Document Number 102-94-002U

4

Technical Report

Naval Security Standards and Applications Analysis

Task 2
Contract No. N00039-93-C-0099
CDRL No. A003

February 14, 1994

Prepared for:

Space and Naval Warfare Systems Command
Information Systems Security Office (SPAWAR OOI)
Mr. Tim McChesney, SPAWAR PMW 151T / Mr. Robert Patton, SPAWAR OOI-E2
Washington D.C. 20363-5100

and

Department of the Navy
Naval Command, Control and Ocean Surveillance Center
Mr. John Campbell / Mr. Jim Weatherford, Code 412
RDT&E Division, San Diego, CA 92152-5000

Prepared by:

Secure Solutions, Inc.
9404 Genesee Avenue, Suite 237
La Jolla, CA 92037
(619) 546-8616

DISTRIBUTION STATEMENT: Approved for public release; distribution is unlimited.

Document Number 102-94-002U

Technical Report

Naval Security Standards and Applications Analysis

Task 2
Contract No. N00039-93-C-0099
CDRL No. A003

February 14, 1994

Prepared for:

Space and Naval Warfare Systems Command
Information Systems Security Office (SPAWAR OOI)
Mr. Tim McChesney, SPAWAR PMW 151T / Mr. Robert Patton, SPAWAR OOI-E2
Washington D.C. 20363-5100

and

Department of the Navy
Naval Command, Control and Ocean Surveillance Center
Mr. John Campbell / Mr. Jim Weatherford, Code 412
RDT&E Division, San Diego, CA 92152-5000

Prepared by:

Secure Solutions, Inc.
9404 Genesee Avenue, Suite 237
La Jolla, CA 92037
(619) 546-8616

This Page Intentionally Left Blank

Table of Contents

Section **Page**

Table of Contents (continued)

Section **Page**

Table of Contents (continued)

Table of Contents (continued)

Appendices

Index of Figures

Index of Tables

This Page Intentionally Left Blank

Executive Summary

Secure Solutions, Inc. was tasked by the Department of the Navy's Space and Naval Warfare Systems Command (SPAWAR) to perform a Small Business Innovation Research (SBIR) Phase II network security research effort on the "Placement of Security Services for Secure Data Exchange."

A major thrust in Naval command and control is to securely interconnect host computers using networks for the purpose of sharing information and improving overall survivability. The purpose of Task 2 of the SBIR Phase II effort is to assess the status of security standardization for host computers, networks, and the project support environment, with an emphasis on network standards. For host computers, the technological areas of standardization that are addressed include operating systems, database management systems, graphical user interfaces, and backplanes.

The study begins with a review of recent security related studies on distributed processing and military telecommunications architectures in order to determine what security functions and services should be provided and standardized to support computer network applications. It was discovered that major changes are occurring with respect to telecommunications. These changes include the migration toward multimedia services and the use of fiber optic media to provide the physical resources needed for multimedia capabilities. Another important area of development is concerned with multilevel security products for computers and networks.

The technology assessment is followed by the primary task, the review of security guidance documents and standards and the determination of the status of those standards. Security standards for most areas are relatively new, though there is a significant commitment within industry and government toward developing and implementing the standards. Standards that include security services are being adopted by standards bodies and are beginning to be used. Most have not yet been widely implemented, and are therefore not stable. Vendors hesitate to implement products based on draft standards because standards often undergo significant revision when being upgraded from draft to international standard status. Even when standards are finalized, they are not stable. Stability comes when the standards have been implemented and there is little technological pressure to change them. Since many of the international standards are not stable, existing standards that are more widely implemented may be used in the interim.

After reviewing the standards, the study describes specific security mechanisms that can be implemented to provide the security services specified by the standards. The services include authentication, access control, audit and accountability, confidentiality, integrity, non-repudiation, and service assurance. The mechanisms include peer address checking, challenge-response exchanges, certification authorities, discretionary and mandatory access controls, digital signatures, notary services, encipherment, traffic padding, integrity check values, sequence numbering, timestamps, redundancy, and others. Finally, the study suggests additional factors concerning the choice and placement of network security mechanisms that must be considered when evaluating architectural alternatives for secure computer and communications systems.

This Page Intentionally Left Blank

Section 1

Introduction

This Page Intentionally Left Blank

1.0 Introduction

This report documents the status of host computer and network security standards and guidelines and discusses their applicability to the Navy and other government agencies. The analysis was performed by Secure Solutions under the Small Business Innovation Research (SBIR) Program for the Navy's Space and Naval Warfare Systems Command (SPAWAR) under Contract Number N00039-93-C-0099.

System designers have a responsibility to insure systems are interoperable. It is standards that can allow the computer and communications industry to achieve the goal of interoperability, and it is security standards that can allow this goal to be met in a secure manner. To better understand why security standards are needed in supporting the development of secure computer and network systems, and the types of standards that are needed, the early sections of this report briefly review the state of automation technology and the Naval data processing and communications environments. Section 1 provides background information concerning technological advances that have occurred in recent years and those that are on the horizon. Section 2 discusses related studies which describe Naval communications environments. Section 3 describes a generic computer network model based on those studies.

Having acquired the necessary background, Section 4 begins the primary objective of reviewing security guidance documents and standards in selected areas including host computers, networks, and the project support environment, with an emphasis on network standards. For this study, the host computer is further broken into specific areas of standardization: operating systems, database management systems, graphical user interfaces, and backplanes. The discussion about each standard has three parts: a description of the standard, the current status of the standard, and the security services that the standard addresses.

Security standardization for most areas are relatively new, though there is a significant commitment within industry and government toward developing and implementing the standards. Standards that include security services are being adopted by standards bodies and are beginning to be used. Most have not yet been widely implemented, and are therefore not stable. Vendors hesitate to implement products based on draft standards because standards often undergo significant revision when being upgraded from draft to international standard status. Even when standards are finalized, they are not stable. Stability comes when the standards have been implemented and there is little technological pressure to change them. Major flaws requiring correction may be discovered during implementation. Since many of the international standards are not stable, existing standards that are more widely implemented may be used in the interim.

Many of the standards describe or refer to specific mechanisms that can be implemented to provide security services in networks. Section 5 summarized the network security mechanisms that are available for implementation. Section 6 discusses additional factors that system designers should be aware of when choosing appropriate network security mechanisms and deciding where to place those mechanisms. Section 7 summarizes the entire report.

1.1 Scope

The scope of this Technical Report is to determine which security services are provided by security standards that either exist or are being developed which may be useful for specific applications by the Navy and other government agencies. This report does not address whether the standards have been implemented, nor the extent to which system designers are considering their use. Future tasks of this Phase II SBIR effort will address these aspects of the standards.

This part of the study also looks at the security services that are needed within the context of the entire computer network to decide what security services should be allocated to the host computer and what should be allocated to the communications protocol stack. Technology areas that are addressed include:

- Operating System
- Data Base Management System
- Graphical User Interface
- Backplane
- Network
- Project Support Environment (i.e., software development environment).

1.2 Study Objectives

The first technical objective of Task 2 is to look at each of the areas of automation standardization to consider what security functions and services should be provided and standardized across the board to support computer network applications, and to assess which security functions and services should be allocated to the communications protocol stack.

The second, and primary, objective is to report on the progress of standardization efforts in both commercial and government sectors for each of the areas specified above.

The third objective is to provide guidance to system designers concerning implementation of the security standards. This includes identification of security mechanisms that implement the security services specified in the standards and a discussion of additional factors concerning the determination of where to place those mechanism.

1.3 Approach

This study was accomplished by performing the following steps:

- Reviewed recent security related studies in order to develop a composite of the appropriate areas of standardization and the security services required in each of those areas
- Reviewed Naval computer and telecommunications architectures contemplated for the future in order to understand the environment and specific needs of the Navy and other Government agencies
- Developed a generic computer network model
- Interviewed members of standards bodies to identify the standards that have been specified, or may be specified in the near future
- Reviewed standards to assess their progress and to consider whether the required security services and functions have been provided.

1.4 Report Organization

The main body of the report is organized as follows:

- Section 1 – Introduction
- Section 2 – Review of Related Security Studies and Naval Architectures
- Section 3 – Generic Computer Network Model
- Section 4 – Current Standardization Efforts
- Section 5 – Security Services and Mechanisms
- Section 6 – Additional Factors Concerning Placement of Services
- Section 7 – Summary

The following appendices are provided to supplement the main body:

- Appendix A – Acronyms
- Appendix B – References

1.5 Background

Before investigating the security services needed to provide security within a system composed of host computers (e.g., within the operating system, the DBMS, the graphical user interface, and the backplane) operating within a network, it is necessary to review the progression of automation and of the associated security concerns throughout that period.

1.5.1 Trends in Automation Technology

During the period when computers began to become commercially available, there was a community that felt information could not be secured if it were placed on a computer. The information would become subject to compromise, corruption, and delay or loss. The pro-automation group, on the other hand, argued that information processed manually was more likely to include errors during both processing and transmission, that the time needed to retrieve stored data could be shortened through the use of computers, and that the manually processed information was more vulnerable to compromise, particularly during transmission if the message could not be memorized by the courier.

The concerns of those who argued to maintain the status-quo were valid at the time. It was necessary for computer system designers to provide adequate security. In order to provide integrity and reliability by overcoming simple failures in the stand-alone host, designers included security mechanisms such as default processing, handling of out-of-bounds data entries, parity checking, and sequence numbering. Confidentiality was a procedural issue. The systems were dedicated to one group of collocated users who were authorized access to all the data on the system and who were trusted to the same extent that they had been when they processed information manually. The early security mechanisms were not capable of withstanding directed attacks by those who were authorized to use the systems. Their protection from an outside threat came in the form of physical isolation.

As computers became faster and more economical, they began to be shared by groups who had no need to share data and who were, or should have been, mutually suspicious. Additional security services were required and mechanisms were installed in the operating systems to provide those services. Operating system security became well defined. System designers developed trusted computing bases (TCBs) and isolated them from the user community. The reference monitor concept was introduced to refer to that portion of the TCB which mediates all accesses by subjects, such as users and processes, to objects, such as files, programs, and devices. Users were isolated from each other as well and identification, authentication, access control, audit, and accountability mechanisms were developed. Operating systems incorporated mechanisms to prevent deadlock. They also incorporated priority processing to expedite services for processes that needed faster response times. The project support environment was moved from on-line systems to off-line dedicated support systems and was placed under configuration management procedures.

By now, users were processing huge quantities of data very quickly and with relatively few errors. They were dependent on automation and looked for further advancements. They recognized the need for, and even demanded the installation of, stronger security mechanisms. However, they did not want the security mechanisms to impact production. Userids and passwords were considered a necessity, but auditing impacted throughput and was not as well received. With faster processors and background processing, many security mechanisms became transparent to the user. While technological advances improved the ability of system designers to install better security mechanisms, they also improved the acceptability of security within the user community.

