message headers, even if the application-level data are not intelligible to him, to learn the location and identities of the communicating processes. Finally, the intruder can examine the lengths of messages and their frequency of transmission to gain knowledge of the nature of the data being exchanged. These latter types of passive wiretapping attacks are usually referred to as "traffic analysis" or "violations of transmission security"[44]. Although traffic analysis is usually viewed as a means of inferring information by observing legitimate message traffic, this form of attack can also be used in conjunction with a Trojan Horse program operating in a user process at a service host. The Trojan Horse program could perform some legitimate function within the process while clandestinely modulating message destination, length, or frequency of transmission in order to use the connection as a covert channel for transmitting to the intruder, data legitimately accessible by the process. In an interactive communication environment, if the bandwidth of the communication network is high relative to the speed of user terminal equipment, modulation of message length and frequency could by carried out by a Trojan Horse program and still be completely undetected by a user[45].

2. Active Attacks

The intruder can also engage in "active wiretapping", performing a variety of processing on messages passing on the connection. These messages can be selectively modified, deleted, delayed, reordered, duplicated, and inserted into the connection at a later point in time, or may pass through unaffected. He can also synthesize bogus messages and insert them into the connection. Acts such as these can be designated "message stream modification attacks"[46]. Since it is assumed that the intruder can be positioned so that all messages of interest flow through his location, the intruder can discard all messages or, in a less drastic action, can delay all messages going in either or both directions on a connection. Acts of this nature can be classified as "denial of message service attacks"[47]. Depending on the communication medium employed, measures can be used that make it extremely difficult for an intruder to severely disrupt communications. Such tamper free techniques are of interest in any environment where disruption of communications is a problem. In the context of message deletion or delay, the difference between message stream modification and denial of message service attacks is subtle, and is a function both of the degree of the attack and the state of the connection. The distinction is made because different types of countermeasures can be employed for each type of attack. Finally, connections must be initiated in a fashion that supports secure identification of the hosts, terminals, and users at each end, and verifies the time integrity of the connection. Attempts by an intruder to violate time-integrity or secure identification constraints can be classified as "spurious connection initiation" attacks[48]. Such attacks are similar in nature to message stream modification attacks, but the context of connection initiation suggests the use of a somewhat different set of countermeasures.

C. Trusted Hosts

A computer system which has been approved as meeting a specified level of security protection, together with any other parts of the system which are known to be secure, is termed a trusted computer base or TCB. Computers and operating systems which may be considered to be a TCB, together with their applications software, must meet the appropriate security criteria specified in the Orange book, "Trusted Computer System Evaluation Criteria" (TSEC), published by the National Computer Security Council (NCSC). The Orange book specifies three levels of protection, A,B and C (in decreasing order of protection) and within each division numbers are given to classify the categories of security protection and assurance. For example, the highest level of protection and assurance achieved is A1, A indicating verified protection and A1 indicating a verified design, while A2 indicates verified implementation which is beyond the present state-of-the-art. Systems in class A1 are functionally equivalent to those in class B3 but formal design specification and verification techniques are applied. Class B3 systems possess security domains which mediate all accesses of subjects and objects, are tamperproof, and exclude code which is not essential to the security capability. Class B2 (structured protection) systems are based on a clearly defined and documented formal security policy model. It enforces discretionary and mandatory access control enforcement, as found in class B1, but is extended to cover all subjects and objects in the system, including strengthened authentication mechanisms. Class B1 (labelled security protection) systems have all the features of class C2 systems, but include an informal statement on the security policy modes, data labelling and mandatory access control over named subjects and objects[49]. The selection of the appropriate level of security for a system depends upon the local processing capability, communication path, data exposure, as well as the capability of the user.

The use of a trusted computer base is extremely expensive and costs many times more to achieve an A1 system than a C1 system. The Orange book provides a range of security protection from low assurance and low functionality up to high assurance and high functionality, but the need for systems with, for example, low functionality and high assurance or high functionality and low assurance, are not considered.

D. Trusted Networks

Wide area networks are a potentially insecure means of communication and a range of countermeasures are available to combat the threat. Local area networks (LANS) are, however, often considered to be less vulnerable because they are generally located on territory owned or under the control of the user. LANS do, however, possess many of the vulnerabilities found in wide area networks, as well as those vulnerabilities associated with a stand alone-computer system. In particular, most LANs use a broadcast mode of transmission which makes all data available to all devices connected to the LAN[50]. Additionally, the same communication medium may be used for different applications with different security requirements. Another significant problem is that

LANs are frequently connected by gateways to wide area networks, thus making the data remotely accessible.

A trusted network is an extension of the trusted computer base where the transmission of information on the network is considered secure, and each access point includes a trusted network interface unit (TNIU) which prevents users from gaining access to information which they are not authorized to receive[51]. A trusted network provides a service to the trusted computer base by guaranteeing authentication, mutual secrecy, and message delivery. The TNIU must contain only trusted computing facilities and software, and may use encryption to provide protection for data transmitted on the network, but physical security measures may alternatively be used to protect data on the network, possibly at a lower cost.