Security within the host became well understood. Not only were robust security mechanisms incorporated into operating systems, but they were also being installed in database management systems and application programs as well.

The introduction of networks brought vulnerabilities that some skeptics again felt could not be overcome. The skeptics argued that the information would become subject to compromise, corruption, and loss. The pro-networking group argued that information communicated manually was just as vulnerable in many environments. For example, in a military environment there may not be enough time to dispatch couriers to carry information between the front line and headquarters. Information is perishable. Without networks, that information must be transmitted via a manual communications system of radio operators and relay stations. These transmissions can produce errors, delays, and potentially compromise. Of course, technology won and decision makers allowed networks to be introduced to the field of automation.

The network is more than a pipeline for information flowing between host systems. The reference monitor concept must be extended to include the network and the hosts beyond, as well as the users accessing those hosts and their output products. Morrie Gasser points out, "There is one important difference between the security mechanisms in a node on a distributed system and those in a stand-alone system: the node's reference monitor may have to grant access to a subject that it has not authenticated through a trusted path." [GASSER 91] What he is saying is that the trusted path between the remote subject and the reference monitor responsible for controlling access is not under the direct control of the reference monitor.

Therefore, while it is said that each host must be solely responsible for its own security, in practice hosts must rely on other hosts to authenticate users and to provide additional security services which help enforce their security policies. Paths and remote hosts must be trusted to some specified level. That trust must be based on well defined and agreed upon trust relationships.

Generally, the services needed within the network are the same services needed on a host: access control, identification and authentication, accountability, confidentiality, integrity, and availability. However, the mechanisms to provide those services are different. In addition, communications between hosts must be protected from eavesdropping, modification, playback, loss, and other harms. Standards are being developed to provide these required services as well as some additional services such as non-repudiation. Mechanisms implemented in accordance with the standards are beginning to be developed, but are not complete nor widely implemented.

1.5.2 Advances in Network Technology

The number of stations being connected to networks has increased dramatically. In addition, file transfers are becoming larger and more frequent. Furthermore, there is a trend toward multimedia applications. Applications are being developed based on improvements in network technologies. Organizations are migrating applications off of mainframes and onto networked microcomputers. This migration is increasing the demand for even greater improvements in network technology. Consequently, some networks are, or soon will be, experiencing congestion. The use of bridges and gateways is a solution that allows a topology of small interconnected network segments. The bridge or gateway permits traffic to cross between network segments only when it is addressed to stations on the other segment. This concept of interconnected network segments has been capitalized on, causing a demand for newer high-speed network backbones.

Network hubs were introduced just seven years ago to serve as centralized concentrators and management agents for the network. *Smart hubs* with multiple network backplane buses were introduced two years later to support multiple network types. Traditional networks based on these hubs incorporate a bus topology in which all devices contend for the use of one transmission line, and must wait to transmit if another device is using the bus. *Enterprise hubs* which are now emerging, incorporate both conventional contention-based buses and high-speed switched buses to provide the high bandwidths needed for multimedia services. [BAILEY 93] In addition to the significant speed improvements, a positive security side-effect of departing from broadcast networks, in which all stations listen to the bus, in favor of a switched network topology is that eavesdropping is more difficult.

Two high-speed network technologies, each based on dual, counter flowing, fiber optic rings, are becoming popular: the Fiber Distributed Data Interface (FDDI) for a geographically small area such as a campus, small base, or ship, and the Distributed Queue Dual Bus (DQDB) for a geographically larger area such as a city or large military base. [HALSALL 92] FDDI (ISO 9314) [ISO 89B, 89C, and 90A] is a set of standards being developed by the American National Standards Institute (ANSI), and DQDB is an international standard defined in IEEE 802.6 (ISO 8802.6) [IEEE 90]. The purpose of IEEE 802.6 is to allow DQDB subnetworks to provide a range of telecommunications services within a metropolitan area. The interconnection of DQDB subnetworks to form a metropolitan area network (MAN) will be possible through the use of multiport bridges or dual-port bridges, routers, and gateways. IEEE 802.6 forms the basis for what is called the Switched Multi-megabit Data Service (SMDS). [BLACK 93]

Currently SMDS provides transmission rates of 45 Mbps which is several times faster than the Local Area Networks (LANs) it connects (operating at approximately 10 Mbps). FDDI will operate at a speed of 100 Mbps, providing a high-speed LAN backbone. There are enhancements in progress for both FDDI and 802.6. An extension to FDDI is being developed which will increase the maximum link length from two kilometers to 60 kilometers. FDDI-II, being developed by ANSI, does not run any faster than FDDI, but offers isochronous transmission services needed to support multimedia applications.

Improvements in SMDS will provide transmission rates of 150 Mbps, keeping it ahead of FDDI. Not only will both FDDI and SMDS be capable of providing LAN backbone support, but both will be capable of being used as MANs. The distinctions between LANs and MANs are disappearing as the technologies improve. Furthermore, they can serve as an interim solution for the multimedia needs of the future where data, video, and voice share a common pipeline. [SLONE 91]

Local Area Network	Metropolitan Area Network	Wide Area Network
FDDI	**DQDB**	**B-ISDN**
	"Switched Multi-megabit Data Service" (SMDS)	**• ATM** **• SONET**
100 Mbps	**45 to 150 Mbps**	**155 & 622 Mbps**
ANSI X3.166/148/139 (ISO 9314)	IEEE 802.6 (ISO 8802.6)	ATM (CCITT I.150) SONET (ANSI T1.105)

Figure 1.1-1. High Speed Fiber Optic Technologies

The broadband integrated services digital network (B-ISDN) will be even faster than SMDS and is designed specifically to provide a high-performance multimedia wide area network (WAN). Initially, B-ISDN will provide services at 155 Mbps and 622 Mbps. Future standards suggest transmission rates of 2.5 Gbps. [MALAMUD 92] B-ISDN is supported by two underlying services, both of which are beginning to be deployed commercially:

- Synchronous Optical Network (SONET) (ANSI T1.105 and T1.106) [ANSI 88A, 88B, and 89][1]
- Asynchronous Transfer Mode (ATM) (CCITT Recommendation I.150) [CCITT 91].

[1] The ANSI T1 committee is developing a series of approximately 15 documents that specify SONET physical layer characteristics. Drafts are expected to be available in 1994.

SONET is a Physical Layer synchronous protocol developed by ANSI that transmits ATM frames on a point-to-point basis over fiber optic links at speeds (which are multiples of 51.8 Mbps) of up to 2.5 Gbps, and in theory up to 48 Gbps. [MALAMUD 92] SONET links are usually provided in multiples of three. Three SONET links would provide the 155 Mbps specified for B-ISDN and 12 would provide the 622 Mbps also specified for B-ISDN. Three links would be adequate for the European standard (139 Mbps) and nine would be adequate for the Japanese standard (397 Mbps).

ATM, published in 1991 by CCITT as Recommendation I.150, is a connection-oriented switching technique that operates on top of SONET to provide fast packet-switched asynchronous time division multiplexing. [SPRAGGINS 91] It packetizes traffic into small 48 byte cells[2] and switches them between SONET links. ATM was designed under the assumption that a network will carry different kinds of traffic. It combines the packet switching used in data networks, which is efficient for bursty applications, and the circuit switching used in voice network, which guarantees continuous availability, to provide the exact bandwidth that is needed in any environment. The unique feature of ATM is that time slots are not preassigned, but are available upon demand. Voice traffic requires a narrow bandwidth when there is traffic and no bandwidth during idle periods. Data requires a wider bandwidth during transmission bursts, but requires little or no bandwidth during idle periods. ATM multiplexes the various circuits using the same communications channel. From a security perspective, ATM transmissions are circuit switched and are not broadcast or routed to other devices on a network where they could be intercepted.

ATM opponents feel voice should remain segregated on a network that uses smaller cells, say 32 bytes, and data should remain on dedicated digital networks that provide larger cells, at least 64 bytes in size. Alternative cell division techniques have been developed, but none are anywhere near as popular as ATM.

Several adaptation layers are being built on top of ATM. The voice traffic adaptation layer compensates for network delays to deliver a constant voice rate. For data and other variable rate services, the adaptation layer segments datagrams into cells and assigns sequence numbers for reassembly. Two examples of high-capacity (T1 at approximately 1.5 Mbps and T3 at approximately 45 Mbps) variable rate adaptation layer protocols are SMDS, discussed above, and Frame Relay. [FRAME 90] [CCITT 92] [ANSI 92B][3]

Frame Relay is a service that offers the ability to send bursty data packets across a network without tying up bandwidth when there is no traffic. Where ATM supports voice, data, image, and video, Frame Relay supports only data traffic. Frame Relay is similar to X.25 but was designed to provide much faster service (up to 1.5 Mbps) without guaranteeing reliable error-free transmission. It would be excellent for connecting two

[2] The ATM cell also has five bytes of control information for a total cell size of 53 bytes.

[3] The *de facto* industry standard was developed in 1990 by a consortium of vendors [FRAME 90]. ANSI T1.606 [ANSI 92B], CCITT Q.922 [CCITT 92] and CCITT I.122 (not yet published) are Frame Relay standards being developed by standards bodies.

LANs since LANs offer no service guarantees. In fact, a combination of Frame Relay and X.25, placed on top of an underlying ATM switching technology, would be very efficient. Frame Relay provides fast access to a backbone network and X.25 products can provide end-to-end error recovery. [MOTO 93B] Frame Relay is also becoming popular for implementation in MANs and WANs with confidentiality and integrity services being provided by protocols at higher layers in end systems.

Another combination worthy of mention is the interconnection of FDDI LANs over ATM-based B-ISDN networks. Many vendors are developing FDDI products for LAN communications. Similarly, many vendors are developing ATM products for WAN communications. Scholars at the Osaka and Kansai Universities have proposed a scheme that interfaces connectionless FDDI communications with connection-oriented ATM communications, and takes advantage of ATM's ability to dynamically allocate bandwidth to virtual paths according to the traffic volume and thus avoid or reduce traffic congestion. [YAMAMO 93]

There is significant support (soon to be significant demand) for multimedia communications, and B-ISDN will be available in the near future to service that demand. Witness the recent announcement that Bell Atlantic, one of the largest Regional Bell Operating Companies, plans to merge with Tele-Communications Inc., the nation's largest cable TV systems operator. Commercial communications via fiber optical links will provide integrated telephone, interactive data communications, file transfers, video teleconferencing, electronic mail, video mail, facsimile, graphics, and other services. Incorporation of ATM and SONET into ISDN will provide true broadband extensions capable of supporting the high speed data transfers needed for Naval communications as well as support for multimedia services.

Uses for these integrated services within the Navy are limitless. Weather, operations, logistics, and intelligence personnel will be able to input data on graphical workstations at different locations, whether shipboard or on shore, and commanders will be able to observe maps and databases being updated in real-time. War games can be played interactively with players all over the world, as they are today on the Worldwide Military Command and Control System (WWMCCS) and other networks, but will include real-time interactive video. Military communications will indubitable include connection to B-ISDN networks. This magnifies the need to provide security services in host computers as well as across the network, and to have a common framework of standards.

The concept of multilevel secure (MLS) operations has been defined for the Navy for more than 10 years. However, the host systems, operating systems, DBMSs, and network protocols have all lacked the ability to provide reliable multilevel security except in a few isolated cases (e.g., Honeywell XTS-200 multilevel secure operating system and computer, Secureware Compartmented Mode Workstation, Sybase Secure RDBMS SQL Server, Boeing MLS LAN Secure Network Server, Verdix VSLAN 5.0, and some others). Mandatory Access Controls (MAC), Rule Based Access Controls (RBAC), and labeling mechanisms are being designed into these areas. Automation will, perhaps within 10 years, be capable of allowing cleared and uncleared users to share the same resources.

The infrastructure for providing network security services is emerging just as these high-speed technologies are emerging. A common international foundation is provided in the International Standards Organization (ISO) Open Systems Interconnection Reference Model (OSI RM) Security Architecture, described in ISO 7498-2 [ISO 89A]. ISO 7498-2 recently underwent its periodic review, which occurs every five years for all ISO standards. No deficiencies were found, and the standard was determined to be adequate to support the capabilities of the emerging technologies for the next five years.

Another technology on the horizon is wireless LAN technology. As this technology emerges, wired networks will remain better suited for many environments, and wireless networks will be found to be well suited for others. [ROSEN 93] Wireless LANs may be well suited for a factory environment that is typically hostile to copper or fiber cable, for an office environment where the employees move frequently, or for a tactical military environment where temporary facilities are established. Wired networks will, for the foreseeable future, remain preferable for fixed site facilities because there are limitations associated with wireless technology.

Wireless technology uses infrared transmissions or radio transmissions. [SMITH 93] While infrared will have the wider bandwidth, it is limited to a range of approximately 50 feet and requires a clear line of sight. Significant uses for radio transmissions are more likely to emerge. Ranges may be in the hundreds of feet, or more. Wireless LANs can use the cellular telephone network. [BAILEY 93] Wireless devices can also incorporate spread-spectrum capabilities, but will be limited by the FCC to one watt of power if they do, and will thus have a reduced range.

ANSI Committee for Wireless LANs (IEEE 802.11) is expected to complete a draft standard in approximately 1996 and may implement the technology at layer 1 as an add-on module that interfaces to existing layer 2 LAN adapters, at layer 2 as a bundled layer 1 radio and layer 2 LAN protocol for a new LAN adapter, or at higher layers. [SMITH 93] Any of the choices are expected to be significantly more costly than the wired alternative. The benefit is portability.

There is no doubt that there will be a demand for notebook computers to be equipped with wireless LAN adapters that can take advantage of cellular telephone network connectivity for interfacing to wide area networks. This would coincide nicely with the availability of ATM and multimedia communications on the public telephone networks. But, as Bailey points out, "It will be a challenge for router-based networks to keep track of network addresses that shift from place to place." He continues, "Mobile devices represent a challenge to network security." [BAILEY 93]

1.5.3 Naval Environment

Naval command and control systems are hosted on shipboard, shore, and airborne platforms and operate in a variety of environments. Diverse communications networks are used to support these command and control systems. These networks operate from the Extremely Low Frequency (ELF) to Extremely High Frequency (EHF) band and employ both point-to-point and broadcast transmission techniques. A major thrust in Naval command and control is to interconnect these networks for the purpose of sharing information and improving the survivability of the overall network.

To support application-level interoperability among command and control systems which use these networks, the use of a layered architecture is imperative [Copernicus 91]. The most well-known framework for a layered architecture is the ISO seven layer OSI RM, as described in ISO 7498 [ISO 84]. The placement of security services within the OSI RM has always been controversial.

Furthermore, there is a need for an analysis to identify the security services that should be provided at each of the seven layers of the OSI RM for Naval and other agency applications. This effort should take into account the work being done by the International Standards Organization (ISO), the Internet Engineering Task Force (IETF), the American National Standards Institute (ANSI), the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), and the IEEE 802.10 Standard for Interoperable LAN / MAN Security (SILS) Working Group. The analysis should also consider impacts on Communications Security (COMSEC) and Computer Security (COMPUSEC) assurance criteria, and features that are important to user organization missions such as bandwidth conservation, delivery and response times, survivability, and reconfigurability. The SBIR Phase I research effort on the *Placement of Security Services for Secure Data Exchange* helped fulfill this need.

The SBIR Phase II network security research effort extends the work of the Phase I Study by further refining and validating the results of Phase I, conducting system engineering studies to define mission-specific network security needs, and developing specifications for potential network security products. Task 1 began the Phase II effort by demonstrating the concept stated in Phase I that performance improvements in delivery times can be realized for some environments by implementing security services in Layer 2 rather than implementing these services in Layers 3 or 4.

Task 2 provides a more broad view of security, analyzing factors that are important across the board regardless of whether the systems are stand-alone or networked.

This Page Intentionally Left Blank

Section 2

Review of Related Security Studies and Naval Architectures

This Page Intentionally Left Blank

2.0 Review of Related Security Studies and Naval Architectures

Reports from several recent security related studies were reviewed in order to develop a composite of the appropriate security services required in each of the areas of standardization. Each study evaluated specific security threats, services, and mechanisms. The studies include the Information Security Report for Mission Critical Computer Resource (MCCR) System Developers [SPAWAR 92A], Security in Distributed Systems [GASSER 91], the Battle Management System Case Study [SPAWAR 93D], the Submarine Combat System Case Study [SPAWAR 93E], and the Integrated Interior Communications and Control $(IC)^2$ System [NAVSEA 93].

Proposed Naval computer and telecommunication system architectures were reviewed in order to understand the environment and specific needs of the Navy. These include:

- Battle Management Command and Control System
- Submarine Combat System
- Integrated Interior Communications and Control $(IC)^2$ System
- Copernicus and supporting communications systems.

The studies on generic security services and mechanisms are reviewed below. These include the *Information Security Report for MCCR System Developers,* which discusses security services for each of the NGCR areas of standardization, and *Security in Distributed Systems,* which discusses communications services and mechanisms. These are followed by reviews of reports discussing the application of security services for specific Naval systems.

2.1 Navy Mission Critical Computer Resource Security Study

The Information Security Report for Mission Critical Computer Resource System Developers was produced by the NGCR Security Task Group (NSTG) in 1992 to provide technical information on the status of computer and communication systems security to program managers who are developing and maintaining such systems. The report provides an overview of the security guidance and standardization efforts in industry and the DoD, and summarizes the status of security standards. The NSTG report is organized according to six standardization areas which are repeated in this study:

- Operating system
- Multi-system interconnection (e.g., network)
- Multiprocessor interconnection (e.g., backplane)
- Database management system
- Graphical user interface
- Project support environment.

The MCCR system developers report identifies generic threats to computer and communications systems and security services or mechanisms which could be applied to counter those threats, based on the following requirements documents:

- Trusted Computer System Evaluation Criteria (DOD 5200.28-STD)
- Guidance for Applying TCSEC in Specific Environments (CSC-STD-003-85)
- Trusted Network Interpretation of the TCSEC (NCSC-TG-005)
- Trusted Network Interpretation Environments Guideline (NCSC-TG-011).

The generic threats and security services identified in the MCCR report are shown in Figure 2.1-1.

	Security Services												
Threats	Mandatory Access Control	Discretionary Access Control	Object Reuse	Audit	Authentication	Data Confidentiality	Traffic Confidentiality	Selective Routing	Continuity of Operations	Network Management	Protocol-Based Protection	Non-Repudiation	Communications Integrity
Browsing	•	•	•										
System Misuse	•	•	•	•									
Replay	•	•	•	•									
Penetration					•								
Eavesdropping						•		•					
Traffic Analysis							•	•					
Denial of Service								•	•	•	•		
Masquerading												•	•
Modification												•	•

Figure 2.1-1. MCCR Generic Threats and Security Services

In addition to the requirements documents listed above, the MCCR study specified several networking standards, two backplane standards, and one operating system standard. No standards are specified for database, graphical user interface (GUI), or the project support environment. Nearly all of the standards were in draft status in May 1992 when the MCCR report was published. The standards identified in the report are shown in Figure 2.1-2. The standards which describe protocols that include security services (i.e., Secure Data Network System, Standard for Interoperable LAN/MAN Security, Transport Layer Security Protocol, and Network Layer Security Protocol) are being adopted by standards bodies and are beginning to be used today.

Area of Standardization	**Standards**
Operating System	P1003.6 - Security Interface for the Portable Operating System Interface for Computer Environments (POSIX)
Network	Survivable Adaptable Fiber Optic Embedded Network (SAFENET)
	Secure Data Network System (SDNS) – Key Management Protocol (KMP) – Message Security Protocol (MSP) – Security Protocol - Layer 4 (SP4) – Security Protocol - Layer 3 (SP3)
	Standard for Interoperable LAN Security (SILS) – SILS Model – Secure Data Exchange (SDE) – Key Management Protocol – System/Security Management
	Transport Layer Security Protocol (TLSP)
	Network Layer Security Protocol (NLSP)
	Message-Oriented Text Interchange System (MOTIS)
	Directory Authentication Framework
	Security Exchange - Application Service Element (SE-ASE) **
	DoD Network Management (MIL-STD-1813)
	OSI Systems Management Standards
Backplane	Futurebus+
	High Speed Data Transfer Network (HSDTN)
DBMS	No trusted/MLS DBMS standards specified
GUI	No graphical user interface standards specified
PSE	No project support environment standards specified

** Note: The SE-ASE is now the GULS SESE

Figure 2.1-2. Standards Specified by MCCR INFOSEC Report

The MCCR report describes the security services that are identified, proposed, or provided for by the security standards. Figure 2.1-3 summarizes the security services identified for each standard. Some standards do not include particular services but may support those services in the future. These are identified with an 'F'.