An alternative approach to network security is to employ a Secure Terminal Interface Unit (STIU) between the user and the LAN interface unit. A Secure Host Interface Unit (SHIU) is also required between the trusted host and the LAN. Both of these units include equipment which encrypts only the data, not the network control information. Communication between the host computer and the user is achieved by the user establishing a connection with encrypted address codes, and then the host computer authenticating the identity of the user through password validation and checking on the user's access rights[52]. This approach is more complex than a trusted network with TNIUs, but it may be implemented with any LAN.

A trusted network prevents any communication which is not authorized by the network. This is achieved by using a Secure Authentication Server (SAS) as part of the network. The SAS gives each TNIU permission tokens for each session appropriate to the user's rights and needs. The SAS will also maintain a security file which stores passwords. A user on a trusted network initiates authentication directly with the TNIU, and the TNIU communicates with the SAS to get the authentication for the user confirmed. When this is confirmed by the SAS, the TNIU instructs the user to proceed. The user then has to be authenticated to the host computer using a password and a unique identifier from the TNIU. The SAS checks that the two identifiers match and that the user is authorized to access the host computer. When the check is complete, the SAS informs the TNIU that the user can proceed. The user must then enter the names of the devices with which communication is desired in the session, and the SAS checks the user's authority to communicate as requested. If the user is authorized, the SAS will arrange for the connections and inform the TNIU to permit these other connections during the session[53].

E. Summary

When evaluating networks there are two ways to consider communications security. Link-level connections protect messages on each of the communication links. End-to-end level security measures provides continuous protection for each message from its source to its destination. What makes networking systems more vulnerable than stand-alone systems, is the ability to exploit the communication medium that interfaces different networking resources. The exploitation of these weaknesses can be either passive or active, depending on the capabilities or opportunities of the intruder. The use of trusted hosts and trusted networks helps maintain the integrity of link-level and end-to-end systems.

VII. ENCRYPTION

A. Introduction

Of all the topics concerning networking security perhaps the most complicated is the process of encryption. There are hundreds of algorithms used for encryption and the complex topic of encryption by itself is beyond the scope of this thesis. Only a brief description is presented here.

Encryption is the process of changing a message called plaintext to ciphertext, and is based on the concept of a cipher. A cipher is an algorithmic transformation performed on a symbol-by-symbol basis on any data. For the purposes of electronic data transmission, such as that used in networking communications, a cipher is a one to one representation of a message. The original plaintext may be used directly in the computation, or it may be viewed as a binary stream superimposed upon an enciphering stream.

B. Ciphers

There are four basic types of ciphers[54]. A *substitution or stream cipher* substitutes a letter or number for each character being enciphered. A *transposition or permutation cipher* (often called a block cipher), uses letters or numbers of text and scrambles them in some predetermined pattern. A *combination cipher* uses substitution and transposition intermixed to convert the message to ciphertext.

Product cipher encryption combines the operations of permutation and substitution. When formed correctly every bit of the cipher will depend on every bit of the plaintext and every bit of the key. A product cipher may be constructed by using the permutation and substitution operations in an iterative manner. If the result of this pair of operations is reentered into the same process, the cipher that is produced is called a recirculating block product cipher. A complex algorithm that is easy to implement may be based on a recirculating block product cipher.

1. Block and Stream Ciphers

Another form of classification for cipher techniques are the terms "block ciphers" and "stream ciphers". Block ciphers transform a block of characters together, making each encrypted output block a functional combination of the complete key and the input block. In this type of encryption the blocks of plaintext bits are transformed into blocks of cipher bits simultaneously. In general the blocks are the same size. If the cipher block is smaller than the plaintext block then information is lost unless an appropriate data compression method is used in conjunction with the encryption algorithm[55]. If the cipher block is bigger, utilization of the data transmission path is reduced. A stream cipher makes each bit of encrypted data a function of only one bit of the original plaintext and one bit of the key. A stream cipher causes only the plaintext bits, which correspond to bits of ciphertext that are corrupted in transmission, to be lost. With a block cipher, the entire plaintext block is lost if any part of the ciphertext block becomes corrupted. Both forms of cipher lose the rest of the message or text block if a whole character is lost or added, causing the synchronization between the key streams at the transmitter and receiver to be lost.