	Security Services																			
Standards	Identification	Authentication	Data Origin Authentication	Peer-Entity Authentication	Audit/Accountability	Mandatory Access Control	Discretionary Access Control	Labeling	Object Reuse	Trusted Path	Admin/Security Management	Service Assurance	Selective Routing	Data Integrity	Selective Field Integrity	Data Confidentiality	Selective Field Confidentiality	Traffic Flow Confidentiality	Non-Repudiation	Key Management
POSIX P1003.6	F	F			•	•	•	•	F	F	F									
SAFENET	•	•			•	•	•	•	•			•	•	•		•		•	•	
SDNS Key Mgmt Protocol														•		•				•
SDNS Msg Security Protocol			•			•		•						•		•			•	
SDNS SP4			•	•		•		•						•		•				
SDNS SP3			•	•		•		•						•		•				
SILS	•	•			•	•		•			•			•		•	•			•
TLSP	•	•	•	•		•		•						•		•				
NLSP	•	•	•	•		•		•						•		•		•		
MOTIS	•	•	•			•		•			•			•		•		•	•	•
Directory Authentication	•	•	•	•		•								•		•			•	•
SE-ASE (now GULS SESE)			•	•		•	•	•						•	•	•	•		•	•
MIL-STD-1813 Network Mgmt	•	•			•	•	•	•			•									•
Futurebus+		•						•	•			•		•		•				
HSDTN																				
DBMS Standards							F							F		F				
GUI Standards								F		F										
PSE Standards																				

** 'F' indicates future support

Figure 2.1-3. Summary of Security Services Identified by the MCCR Report

2.2 Security in Distributed Systems

"*Security in Distributed Systems*" is a 1991 tutorial on the state of secure distributed systems. The author, Morrie Gasser, attempts to explain communications security services in relation to traditional computer system services. He states that security in a distributed system is generally viewed as being implemented by services for users and applications, and that in the OSI reference model, a layer n+1 entity is the layer n user. To minimize the connotation that services in a distributed environment apply only to communications, Gasser uses the terms "sender" and "receiver." The channel might be storage in computer memory or it might be a virtual circuit or a communications line. The paper then discusses general security services for a distributed system without regard for whether the service is available on a host or over a network.

Figure 2.2-1 identifies the threats and security services discussed by Gasser and indicates where he suggests the services should be applied to the threats. The figure also identifies the primary mechanisms suggested to provide the services.

	Services						Security Mechanisms												
Threats	Authentication	Confidentiality	Integrity	Access Control	Non-Repudiation	Availabilability	Access Control Lists	Capabilities List (subject's)	Mandatory Access Control	Integrity Check Value	Encryption	One-Way Hash Algorithm	Digital Signatures	Certification Authorities	Challenge-Response Protocol	Sequence Numbers	Timestamping	Redundancy	Selective Routing
Eavesdropping		•		•	•		•	•	•		•								
Traffic Analysis		•		•							•								
Covert Channels		•									•								
Modification			•	•						•	•								
Masquerading	•		•		•		•	•		•	•	•	•	•	•				
Insertion			•	•						•	•				•	•			
Replay			•							•	•				•	•	•		
Cascading Effect									•										
Denial of Service						•												•	•

Figure 2.2-1. Threats and Security Mechanisms in Distributed Systems

"*Security in Distributed Systems*" concludes with a discussion of standardization where he says, "Security standards are more difficult to develop than communications standards because security is more visible to the end user, and precise requirements are hard to define."

2.3 Battle Management System Case Study

A case study on the security considerations of a Battle Management Command and Control System was performed during 1992 and 1993 by the Naval Command, Control, and Ocean Surveillance Center, NRaD Division and Booz, Allen, and Hamilton for the SPAWAR-sponsored Next Generation Computer Resources (NGCR) Security Task Group (NSTG). [SPAWAR 93D]

The case study describes the current architecture whereby two networks exist: one operates in the Dedicated Security Mode for General Service (GENSER) processing with all information classified Secret NOFORN, and the other operates in the System High Security Mode for Sensitive Compartmented Information (SCI) processing with individual workstations and associated networked components operating in the Dedicated Security Mode. All information on the SCI system is classified Top Secret. Information may be automatically passed from the GENSER to the SCI systems via one-way paths. Information must be manually downgraded by removing source information before it is passed from the SCI system to the GENSER system.

The case study also sets forth four security architectures that could be implemented in future Naval platforms:

1. Dedicated Security Mode of Operations
   - GENSER network, with all information classified Secret NOFORN
   - SCI network, with all information classified Top Secret/SCI
   - Users have a need-to-know for all information on their network
2. System High Security Mode of Operations
   - GENSER network, with all information classified Secret NOFORN
   - SCI network, with all information classified Top Secret/SCI
   - Users do not have a need-to-know for all information on their network
3. Multi-Level Security Mode of Operations
   - GENSER network, with information from unclassified up to Secret NOFORN
   - SCI network, with information from unclassified up to Top Secret/SCI
   - Guards to automatically filter information passing from SCI to GENSER
4. Multi-Level Security Mode of Operations
   - One GENSER-SCI network, handling information from Secret to TS/SCI (May eventually carry unclassified and Confidential as well).

The third and fourth architectures are radical departures from the current architecture and can only become reality when general-purpose systems rated at B2, B3, and A1 become commercially available at reasonable costs and when those multi-level secure (MLS) components are suitable for battle management command and control system use.

In consideration of that future reality, the case study identifies the security services that must be available in systems operating in each of those security modes. The security services are described for each of the NGCR areas of standardization and are based primarily on requirements established in the following documents:

- Trusted Computer System Evaluation Criteria (DOD 5200.28-STD)
- Guidance for Applying TCSEC in Specific Environments (CSC-STD-003-85)
- Trusted Network Interpretation of the TCSEC (NCSC-TG-005)
- Trusted Network Interpretation Environments Guideline (NCSC-TG-011)
- Trusted DBMS Interpretation of TCSEC (NCSC-TG-021)
- DON ADP Security Program (OPNAVINST 5239.1A)
- Automated Information Systems Security Program (SECNAVINST 5239.2)
- Security Policy for Uniform Protection of Intelligence Processing in AISs and Networks (DCID 1/16).

In the Dedicated Security Mode, both host and network components must have authentication and audit capabilities. For host components the access control components are called Discretionary Access Controls (DAC), and in the network they are called Identity Based Access Controls (IBAC). In addition, the backplane and network components must provide service assurance (e.g. denial of service protection with recovery), data integrity, and data confidentiality services. Non-repudiation services must also be provided by the network.

In the System High Security Mode, in addition to providing the services required in the Dedicated Security Mode, all components must provide support for discretionary access control and security labeling of output at the System High level.

In the Multi-Level Security Mode, in addition to providing the services required in the System High Security Mode, all components must provide access control mechanisms based on the security clearance of the subjects and the security classification of the objects. For host components this form of access control is called Mandatory Access Control (MAC), and in the network it is called Rule Based Access Control (RBAC).

The project support environment (PSE) is a unique area of standardization. It is not implemented in live system components and as such has no security services associated with it except the creation of secure products.

Figure 2.3-1 depicts the security services for the areas of standardization with respect to the three security modes of operation that were identified during the Battle Management System Case Study.

	Operating System Interface	DBMS Interface	Graphical User Interface	Backplane Interface	Network Interface	Project Support Environment
DEDICATED SECURITY MODE						
• Identification and Authentication	●	●	●	●	●	
• Audit	●	●	●		●	
• Access Control (DAC/IBAC)	●	●	●	●	●	
• Service Assurance				●	●	
• Data Integrity				●	●	
• Data Confidentiality				●	●	
• Non-Repudiation					●	
SYSTEM HIGH SECURITY MODE						
• Labeling	●	●	●	●	●	
MULTI-LEVEL SECURITY MODE						
• Access Control (MAC/RBAC)	●	●	●	●	●	
• Display Labels			●			
• Creation of Secure Products						●

Figure 2.3-1. Required Services Identified by Battle Management System Case Study

2.4 Submarine Combat System Case Study

Another case study performed for the NGCR Security Task Group (NSTG) during 1992 and 1993 was on the security considerations of a Submarine Combat System. [SPAWAR 93E] This study was performed by the Naval Undersea Systems Center (NUSC), the Naval Surface Warfare Center (NSWC), and Mitre.

As with the Battle Management Command and Control System, the Submarine Combat System supports operations ranging from unclassified to Top Secret/SCI. Most systems on the submarine operate in the Dedicated Security Mode at the Secret level. The radio room is the only compartment on the submarine which is a Top Secret SCIF.

Computer security controls for the Submarine Combat System currently do not exist within the equipment. Security is provided through operational and procedural safeguards. This is similar to the current Battle Management System environment in which no encryption is provided for either network, and active security mechanisms include only identification and authentication that is limited to a userid/password logon routine and an audit capability that is limited to journaling successful logons and file accesses. The four proposed architectures described in the Battle Management System Case Study would be appropriate for the Submarine Combat System with little modification.

Figure 2.4-1 depicts the security services for the areas of standardization that were identified as requiring incorporation into the NGCR standards by the Submarine Combat System Case Study.

	Operating System Interface	DBMS Interface	Graphical User Interface	Backplane Interface	Network Interface	Project Support Environment
• Identification and Authentication	•	•	•	•	•	
• Accountability (supported by Audit)	•	•	•	•		•
• Access Control (DAC, MAC, Labels)	•	•	•	•	•	
• Service Assurance (Availability)		•		•	•	
• Data Integrity		•		•	•	•
• Data Confidentiality	•	•			•	
• Non-Repudiation					•	
• Security Management		•	•	•	•	

Figure 2.4-1. Required Security Services Identified by Submarine Case Study

2.5 Integrated Interior Communications and Control System

The Integrated Interior Communications and Control (IC)^2 Program Plan [NAVSEA 93] describes the plan for installing fiber optic networks to provide total shipboard communication connectivity, integration, and information management. (IC)^2 is the portion of the Copernicus architecture (described in the following section) that will service the users within the lifelines of the ship, and will include the integration of all voice, data and imaging, and video communications. The program plan identifies three types of application program execution platforms that will be networked together: main frames (including embedded tactical systems), workstations, and personal computers. The timeframes described are for initial deployment on new ship designs in FY95 and full capability (IC)^2 systems on combatants by the year 2010.

The designers have recognized that the basis for this unprecedented connectivity must be an open environment that spans computer hosts and network environments. They have recognized that through commercial initiatives, industry is making dramatic advances in the communications technology required by (IC)^2, and that these advances are being made independent of military requirements. They further recognize the applicability of this new technology in military systems and state that the Navy must take the position of adapting and adopting the commercial technology wherever possible.

The Broadband Integrated Services Digital Network (B-ISDN) is identified as the enabling communications technology for (IC)^2, though it is understood that the applicable standards are undergoing change and growth. In recognizing the need for an open architecture, the Government Open Systems Interconnection Profile (GOSIP) and the Portable Operating System Interface for Computer Environments (POSIX) standards were adopted as cornerstones for (IC)^2 communications. Security is recognized as a basic requirement in order to control information sharing to the extent required.

The program plan states that since the Transmission Control Protocol / Internet Protocol (TCP/IP) is the existing *de facto* open environment standard for networking, and since there are a vast array of commercial products available, TCP/IP has been established as the baseline (IC)^2 communications architecture in order to achieve connectivity as quickly as possible. It further states that the Open System Interconnection (OSI) protocol suite is the emerging *de jure* standard for networking, but that many of the OSI protocol standards remain in development and that commercial products are just now beginning to become available. Therefore, the communications architecture will evolve from TCP/IP to GOSIP protocols as finalized standards, commercial technology, and a strong support base emerge.

The basic network protocol specified for the (IC)^2 is the Fiber Distributed Data Interface (FDDI). FDDI and ISDN are included in both the TCP/IP and GOSIP environments and are therefore identified as part of the foundation for migrating (IC)^2 from TCP/IP to GOSIP. With the conversion to GOSIP protocols, the FDDI TCP/IP network will be converted to the Survivable Adaptable Fiber Optic Embedded Network (SAFENET), a Navy standard network based on FDDI and specifying all seven OSI layers. The FDDI and ISDN architectures for the (IC)^2 are illustrated in Figure 2.5-1.

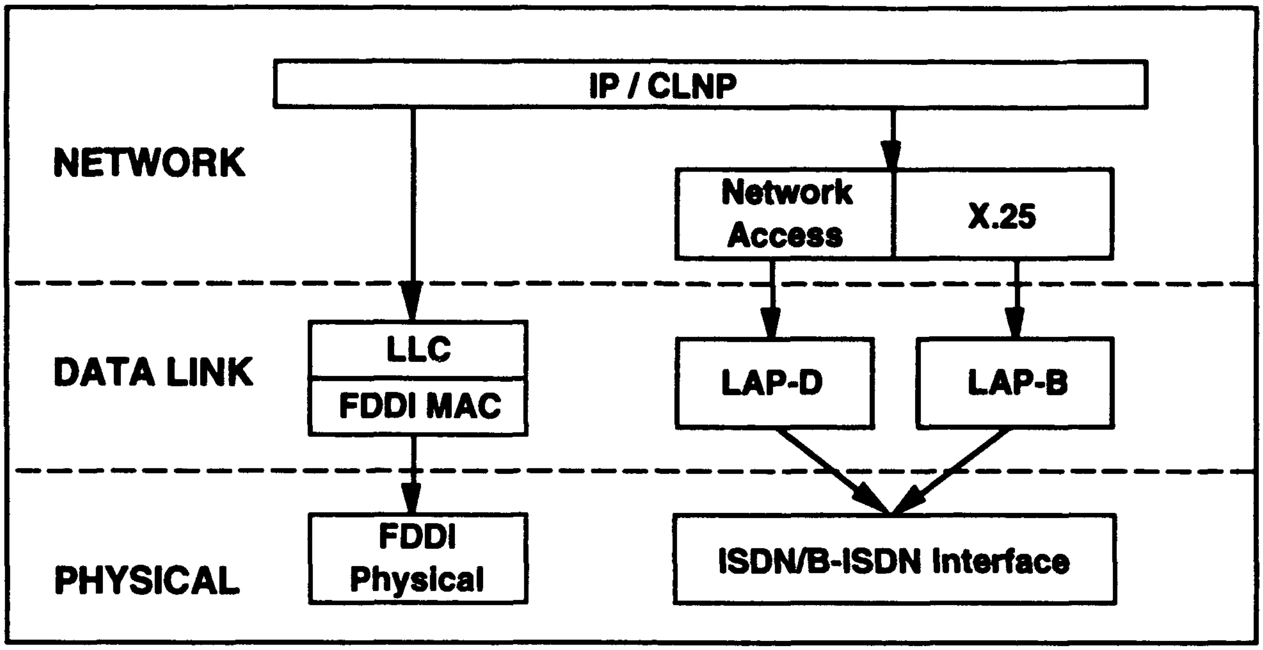

Figure 2.5-1. FDDI and ISDN Basic Networks for the (IC)2

The (IC)2 Program Plan does not describe security services in detail, nor does it identify areas of standardization where security services should be placed. It does identify the need for identification and authentication, discretionary access controls, and mandatory access controls in hosts and across the network. It also identifies the DoD and the ISO protocol stacks for providing the needed services for the network, presumably to include security services.

2.6 Copernicus Architecture

The NSTG and (IC)2 case studies provide a perspective for a network environment generally found on ships, submarines, aircraft, and shore stations. Taking a broader perspective, Copernicus provides an architecture for a Naval command and control, communications and computers, and intelligence (C^4I) system. The Copernicus Architecture Requirements Definition document [SPAWAR 91A] identifies several shortfalls in existing architecture which necessitated the design of Copernicus:

- Users must be in worldwide contact with government and industry colleagues
- Information presentation must be upgraded from narrative to video display
- Command and control doctrine must be based on the threat
- Operational traffic must be able to take precedence over administrative traffic.

Copernicus is being designed to address these shortfalls by using modern database management systems, graphical user interfaces, and communications and computer equipment. The Copernicus Architecture, shown in Figure 2.6-1, is based on four pillars: the Global Information Exchange Systems (GLOBIXS), the CINC Command Complex (CCC), the Tactical Data Information Exchange Systems (TADIXS), and the Tactical Command Center (TCC).

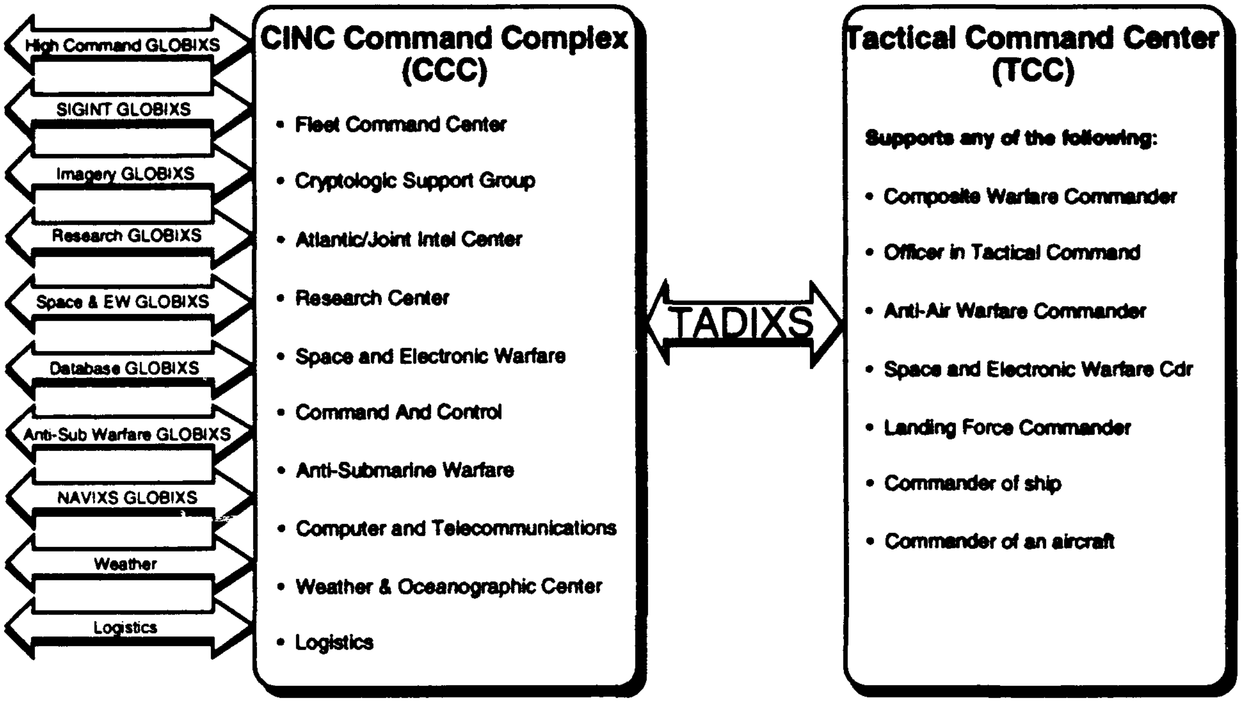
High Command GLOBIXS
SIGINT GLOBIXS
Imagery GLOBIXS
Research GLOBIXS
Space & EW GLOBIXS
Database GLOBIXS
Anti-Sub Warfare GLOBIXS
NAVIXS GLOBIXS
Weather
Logistics
CINC Command Complex (CCC)
• Fleet Command Center
• Cryptologic Support Group
• Atlantic/Joint Intel Center
• Research Center
• Space and Electronic Warfare
• Command And Control
• Anti-Submarine Warfare
• Computer and Telecommunications
• Weather & Oceanographic Center
• Logistics
TADIXS
Tactical Command Center (TCC)
Supports any of the following:
• Composite Warfare Commander
• Officer in Tactical Command
• Anti-Air Warfare Commander
• Space and Electronic Warfare Cdr
• Landing Force Commander
• Commander of ship
• Commander of an aircraft

Figure 2.6-1. The Copernicus Architecture

CCCs incorporate virtual networks consisting of many local area networks (LANs) connected by a metropolitan area network (MAN). CCCs will be established at a few locations around the world. TCCs will support tactical commanders such as commanders of carriers, submarines, aircraft, land forces, and joint task forces. Tactical level TCCs are analogous to theater level CCCs. The TCC provides the tactical connectivity to units and other force commanders.

GLOBIXS are shore-based worldwide virtual networks supported by the Defense Communications System (DCS) and commercial networks including the General Service Administration's Federal Telephone System 2000 (FTS2000). GLOBIXS will provide strategic connectivity among government agencies and industry. TADIXS are afloat virtual networks that provide tactical communications to a wide variety of user communities and are implemented over Communications Support System (CSS) assets using shared HF, VHF, UHF, SHF, EHF military satellite, and commercial satellite circuits.

Security services called for in the Copernicus Architecture Phase I Requirements Definition include those shown in Figure 2.6-2.