2. Private Key Ciphers

Conventional private key ciphers use the same key to decipher the message as well as to encipher it. Anyone in possession of the key and a decryption unit which implements the correct algorithm can decipher the message. Private key systems provide a two-way channel to their users. If two users A and B share a secret key, they can both encrypt information that they are sending to each other as well as decrypt information sent from the other. The best example of a private key system is the Data Encryption Standard or DES algorithm. DES was developed by the US National Bureau of Standards in conjunction with IBM and is used by the general public. It is the only encryption standard which is widely used in industry. The cryptographic strength of the DES algorithm is the number of possible combinations that must be utilized to break the cipher. If you had a 56-bit key the number of possible combinations of bits which could produce a key is 2^{56} or 7.2 * 10^{16}. With an example of ciphertext and the corresponding plaintext available, a computer would be required to try up to 2^{56} different keys by trial an error to discover the true key[56]. The time and expense required to break a DES key is considered to exceed the value of any information transmitted, however, advances in computer technology have made this assumption questionable.

There are several disadvantages with private key systems. If the key is compromised the intruders can immediately decrypt all encrypted information and can also produce bogus messages. For this reason, cipher keys are changed frequently so that a compromised key will reveal only a limited amount of information[57]. This poses an additional problem since the keys in many cases must be distributed by hand or by courier. This makes them vulnerable to exploitation. One approach to this problem is to distribute the keys in pieces under separate channels, so that any compromise of a part of the key will not compromise the entire key. An associated problem is the number of keys that must be maintained, since the number of keys required increases with the square of the number of users. This compounds the problem of key distribution and makes adding new users to the system impractical in many situations. The magnitude of this problem is usually contained by having only a few people exchange secrets so that the network of interchanges is relatively small.

3. Public Key Ciphers

A public key cipher uses different keys to encipher and decipher the message. Pairs of keys are used, and these define a pair of transformation algorithms, each the inverse of the other, and one may not be derived from the other[58]. All users possess a pair of keys, one of which is publicly known and is used to encipher messages for that user, while the second key is kept secret for use in deciphering messages sent to the user. If user A wishes to send a message to user B, the message is encrypted using the public key of user B, and the private key of user A. Since it is impossible for anyone else to reproduce this combination of keys, except users A and B, the message is unforgeable and cannot be altered. User B can decrypt the message using the public key of user A, and the private key of user B. This insures that the message is authentic and provides a digital signature, since only user A could have sent the message.

Public key cryptosystems are based on one-way functions which are computationally infeasible in the reverse direction. If a solution to the reverse computation were found, the cryptosystem would be compromised. The major advantage of public key cryptosystems is that only public keys are distributed to potential information sources; whereas, conventional ciphers require the highly sensitive keys to be distributed, therefore increasing the risk of being compromised as well as requiring frequent key changes[59]. The disadvantage of public key cryptosystems is that they are slow and that the integrity of the public key directory must be maintained.

The best example of a public key system is the RSA public key encryption scheme developed at the Massachusetts Institute of Technology by Rivest, Shamir and Adleman, from whose names the title was derived. It is the most widely used public key cryptosystem suitable for applications in electronic mail, where a signature may be verified by consulting a directory of public keys, and in data communications for privacy and authentication[60]. The RSA algorithm is based on the underlying hard problem of factoring large numbers. The high processing requirement for public key cryptosystems has restricted their commercial use to a few banking applications; however, they are extensively used by the government. RSA uses large data blocks, typically 512 bits, and encryption requires the equivalent of three million sixteen-bit multiplications per block. Software implementations require about 45 seconds to process a 512-bit block on an IBM PC while hardware implementations take at least 0.1 seconds[61]. With these long processing times, RSA is not attractive for many high-speed data communication requirements. The RSA keys are 200-bit words. The encryption key is the product of two secret prime numbers, each about 100 bits, and the decryption key may also be computed from the two prime numbers. To derive the secret prime numbers, the key may be factored, but this would take 3.8 billion years for a 200-bit key, assuming one operation per microsecond[62]. A plaintext message is first converted into a data block up to 512 bits in length. Encryption of a plain text block, using the encryption key, produces a cipher text block of the same size. Decryption is the reverse of the encryption process but using the decryption key.

C. Encryption Techniques

Encryption is primarily a countermeasure against passive attacks to prevent the disclosure of data, but can also be used as the basis of countermeasures against active attacks in order to prevent the modification of data. Encryption may be implemented on each data transmission link without regard for message content, or as end-to-end encryption, applied at the user level before data enters the network and decrypted at the destination. End-to-end encryption makes it necessary to put information such as headers, which are required by the network, in plaintext.

1. Link Encryption

Link encryption can be performed independently on each of the different communication links in a network. Usually, a different key is employed for each link so that subversion of one link does not necessarily result in release of information transmitted on other links. Stream ciphers are generally employed in link encryption, and a continuous stream of ciphertext bits is maintained between nodes. Because switching functions are performed only at nodes in a network, both the headers and the data of packets used can be enciphered on links. Since many of the links in the network are multiplexed, no segregation of connections on links is enforced. Since information is enciphered only on the links and not within the nodes connected by links, these nodes must be secure. Although the origin and destination nodes in the network are assumed to be physically secure, link encryption requires the extension of this physical security to all intermediate nodes as well. Not only must these intermediate nodes be physically secure, but also the hardware and software components of these nodes must be certified to isolate the information on each of the connections passing through it[63].

2. End-to-End Encryption

In end-to-end encryption each message is enciphered at its source and not deciphered until it reaches its destination. A unique key can be used for each connection or a different key can be used between each pair of communicating hosts, or a single key can be used over an entire secure subnet. These schemes afford end-to-end protection but do not provide the connection segregation of link encryption. In accordance with the principle of least privilege or need to know, messages should be enciphered so that each module that processes a message, has available to it, only the information necessary in performing its task. The information in a message can be categorized based on whether the information must be accessible to gateways, hosts, or processes at the end of the connection. Gateways must access header fields, indicating the destination network, as well as any fields associated with internet services[64]. The gateway into the destination network must also be able to access the address of the destination host. The information in the message can be enciphered under a key used only for that connection. The encryption can be achieved either by selective encipherment of appropriate information fields or by embedding the information from each level in a protocol layer for the next level and performing encryption on the layered message at each level[65]. In practice variations on these techniques are employed, using some aspects of selective encryption and protocol layering.

D. Summary

Encryption in computers and networks is an extensive and complex topic. Understanding the basics of encryption allows for the utilization of varying techniques to help maintain a secure communications network. Encryption is the process of changing a message called plaintext to ciphertext and is based on the concept of a cipher. Conventional private key ciphers use the same key to decipher the message as used to encipher it. A public key cipher uses different keys to encipher and decipher the message. Link encryption encrypts data at each individual link in the transmission path of the message. End-to-end encryption enciphers each message at its source and deciphers it at its destination.

VIII. DETECTION AND PREVENTION

A. Introduction

In order for any network security policy to be effective there must be a way to detect potential intruders, and a means of preventing their access to the resources of the network. A capability must exist to monitor security compliance and respond to incidents involving violations of security. An ongoing monitoring and enforcement program assures continued effectiveness of information protection measures. Early monitoring and detection of potential abusers greatly facilitate the ability to maintain a safe and secure network.

B. Prevention and Detection

We can establish five goals for the design of mechanisms that provide for communications security in a network:[66]

1. Prevention of release of message contents.
2. Prevention of traffic analysis.
3. Detection of message stream modification.
4. Detection of denial of message service.
5. Detection of spurious connection initiation.

1. Prevention of Release of Message Contents

The primary means of preventing the release of message contents is by the use of encryption. Both link and end-to-end encryption techniques can be employed.

2. Prevention of Traffic Analysis

Traffic analysis countermeasures center around masking the frequency, length, and origin-destination patterns of message traffic. The precision with which an intruder can carry out such pattern analysis directly influences the amount of information that can be gained from the analysis. This precision is a function of several factors, including the protocols employed in the network, transmission medium of the communication subnet, and operating characteristics of the hosts[67]. For example, analysis can take place at several levels in the network environment, enabling an intruder to determine the origin and destination of the messages. The difficulty associated with countering attacks at each level depends heavily on the specific protocol being used and on the network environment.

3. Detection of Message Stream Modification

To achieve the third goal, detection of message stream modification, mechanisms must be employed to determine message authenticity, integrity, and ordering. Authenticity implies that the source of a message can be reliably determined. Integrity implies that a message has not been modified enroute, and ordering implies that a message can be properly located in the stream of information being transmitted from the source to the destination. Although these functions are usually provided by a communication protocol for reliability purposes, they must be provided in the face of attacks by an intruder, as opposed to failures by components. Message authenticity and ordering requirements, combined with a secure connection, require the use of distinct encryption keys for each connection. More important, the protocol data that provide the basis for authentication and ordering must be bound to application data in a fashion that precludes undetected modification of any portion of the resulting message[68].

4. Detection of Denial of Message Service

The fourth protection goal, detection of denial of message service, can be achieved through the use of a request-response protocol[69]. Such a protocol, built on top of message authentication and ordering, involves the exchange of a pair of messages that establish the time integrity and status of the connection. At each end of the connection a timer is used to periodically trigger the transmission of a request message that forces a response from the other end of the connection. Each of these messages conveys the status of its transmitter in terms that permit detection of any messages missing f' om the connection. An explicit request-response protocol can be provided by defining a pair of end-to-end control messages containing both a sequence number and an acknowledgement field along with an error-detection code[70]. Many applications provide implicit checking for denial of message service attacks because of the command response nature of the application. General purpose protocols for interactive and other types of applications cannot rely on such application dependent characteristics.