Security Services	Attribute Required of Copernicus Architecture
Identification and Authentication	Support user identification and authorization
Audit	Provide auditable access to mission-critical and security-critical system elements
Access Control (DAC, MAC, Labels)	Support secure transfer of information that originates at multiple security levels (implemented at the user level)
	Alert users to intrusion or manipulation
	Provide controlled access to mission-critical and security-critical system elements based on clearance, authorization, and need-to-know
Service Assurance	Continue to operate in the face of enemy attempts to deny service
	Deliver needed information when and where needed
	Provide timely access to high priority information
	Support degraded modes of operation
	Robust
	Provide capability to rapidly reconstitute essential capabilities
	Maintain continuity of information
	Provide capability to rapidly recover from overload
Data Integrity	Maintain security integrity for user-to-user and system control information throughout the information system
Data Confidentiality	Deny intelligence to the enemy
	Provide confidentiality for user information

Figure 2.6-2. Copernicus Security Requirements

The NGCR areas of standardization are relevant to the Copernicus architecture. Standards specifically cited by the Copernicus Architecture Phase I Requirements Definition of August 1991 include those shown in Figure 2.6-3.

Areas of Standardization	Copernicus Standards
Operating System	POSIX
	UNIX
Graphical User Interface	
– Man-Machine Interface	X-Windows II Release 4
– Display Toolkit	MOTIF
– Display	Chart+
Database Mgmt System	SQL/RDBMS
Backplane	VME/Futurebus+
Communications	GOSIP/TCP-IP/SAFENET

Figure 2.6-3. Copernicus Standards

TADIXS networks implemented over CSS assets will require specialized security devices. The Embeddable Information Security (INFOSEC) Product (EIP) is being designed to support those security requirements. [SPAWAR 92B] A study by SPAWAR on the security placement options for EIP recommends that EIP devices be placed at:

- Layer 7 to provide a fine granularity of security services
- The top of Layer 3 to provide interoperability between afloat and existing shore based networks
- Layer 2 to provide link encryption and transmission security (TRANSEC) services.

2.7 Summary of Review of Related Studies

The first two reports that were reviewed provide a general understanding of the threats which may be brought to bear against computer and communications assets and the general categories of security mechanisms that may be successful in limiting harm from those threats.

The NSTG INFOSEC Report to Navy MCCR System Developers considered security services for host computers (i.e., operating system, DBMS, graphical interface, and backplane), networks, and the project support environment that could be implemented to counter specific threats identified in the report. It also identified protocol and system standards that could be specified in order to provide the needed security services.

The report on Security in Distributed Systems by Morrie Gasser took the approach of recognizing the similarities between networks and host computer systems in order to discuss common security threats and generic services. In spite of this, the report identified very similar threats to those which were identified by NSTG. This report also recommended various security mechanisms which would be appropriate for providing security services for distributed systems.

Next, three specific Naval systems were studied. Security services that were needed to enforce the security policies of the systems were identified. In each case, the services conformed approximately to those discussed in the generic sense by the first two studies. This means that Naval systems require the types of security services that apply to all networked systems. Furthermore, the specific mechanisms that are required for the Navy systems are those that are commonly used.

Some of the studies specified which areas of standardization the security services should be applied. The studies did not discuss the actual placement of those mechanisms, nor how they should be implemented.

Finally, the Copernicus documentation was reviewed and found to specify security requirements which equate to the general security services suggested in the first two reports that were reviewed. The standards that are specified for Copernicus also conform to those that have been recommended for general application within the Navy by the NGCR staff with the exception that the Copernicus architecture calls out standards for graphics while the NGCR report does not.

Overall, standards which describe security services are in their infancy. At the time of the NSTG report to MCCR system developers, every standard discussed for providing network or backplane security was in draft form. Desired security services, as identified in the case studies above, are being incorporated by standards committees into standards. Some standards that describe protocols which include security services are now being adopted by standards bodies and are beginning to be used today, though it will be several years before they are widely implemented. However, except for the Secure Data Network System (SDNS), a full and complete set of standards that provides well rounded and complete services with high assurance does not yet exist. Even SDNS, while being put into use, is relatively new and is undergoing revision and expansion.

In the next section, a model of a generic computer network will be developed based on the findings of these reviews. The model will be useful in the identification and placement of appropriate security services and mechanisms.

This Page Intentionally Left Blank

Section 3

Generic Computer Network Model

This Page Intentionally Left Blank

3.0 Generic Computer Network Model

Task 2 proposes a model for the Naval computer network of the future. This model will be used throughout the task as a reference so that recommendations for security services and mechanisms may be viewed in their proper perspective. The model, depicted in Figure 3.0-1, consists of the following components:

- Host computers
- Local area networks
- Network switching elements (NSE)
- Tactical transmission media
- Strategic communication system interfaces.

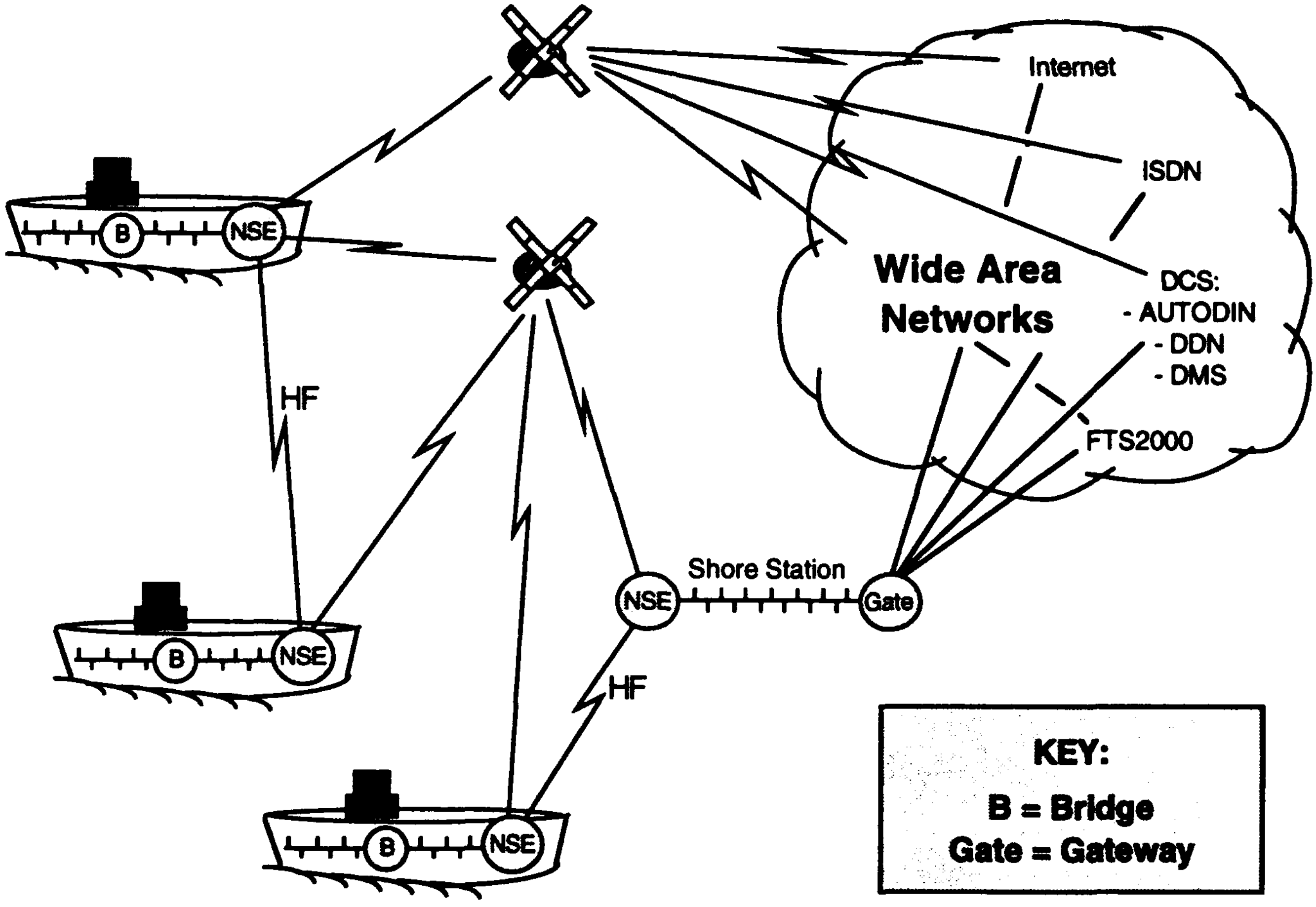

Figure 3.0-1. Generic Computer Network Model

As shown in the figure, host computers and LANs are located on ships and shore stations. They are also located on submarines and airborne platforms, not shown in the figure. Each ship or shore station can be thought of as a node on a network capable of communicating with other nodes via network switching elements and tactical transmission media. The tactical transmission media includes point-to-point transmission links (such as HF) and broadcast channels (such as satellite transmissions). In the past, connection to strategic communications systems has typically been through land-based gateways. However, network switching elements can also incorporate gateway functionality to interface any node to the strategic communications systems; or the gateway functionality could be incorporated within the strategic system itself. The network switching elements will process network layer protocols in order to perform internetwork routing. Bridges are shown on the ships, but are not included as major components of the model because they can only be used to connect adjacent LANs and cannot be used for entry into wide area networks. Remote bridges could be used to connect two logically adjacent LANs located on different ships.

The components of the model will require security functions in computing and communications areas of standardization, and these functions must cooperate with those provided by the communications protocols. For example, an application may provide mandatory access controls and may rely on mechanisms in the operating system, DBMS, as well as communications protocols to maintain security. The allocation of security services to non-network related areas of standardization will thus have a direct impact on the placement of network security services within the OSI stack. With the model in mind, we can view where each of the technological areas of standardization are to be applied and how security functions within these areas are relevant to the Navy environment. Figure 3.0-2 correlates the security areas of standardization to the components of the generic model.

Areas of Standardization	Host Computers	Local Area Networks	Network Switching Elements	Tactical Transmission Media	Strategic System Interfaces
Operating Systems	•		•		•
Data Base Management Systems	•		•		•
Graphical User Interface	•				
Backplane	•				
Networks		•		•	
Project Support Environment	•	•			

Figure 3.0-2. Areas of Standardization for Generic Model

3.1 Description of a Generic Computer Network

The generic computer network model includes all Naval automation capabilities. It encompasses:

- ***Host Computers***

  The host computer category includes resources in both the development and operational environments. These host resources are available to users for performing mission related functions including software development, information gathering, database manipulation, word processing, command briefings, and message transmission. Examples of host computers are:

  - Data processing and graphical workstations
  - Special purpose command and control components
    - Display systems
    - Computationally intensive support processors
    - Database support processors
  - Network servers

  All of the host computers will have operating systems. Some will have a database management system (for example a directory server). The security functions that must be provided in the host computers include:

  - User identification and authentication
  - Mandatory and discretionary access controls
  - Audit
  - Configuration management
  - Software and data file backup procedures
  - Checksums for distribution of software
  - Distribution of executable files only
  - Encryption of storage media and communications information.