5. Detection of Spurious Connection Initiation

Countermeasures for accomplishing the fifth goal, detection of spurious connection initiation, are designed to provide a secure basis for verifying the identities of the users at each end of the connection, and verifying the time integrity of the connection. Verification of the time integrity of the connection protects against "playback" attacks in which an intruder uses a recording of a previous legitimate connection to mislead or confuse a user, or cause a service host process to perform redundant activities, possibly resulting in errors. Mechanisms for verifying the time integrity of the connection initiation procedure should not require human intervention, so as not to restrict their applicability, and to avoid dependence on and inconvenience to users. Verification of identities of users at ends of the connection during the connection initiation procedure provides the basis on which the authenticity of subsequent message traffic is founded. Maintenance of this association between the users identified during connection initiation involves appropriate key distribution techniques and other measures[71].

C. Audit Trails

One of the most effective means of detecting and preventing unauthorized access to networking resources is to establish effective audit mechanisms[72]. Audit trails are used to detect and deter penetration of a computer or network system and may be limited to specific events, or may encompass all of the activities on a system. The audit mechanism has four important security goals[73]. First, the mechanism must allow access to individual objects to be reviewed and access histories of specific processes and individuals. Second, the mechanism must allow discovery of repeated attempts to bypass the protection mechanisms. Third, the mechanism must allow discovery of any use of privileges that may occur when a user assumes a functionality with privileges greater than his or her own. Fourth, the mechanism must act as a deterrent against perpetrators' habitual attempts to bypass the system protection mechanisms, even if the attempt to bypass the protection mechanism is successful[74]. The techniques for implementing the audit requirements will vary from system to system depending upon the characteristics of the software and hardware involved.

D. Summary

An effective prevention and detection mechanism is important in implementing a network security program. The incorporation of audit trail mechanisms is just one aspect of an effective monitoring program. A positive benefit of a monitoring and enforcement process is an increased understanding of the degree of information related risk in network operations. Only in this way can potential intruders be denied access to a network, or if penetration is realized, to detect the intruders and identify the weak links in the network computer system.

IX. CONCLUSIONS AND RECOMMENDATIONS

A. Conclusions

Network security is a diverse and dynamic subject that encompasses not only conventional computer security issues but the added difficulties associated with networks. As such, the problem of maintaining security in networks is a much more difficult one. Every host and network manager must be aware that the DDN as presently constituted is not secure. Recent events have made all concerned with the DDN much more sensitive to the issue of security.

Access control measures, physical security, procedural and personnel security controls, are some of the more apparent problems that can be addressed in maintaining security. The medium used to interconnect computer communications systems represents an additional security dimension that significantly increases the vulnerability of computing resources. The use of encryption in networks, both end-to-end and link-level, is fundamental in addressing network communications security. The problems of network security are applicable not only to the DDN and its large infrastructure, but to any networking or Internet environment where there is a concern against unauthorized access. The success of a network protection program depends on the policy generated, and on the attitude of management toward security and security related issues. The administrator sets the tone and the emphasis on how important a role network security will have within the organization. The primary responsibility of management is to set the network security policy with the objectives of reduced risk, compliance with laws and regulations, assurance of operational continuity, information integrity, and confidentiality. This can most easily be accomplished with a comprehensive security plan. This chapter proposes a set of recommendations that will help network administrators identify potential problems and to take steps to alleviate them.

B. Recommendations

There are several things network managers can due to ensure that security and integrity are maintained in a network. One must take in to consideration that the implementation of any comprehensive security plan is not without costs or trade-offs. The value of the information to be protected, and the degree to which systems administrators are willing to define and implement policy, are a major factor in security of networks. By following the recommendations presented in this thesis, the network administrator can identify and evaluate the potential vulnerabilities of a network, and implement an effective security policy. The bottom line to remember is that the network as a whole is only as secure as its weakest link. Adequate security controls must be in place to protect the network.

1. Security Plan

A security plan will require the staff, funding and positive incentives to personnel to participate in a program to protect the organizations assets. The administrator should state precisely[75], the value to the organization of data and information resources, and the need to preserve their integrity, availability, and confidentiality. The intent of the organization to protect the resources from accidental or deliberate unauthorized disclosure, modification, or destruction, must be identified. There must be responsibility for data security throughout the organization and personnel should be held personally accountable for information resources entrusted to them. Computer security and awareness training should be administered to all personnel having access to information resources. Finally, there needs to be a requirement to monitor and assess data security via internal and external audit procedures.

2. Reduce Risk to an Acceptable Level

The dollars spent for security measures to control or contain losses should never be more than the projected dollar loss if something adverse happened to the information resource. Cost effective security results when reduction in risk is balanced with the cost of implementing safeguards. The greater the value of information processed, or the more severe the consequences if something happens to it, the greater the need for control measures to protect it. It is important that these trade-offs of cost versus risk be explicitly considered, and that management understands the degree of risk remaining after selected controls are implemented.

3. Assure Operational Continuity

With ever increasing demands for timely information and greater volumes of information being processed, availability of essential systems, networks, and data is a major protection issue. In some cases, service disruptions of just a few hours are unacceptable. Agency reliance on essential computer systems requires that advance planning be done to allow timely restoration of processing capabilities in the event of severe service disruption[76]. The impact due to an inability to process data should be assessed, and action taken to assure availability of those systems considered essential to agency operation.

4. Comply with Federal Laws and Regulations

As the pervasiveness of computer systems increases and the risks and vulnerabilities associated with information systems become better understood, thε body of law and regulations governing positive action to protect information resources grows. The "Rainbow" series of documents published in accordance with DOD directive 5215.1, "Computer Security Evaluation Center", provide a baseline for an information resources security program.

5. Assure Integrity and Confidentiality

An important objective of a network resource management program is to ensure that the information accessed via the network is accurate. Integrity of information means you can trust the data and the processes that manipulate it. A system has integrity when it provides sufficient accuracy and completeness to meet the needs of the users. It should be prcperly designed to automate all functional requirements, include appropriate accounting and integrity controls, and accommodate the full range of potential conditions that might be encountered in its operation[77]. A network should also be protected from intruders, as well as from personnel with authorized computer access privileges who attempt to perform unauthorized actions. Assured confidentiality of sensitive data is often, but not always, a requirement of network computer systems. Privacy requirements for personal information are generally dictated by directive while protection requirements for other agency information are a function of the nature of that information. Determination of requirements in the latter case is made by the official responsible for that information. The impact of wrongful disclosure should be considered in understanding confidentiality requirements.

6. Accountability for Information

An effective information resource protection program identifies the information used by the agency and assigns primary responsibility for information protection to the managers of the respective functional areas supported by the data. These managers know the importance of the data to the organization and are able to quantify the consequences of undesirable events. They are also able to detect deficiencies in data and know definitively who must have access to the data supporting their operations. A fundamental networking security issue is assignment of accountability. Information flows throughout the organization and can be shared by many individuals. This tends to blur accountability and disperse decision making regarding information protection. Accountability should be explicitly assigned for determining and monitoring security for appropriate agency information. When security violations occur, management must be accountable for responding and investigating. Security violations should trigger a reevaluation of access authorizations, protection decisions, and control techniques. All apparent violations should be resolved since absolute protection will never be achieved and some losses are inevitable. It is important, however, that the degree of risk assumed be commensurate with the sensitivity or importance of the information resource to be protected.

7. Vulnerability Assessment

A risk assessment program ensures management that periodic reviews of information resources have considered the degree of vulnerability to threats causing destruction, modification, disclosure, and delay of information availability, in making protection decisions and investments in safeguards. The official responsible for a specific information resource determines protection requirements. Less sensitive information will require minimal safeguards, while highly sensitive or critical information will require strict protective measures. Assessment of vulnerability is essential in specifying cost-effective safeguards. Overprotection can be needlessly costly and add unacceptable operational overhead. Once cost-effective safeguards are selected, residual risk remains and is accepted by management. Risk status should be periodically reexamined to identify new threats, vulnerabilities, or other changes that affect the degree of risk that management has previously accepted. Appendixes B through E provide checklists for a vulnerability assessment.

8. Data Access

Access to information should be delegated according to the principles of need-to-know and least possible privilege. For a multi-user application system, only individuals with authorized need to view or use data are granted access authority, and they are allowed only the minimum privileges needed to carry out their duties. For personal computers with one operator, data should be protected from unauthorized viewing or use. In networking environments the principles of need-to-know are much more difficult to implement. It is ultimately the administrators and the individual's responsibility to ensure that the data is secure and to know the vulnerabilities of data to possible exploitation.

9. Degree of Centralization

The desirability of centralized versus decentralized security is heavily debated and largely depends on size, organizational structure, and management approach at an individual agency[78]. A centralized approach to security has the advantages of being directly responsive to executive direction and specifically accountable for progress and status. A decentralized approach to security has the advantages of being close to the local network administrator. In the long term, decentralization may provide better integration of security with other entity functions. A small dedicated resource at the local level can direct the information protection program, while additional resources are utilized to maintain the integrity of the network as a whole.

10. Implementation Stages

Development of a comprehensive information protection program that is practiced and observed widely throughout a network usually occurs in stages and requires ongoing monitoring and maintenance to remain viable. First, organizational requirements for information protection are identified. Different agencies have varying levels of need for security, and the information protection program should be structured to most effectively meet those needs. Next, organizational policies are developed that provides a security architecture for agency operations. The policies undergo normal review procedures, then are approved by agency management for implementation. Activities are then initiated to bring the agency into compliance with the policies. Depending on the degree of centralization, this might require development of further plans and budgets within the agency to implement the necessary logical and physical controls.