  Special consideration should be given to the requirements of:

  - Trusted Computer System Evaluation Criteria (DOD 5200.28-STD)
  - Trusted DBMS Interpretation of TCSEC (NCSC-TG-021).

- ***Local Area Networks***

Networks, typically on ships and shore stations, but also on submarines and aircraft, may include multiple LANs with local relays to connect the LANs. The security functions for this category have been described in the SBIR Phase I effort. They include:

Generic Service	Specific Service
Authentication	Peer Entity Authentication
	Data Origin Authentication
Access Control	Access Control
Data Confidentiality	Connection Confidentiality
	Connectionless Confidentiality
	Selective Field Confidentiality
	Traffic Flow Confidentiality
Data Integrity	Connection Integrity with Recovery
	Connection Integrity without Recovery
	Selective Field Connection Integrity
	Connectionless Integrity
	Selective Field Connectionless Integrity
Non-repudiation	Non-repudiation with Proof of Origin
	Non-repudiation with Proof of Delivery

Categorization based on ISO 7498-2

Security Mechanism	Description
Encipherment	The cryptographic transformation of data to produce ciphertext.
Digital Signature	Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g. by the recipient).
Access Control	The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.
Data Integrity	The property that data has not been altered or destroyed in an unauthorized manner.
Authentication Exchange	A mechanism intended to ensure the identity of an entity by means of information exchange.
Traffic Padding	The generation of spurious instances of communication, spurious data units and / or spurious data within data units.
Routing Control	The application of rules during the process of routing so as to choose or avoid specific networks, links or relays.
Notarization	The registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, origin, time and delivery.

Definitions extracted from section 3 of ISO 7498-2

Figure 3.1-1. Security Services and Mechanisms

- ***Network Switching Elements***

  Network switching elements are necessary to provide dynamic allocation of the capacity of tactical transmission media between ships, shore stations, and other platforms. Examples are:

  - Packet switches
  - Circuit switches
  - Hybrid switches
  - ISDN switches.

  Security issues related to switching includes:

  - Routing control
  - Congestion control
  - Avoidance of deadlock
  - Authentication services
  - Access control service
  - Data integrity service
  - Data confidentiality service
  - Service assurance.

- ***Tactical Transmission Media***

  Tactical transmission media (such as HF, UHF, SHF, and EHF) carry information between shore stations, ships, and other platforms. This component of the model may also include the use of strategic assets (e.g., SATCOM). Examples of points requiring connection by tactical transmission media include:

  - Ship to ship
  - Ship to aircraft
  - Ship to submarine
  - Ship to shore station
  - Aircraft to station
  - Submarine to station
  - Station to station.

The security functions that must be provided in the tactical transmission media include:

- Confidentiality
- Integrity
- Authentication
- Access control
- Jamming detection
- Anti-jamming services
  - Spread spectrum
  - Adaptive arrays
  - Null steering techniques
- Traffic flow security services
- Low probability of intercept (LPI)
- Low probability of exploitation (LPE)
- Error control
- Uninterruptible power supply (UPS).

This study is primarily concerned with security issues associated with interfacing LANs with tactical communications media, rather than with specifying tactical communications security requirements.

- ***Strategic Communication System Interfaces***

Interfaces to the Defense Communication System (DCS) and its' wide area networks (WANs), the Automatic Digital Network (AUTODIN) and Defense Special Security Communications System (DSSCS), and the Defense Data Network (DDN) and eventually the Defense Message System (DMS), are strategic in nature and are typically provided by shore based elements. Since one station may support multiple units afloat, security functions must focus on reliability. Countermeasures which support reliability include:

- Dual-homing to multiple DCS entry points
- Redundant components
- Diverse communications media
- Alternate routing
- Selective routing
- Congestion control
- Precedence handling with preemption.

Other strategic interfaces that will be necessary in Naval environments of the future are interfaces to Internet, a worldwide unclassified commercial network that is used for e-mail, file transfers, teleconferencing, and other automation services, and the broadband ISDN which will enrich the interactive capabilities of all Naval automation by supporting interactive video and other services, as discussed in the introductory section of this report. Interfaces to the Federal Telephone System 2000 (FTS2000) will also be needed to provide connectivity of Naval and other organizations.

3.2 Standardization of Security Functions

The generic computer network model consists of host computers, local area networks, network switching elements, tactical transmission media, and strategic communication system interfaces that require varied but related security functions. Standardization of the security functions is necessary so that parallel and compatible efforts can be applied to each of the areas to enhance open systems security. Use of the model helps direct the focus of where standardization is needed.

Security services are needed in each of the areas of standardization. However, some of those services are necessary only to support functions in another area. Figure 3.2-1 identifies the general categories of security functions needed in the areas of standardization, and shows the network components where they are needed.

	Security Functions							
Areas of Standardization	Identification & Authentication	Discretionary Access Control	Mandatory Access Control	Audit and Accountability	Service Assurance	Data Confidentiality	Data Integrity	Non-Repudiation
Operating System Host computers Network switching elements Strategic Communication System Interfaces	●	●	●	●	●			
Database Management System Host computers Network switching elements Strategic Communication System Interfaces	●	●	●	●	●	●	●	
Graphical User Interface Host computers			●			●	●	
Backplane Host computers	●	●	●		●	●	●	
Network Local area networks Tactical transmission media	●	●	●	●	●	●	●	●
Project Support Environment	●	●	●	●		●	●	

Figure 3.2-1. Categories of Security Functions Needed in Areas of Standardization

Section 4

Current Standardization Efforts

This Page Intentionally Left Blank

4.0 Current Standardization Efforts

This section provides a synopsis of the current status for each of the areas of standardization, and identifies security functions and services that should be provided in each of the areas:

- Operating Systems
- Database Management Systems
- Graphical User Interfaces
- Backplanes
- Networks
- Project Support Environment.

4.1 Current Status of Standardization

Within each area of standardization, there are guidance documents and standards which have been or are being developed and which impact security. Security guidance documentation provides security architectures, standards profiles, and security evaluation criteria and guidelines for applying security services. The sources of security guidance documentation are:

a. DoD National Computer Security Center (NCSC)

- Trusted Computer System Evaluation Criteria (DOD 5200.28-STD) [DOD 85]
- Trusted DBMS Interpretation of TCSEC (NCSC-TG-021) [NCSC 91A]
- Trusted Network Interpretation of TCSEC (NCSC-TG-005) [NCSC 87].

b. National Institute of Standards and Technology (NIST)

- Federal Criteria for Information Technology Security (Proposed FIPS PUB) [NIST 92I and 92J]
- Government OSI Profile (GOSIP) (FIPS PUB 146-1) [NIST 91B]
- Government Network Management Profile (GNMP) (FIPS PUB 179) [NIST 92C].

c. Internet and International Standards Organization (ISO)

- Reference Model of Data Management (ISO 10032) [ISO 93J]
- Open Systems Interconnection Reference Model (OSI RM) Security Architecture (ISO 7498-2) [ISO 89A]
- Security Frameworks for Open Systems (ISO 10181) [ISO 92B, 92C, 92D, 92E, 93A, 93B, and 93C]
- Security Labels Framework for the Internet (RFC 1457) [RFC 93A]
- OSI Directory Authentication Framework (ISO 9594-8) [ISO 90D]
- OSI Lower Layers Security Model [ISO 93I]
- OSI Upper Layers Security Model (ISO 10745) [ISO 94A].

Standards documents include general automation standards, national and international security standards, and Naval automation standards. The general and Naval automation standards are not directed toward security, but consider security or have an impact on security. Standards in the three areas are:

a. General Automation Standards

- Relational Database Standard Query Language (FIPS PUB 127-2) [NIST 93N]
- Remote Database Access (ISO 9579-1) [ISO 93H]
- Information Resource Dictionary System Services Interface (ISO 10728) [ANSI 92A]
- X-Windows User Interface (FIPS PUB 158) [NIST 90D]
- X-Windows GUI – Part 1: Modular Toolkit Environment (IEEE P1295.1)
- Uniform Application Program Interface – GUI (IEEE P1201.1)
- Graphics Kernel System (FIPS PUB 120-1) [NIST 91C]
- Programmer Hierarchical Interactive Graphics System (FIPS PUB 153) [NIST 88]
- Computer Graphics Metafile (CGM) (FIPS PUB 128-1) [NIST 93P]
- Initial Graphics Exchange Specification (IGES) (FIPS PUB 177) [NIST 92K]
- Futurebus+ Recommended Practices (IEEE 896.3) [IEEE 92A]
- HSDTN shared memory: Scalable Coherent Interface (IEEE 1596) [IEEE 93B].

b. National and International Security Standards

- Portable Operating System Interface for Computer Environments (POSIX) Security Interface (IEEE P1003.6) [IEEE 93D and 93E]
- Network Management for DoD Communications (MIL-STD-2045-38000 [DoD 93A]
- Generic Upper Layer Security (GULS) (DIS 11586) [ISO 93D, 93E, 93F, and 93G]
- Standard for Interoperable LAN and MAN Security (SILS) (IEEE 802.10) [IEEE 93A and 93C]
- Secure Data Network System (NISTIRs 90-4250, 90-4262, 90-4259) [NIST 90A, 90B, and 90C]
- Network Layer Security Protocol (NLSP) (ISO 11577) [ISO 94B]
- Transport Layer Security Protocol (TLSP) (ISO 10736) [ISO 94C and 94D]
- Standard Security Label for the GOSIP (Proposed FIPS PUB) [NIST 93R]
- Presentation Layer Confidentiality, Integrity, and Cryptography (ISO 8822 and ISO 8823)
- Message Digest Algorithms (RFCs 1319 and 1320) [RFC 92A and 92B]
- Secure Hash Standard (SHS) (FIPS PUB 180) [NIST 93H]
- Digital Signature Standard (DSS) (Proposed FIPS PUB) [NIST 93I]
- Message-Oriented Text Interchange System (ISO 10021) [ISO 90C]
- Privacy Enhanced Internet Electronic Mail (RFCs 1421, 1422, 1423 1424) [RFC 93B, 93C, 93D, and 93E]
- Key Management Using ANSI X9.17 (FIPS PUB 171) [NIST 92D].

c. Naval Standards

- Operating System Interface (OSIF) Standard (MIL-STD-OSIF) [SPAWAR 93C]
- SAFENET Standard (MIL-STD-2204) [SPAWAR 92C].

Tables 4.1-1 and 4.1-2 identify the areas of standardization where each of the security guidance documents and standards listed in the previous paragraphs apply. Table 4.1-1 identifies the documents that are applicable to all of the areas except network standardization, and Table 4.1-2 identified the documents that are applicable to network standardization. The status of each document is discussed in the following sections, beginning with those that apply to the host, followed by those that apply to the network, and concluding with those that apply to the project support environment.