11. Hardware and Software Configuration Controls

Protection of hardware and resources of computer systems and networks greatly contributes to the overall level of control and protection of information in the DDN. Network protection policies should provide substantial direction concerning the management and control of computer hardware and software. Agency information should be protected from the potentially destructive impact of unauthorized hardware and software. For example, software viruses inserted into computers through games and other apparently useful software, acquired via public access bulletin boards, have spread from system to system before being detected. Also, unauthorized hardware additions to personal computers can introduce unknown dial-in access paths. Accurate records of hardware and software inventory, configurations, and locations should be maintained, and control mechanisms should provide assurance that unauthorized changes have not occurred. To avoid legal liability, no unauthorized copying of software should be permitted. Agencies should also address the issue of personal use of federal computer systems, giving personnel specific direction about allowable use and providing consistent enforcement.

12. Operational Controls

Agency standards should clearly communicate minimum expected controls to be present in all computer facilities, computer operations, input/output handling, network management, technical support, and user liaison. More stringent controls would apply to those areas that process very sensitive or critical information. Protection of these areas would include:

1. Security management.
2. Physical security.
3. Security of system/application software and data.
4. Network security.
5. Contingency planning.

13. Dedicated Staff

The common practice of assigning responsibility for information security to existing staff with other major responsibilities is often unsuccessful. At least one dedicated staff member is recommended at the program management level. The need for additional full-time resources depends on the organizations computer environment. The number of information systems, their technical complexity, the degree of networking, the importance of information processed, and extent of the organization's dependence on information systems, affect the resources needed.

14. Training

Training should be a major activity in any network security environment. Security violations are the result of human action, and problems can usually be identified in their earliest stages by people. Developing and maintaining personnel awareness of information security issues can yield large benefits in early detection and prevention of problems. Target audiences for this training are executives and policy makers, program and functional managers, security and audit personnel, computer management and operations, and end users. Training can be delivered through existing policy and procedures manuals, written materials, presentations and classes, and audio-visual training programs. The training provided should create an awareness of risk and the importance of safeguards, underscoring the specific responsibilities of each of the individuals being trained.

C. Summary

Successful utilization of the DDN requires establishing agency policies and practices regarding information protection. The security policy directive facilitates consistent protection of information resources. Supporting procedures are most effectively implemented with top management support, through a program focused on areas of highest risk. A compliance assessment process ensures ongoing effectiveness of the information protection program throughout the network.

Security is subjective, what one site might view as an idle curiosity another would see as a hostile probe. The existence of the DDN depends on its usefulness to all those who use it. Network managers must be willing to accept and act on other sites' security issues. The issue of security in the DDN is a cooperative adventure requiring the participation of all.

APPENDIX A - PASSWORD SELECTION GUIDELINES

1. Do not use your login name in any form as a password.

2. Do not use your first or last name in any form.

3. Do not use your spouse or child's name in any form.

4. Do not use any information easily obtained about you. This includes license plate numbers, social security numbers, telephone numbers and other information.

5. Do not use a password of all digits, or all the same letter. This significantly reduces the search time for an intruder.

6. Do not use a word contained in dictionaries, spelling lists, or other lists of words.

7. Do not use a password shorter than six characters.

8. Do use a password with mixed case alphabetic.

9. Do use a password with nonalphabetic characters, such as digits or punctuation.

10. Do use a password that is easy to remember so you do not have to write it down.

11. Do not use the same password for more than one year. (six months is probably optimal).

APPENDIX B - RISK ANALYSIS (PERSONNEL)

1. Are formal reports required for each reported instance of computer penetration?

2. Are records maintained on the most common methods of computer penetration?

3. Are records maintained on damage caused to computer equipment and facilities?

4. Is one individual held accountable for each data processing resource?

5. Does management understand threats posed by host connection to the DDN?

6. Is management evaluated on its ability to maintain a secure computer facility?

7. Are the activities of any non-employees in the computer center monitored? Is an escort policy enforced?

8. Are contractor personnel subject to the same security procedures as other non-employees?

9. Are procedures installed to restrict personnel without a "need to know"?

10. Have procedures been established to limit the damage, corruption, or destruction of data base information?

11. Has a security incident report form been created?

APPENDIX C - RISK ANALYSIS (OPERATIONS MANAGEMENT)

1. Has a systems security officer been appointed?

2. Have procedures been developed defining who can access the computer facility, and how and when that access can occur?

3. Have procedures been established to provide physical protection of local and remote terminal access equipment?

4. Have procedures been established to provide physical protection of host computers?

5. Is someone designated as a terminal area security officer?

6. Have procedures been established to positively identify transactions occurring to and from remote locations?

7. Have security procedures been established for the microcomputers which will communicate with the DDN?

8. Have procedures been established for providing physical security over these microcomputers and the data processed by them?

9. Have procedures been established to protect data within the custody of the microcomputer user?

10. Have alternate means of processing been established in the event either the individual or the personal computer is lost?

11. Is the security over the microcomputer environment regularly reviewed?

12. Have the vendor installed passwords been changed?

13. Does someone verify that all current passwords are different from a list of commonly used or vendor installed passwords?

14. Has a backup policy been defined? Is this policy strictly enforced?

APPENDIX D - RISK ANALYSIS (COMMUNICATIONS)

1. Is sensitive information transmitted over common carrier lines protected?

2. Can data being transmitted or processed be reconstructed in the event either main processing or remote processing loses integrity?

3. Are processing actions restricted based on the point of origin or the individual making the request?

4. Have procedures been established for providing host connection access control over remote terminals and on-site terminals?

5. Is a log maintained of accesses to computer resources?

6. Do non-employees have access to communications facilities?

APPENDIX E - RISK ANALYSIS (DISASTERS)

1. Have the types of potential disasters been identified?

2. Has equipment been provided to deal with minor disasters, such as fire and water damage?

3. Have alternate processing arrangements been made in the event of a disaster?

4. Have procedures been established to provide backup of automatic data processing capabilities in event of loss of primary ADP resources?

5. Have simulated disasters been conducted to ensure that disaster procedures work?

6. Are critical programs and data retained in off-site storage locations?

7. Have users been heavily involved in developing disaster plans for applications that affect their areas?

LIST OF REFERENCES

1. DDN New Users Guide, Varallo Barbara, September 1991, p.7.
2. Protocols and Techniques for Data Communication Networks, Kuo Franklin ,1981 Prentice Hall.
3. Ibid
4. Ibid
5. Internetworking with TCP/IP, Comer Douglas,1991,Prentice Hall.
6. DDN New Users Guide, Varallo Barbara, September 1991, p.7.
7. Security in Computing, Pfleger Charles P.,1989. Prentice Hall.
8. Ibid
9. Ibid
10. Ibid
11. Internetworking with TCP/IP, Comer Douglas,1991,Prentice Hall.
12. Ibid
13. Ibid
14. DDN Security Management Procedures for Host Administrators,DCA Circular,1992,p.2.
15. Ibid
16. Ibid
17. Ibid
18. Ibid
19. Security in Computing, Pfleger Charles P.,1989. Prentice Hall.
20. The Internet Worm Incident, Spafford Eugene H.,1991,Purdue University, p.3.
21. DDN Security Management Procedures for Host Administrators, DCA Circular,1992,p.10.
22. Ibid
23. Ibid
24. Ibid
25. Ibid
26. Protocols and Techniques for Data Communication Networks, Kuo Franklin,1981 Prentice Hall.
27. Improving the Security of Your UNIX System,Curry David A.,1990,SRI International.
28. Ibid
29. Ibid
30. Ibid
31. Practical Applications of Data Communications, Meissner Paul,1980, McGraw Hill.
32. Ibid
33. Ibid
34. Ibid

35. Ibid
36. Local Networks, Stallings William, 1984, Macmillan.
37. Ibid
38. Security in Computer Networks,Kent Stephen T.,1981, Prentice Hall.
39. Ibid
40. Ibid
41. Ibid
42. Ibid
43. Ibid
44. Ibid
45. Ibid
46. Ibid
47. Trusted Computer System Evaluation Criteria, DoD,Dec 1985
48. Security in Computers and Communications Systems, Freer John R.,1988, Plenum Press, NY.
49. Ibid
50. Ibid
51. Ibid
52. Computer Networks,Winkler Stanley,1978,Computer Science Publications, NY.
53. Ibid
54. Security in Computers and Communications Systems, Freer John R.,1988, Plenum Press, NY.
55. Security in Computing, Pfleger Charles P.,1989. Prentice Hall.
56. Security in Computers and Communications Systems, Freer John R.,1988, Plenum Press, NY.
57. Ibid
58. Ibid
59. Ibid
60. Ibid
61. Security in Higher Level Protocols,Voydock Victor L.,1981, National Bureau of Standards.
62. Protocols and Techniques for Data Communication Networks, Kuo Franklin ,1981 Prentice Hall.
63. Ibid
64. Ibid
65. Ibid
66. Ibid
67. Ibid
68. Ibid
69. Ibid
70. Audit in Trusted Systems,National Computer Security Center,1988,DoD.
71. Ibid
72. Executive Guide for the Protection of Information Resources, National Institute of Standards and Technology,1991.
73. Ibid
74. Ibid

75. Ibid
76. Ibid
77. Ibid
78. Ibid

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   Cameron Station
   Alexandria, VA 22304-6145

2. Library,Code 52 2
   Naval Postgraduate School
   Monterey, CA 93943-5002

3. ATTN: Professor T. Bui 1
   Code AS/BD
   Naval Postgraduate School
   Monterey, CA 93943-5002

4. ATTN: Professor R. Stemp 1
   Code OR/ST
   Naval Postgraduate School
   Monterey, CA 93943-5002