Table 4.1-1. Security Guidance Documents and Standards for Non-Network Areas

Area of Standardization	Security Guidance Documents and Standards
Operating System Guidance Documentation	DoD Trusted Computer System Evaluation Criteria (TCSEC)
	Federal Criteria for Information Technology Security
Operating System Standards	Portable Operating System Interface for Computer Environments (POSIX) Security Interface
	Operating System Interface (OSIF) – OSIF Standard (MIL-STD-OSIF) – OSIF Handbook (MIL-HDBK-OSIF)
DBMS Guidance Documentation	Trusted DBMS Interpretation of TCSEC (TDI)
	Reference Model of Data Management
DBMS Standards	Relational Database Standard Query Language (SQL)
	Remote Database Access (RDA)
	Information Resource Dictionary System (IRDS) Services Interface
	MLS/Trusted DBMS security standards
Graphical User Interface Standards	X-Windows User Interface
	X-Window GUI Modular Toolkit Environment (based on MOTIF)
	Uniform Application Program Interface – GUI (for non-X-Windows)
	Graphics Kernel System (GKS)
	Programmer's Hierarchical Interactive Graphics System (PHIGS)
	Computer Graphics Metafile (CGM)
	Initial Graphics Exchange Specification (IGES)
	Graphics User Interface security standards: None
Backplane Standards	Futurebus+
	High Speed Data Transfer Network – Shared Memory Paradigm: Scalable Coherent Interface (SCI) – Data Channel: None
PSE Guidance Documentation	NCSC Guidelines
PSE Standards	Portable Common Tools Environment (PCTE) Standard
	Project Support Environment security standards: None

Table 4.1-2. Network Security Guidance Documents and Standards

Area of Standardization	Security Guidance Documents and Standards
Network Guidance Documentation	Trusted Network Interpretation of TCSEC (TNI)
	Government Open Systems Interconnection Profile (GOSIP)
	Government Network Management Profile (GNMP)
	DoD Network Management Standard (MIL-STD-2045-38000)
	OSI Reference Model Security Architecture
	Security Frameworks for Open Systems – Security Frameworks Overview – Authentication Framework – Access Control Framework – Confidentiality Framework – Integrity Framework – Non-Repudiation Framework – Security Audit Framework – Guide to Open Systems Security
	Security Labels Framework
	Directory Authentication Framework
	OSI Lower Layers Security Model
	OSI Upper Layers Security Model
Network Standards	Generic Upper Layer Security (GULS) Standard
	Survivable Adaptable Fiber Optic Embedded Network (SAFENET) – SAFENET Standard (MIL-STD-2204) – SAFENET Handbook (MIL-HDBK-818-1)
	Standard for Interoperable LAN and MAN Security (SILS) – SILS Model – Secure Data Exchange (SDE) – Key Management Protocol – System/Security Management
	Secure Data Network System (SDNS) – Key Management Protocol (KMP) – Message Security Protocol (MSP) – Security Protocol - Layer 4 (SP4) – Security Protocol - Layer 3 (SP3)
	Network Layer Security Protocol (NLSP)
	Transport Layer Security Protocol (TLSP)
	Standard Security Label for the GOSIP (SSL)
	Presentation Layer Confidentiality, Integrity, and Cryptography
	Message Digest Algorithms (MDA)
	Secure Hash Standard (SHS)
	Digital Signature Standard (DSS)
	Message-Oriented Text Interchange System (MOTIS)
	Privacy Enhancement for Internet Electronic Mail (PEM)
	Key Management Using ANSI X9.17

4.1.1 Operating System Standards

4.1.1.1 DoD Trusted Computer System Evaluation Criteria (DOD 5200.28-STD)

Description. The DoD Trusted Computer System Evaluation Criteria (TCSEC), commonly known as the Orange Book, was developed by the National Computer Security Center (NCSC) in 1983 to provide system developers with the criteria to build secure computer systems. [DoD 85] The Orange Book applies to host computers and identifies the characteristics needed in secure systems. These characteristics are implemented by the operating system and are supported by hardware mechanisms. Government agencies have since referenced the Orange Book criteria as specifying required computer system features, so in effect, the Orange Book has become a regulatory document.

The Orange Book provides the design criteria for systems capable of being used for multilevel operations. It specifies more stringent security features for systems that are intended for multilevel environments than for systems intended for dedicated or system high use. The TCSEC also specifies assurance requirements that are particularly important for systems being developed for multilevel operations. Assurance is a philosophy of developing a system in a secure environment using methods that demonstrate the system is likely to comply with its security policy, is relatively tamperproof, and will remain that way. Assurance cannot be demonstrated when security mechanisms are added to existing systems that were not designed to accommodate security.

Other nations have found the Orange Book to meet many of their security needs and have implemented similar standards for their computer systems. Examples include:

- Information Technology Security Evaluation Criteria (ITSEC), Harmonised Criteria of France - Germany - the Netherlands - the United Kingdom, 1991
- United Kingdom Information Technology and Certification Scheme, 1991
- Technical Rationale for Australian Computer Security Risk Analysis Guidelines, 1992
- Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), (being revised, 1993).

The Orange Book specifies security features that enforce accountability and access control. It also specifies criteria for assurance and documentation. The latter do not identify computer security services, but are concerned with implementation. As such, they are not discussed in this document.

Status. The Orange Book was published more than 10 years ago, was revised slightly in 1985, and has not changed since. Discussions of extending the document to include mechanisms involving new technologies have been deferred until well into the future.

Security Services. Operating systems implemented in accordance with Orange Book criteria will provide some or all of the following security services:

- Identification and Authentication
- Discretionary Access Control
- Mandatory Access Control
- Labels
- Audit
- Object Reuse
- Trusted Path
- Covert Channel Protection
- Assurance.

4.1.1.2 Federal Criteria for Information Technology Security (Proposed FIPS PUB)

Description. The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) are engaged in a joint project to develop a series of Federal Information Processing Standards (FIPS) to specify requirements for development of trusted systems. The Federal Criteria will become the first of these FIPS, and is intended to eventually replace the Orange Book. [NIST 92I and 92J]

The standard distinguishes information technology (IT) products, which are off-the-shelf hardware/software packages, from IT systems, which are generally composed of many IT products, and addresses IT product requirements only. Future FIPS publications will address system compositions and specific product profiles. Like the Orange Book, the Federal Criteria specifies functional requirements which are relevant to this report, and assurance requirements which are not.

The Federal Criteria identifies commercial security requirements for products intended to be useful to users in the private, civil government, and defense sectors.

Status. The first public draft was circulated in January 1993 for review and comment. As a draft, it is not intended for compliance or for any other use other than to stimulate discussion and comment. Progress is currently in abeyance, pending liaison with the European community. The second public draft is expected to be circulated in early 1994. The Federal Criteria is expected to be published as a FIPS PUB in 1994.

Security Services. Information technology products implemented in accordance with the Federal Criteria for either government or commercial use will provide some or all of the following security services:

- Identification and Authentication
- System Entry Control
- Discretionary Access Control
- Non-Discretionary Access Control
- Labels
- Reference Mediation
- Trusted Path
- Audit
- Covert Channel Handling
  - Covert Storage Channels
  - Covert Timing Channels
- Object Reuse
- TCB Assurance Functions
  - Logical Protection
  - Physical Protection
  - Self-Checking
  - Start-Up & Recovery
  - Privileged Operations
  - Ease-of-Use
- Security Management
- Availability
  - via Resource Allocation
  - via Fault Tolerance

4.1.1.3 Portable Operating System Interface for Computer Environments (POSIX) Security Interface (IEEE P1003.6)

Description. FIPS PUB 151-2 (POSIX) [NIST 93Q] adopted IEEE Std 1003.1 [IEEE 88] as the federal standard for enabling portability of application programs across different vendor systems and architectures. POSIX is also specified in International Standard ISO 9945-1 and 9945-2 [ISO 90E and 93M]. POSIX is not intended to specify internal operating system mechanisms. POSIX requires that vendor-independent interface specifications be defined between application programs and operating systems to achieve portability.

POSIX is supported by additional documents, one of which is P1003.6, the security interface. P1003.6 defines five optional sets of security interfaces to open systems: access control lists, audit, privilege, mandatory access control, and information label mechanisms. Goals of the security interfaces are:

- Access control list (ACL) interface – provides a finer granularity of control over access to objects by users and groups

- Audit interface – provides portable audit applications, portable audit post-processing applications, and access to implementation-specific audit trail storage mechanisms
- Privilege interface – provides discretionary access control of privileged users by allowing access to only those functions and files that are needed
- Mandatory access control interface – provides interfaces to system-enforced access control policies for portable trusted applications
- Information labeling interface – provides interfaces to data labeling policies that are not related to mandatory access control, such as markings that indicate trustworthiness of the data, handling caveats, warning notices, DAC advisories, release markings, or anything else about the data.

Status. Draft 13 of the POSIX Security Interface was published by the Institute of Electrical and Electronics Engineers (IEEE) in November 1992 as an unapproved draft, and as such possesses no authority as a standard. Draft 14 of the POSIX Security Interface is scheduled for distribution and balloting in February 1994. P1003.6 has been split into sections: P1003.6a applies to ISO 9945-1 and P1003.6b applies to ISO 9945-2.

The security interfaces will become integrated into ISO 9945-1, System Interface, ISO 9945-2, Shell and Utilities, and ISO 9945-3, System Administration as they are approved and published.

Security Services. The POSIX Security Interface currently provides the following security services, though it should be noted that these documents have evolved considerably and are not yet final:

- Discretionary Access Control
- Mandatory Access Control
- Privilege
- Labels
- Audit.

Security services that are explicitly deferred to future versions of P1003.6 include:

- Networking Services and Protocols (not defined)
- Security Management Information Services.

4.1.1.4 Operating System Interface Standard (MIL-STD-OSIF)

Description. The Operating System Interface (OSIF) Standard (MIL-STD-OSIF), being prepared under the Navy Next Generation Computer Resources (NGCR) Program's Operating Systems Standards Working Group (OSSWG), details the use of POSIX standards and profiles for specifying operating system services for Mission Critical Computer Resource (MCCR) systems so that portable applications executing under an operating system that conforms to the profile will execute properly. It is intended to provide for the interoperability, integration, and portability of diverse software for various types of computer hardware and systems to allow systems to be built of integrated interchangeable commercial-off-the-shelf products. The use of POSIX compliant operating systems is a fundamental part of the transition toward adopting an open systems approach. Because MIL-STD-OSIF is undergoing significant change, the profiles that will be specified cannot be identified with certainty. However, the profiles that were originally planned to be specified for MCCR use were:

- **POSIX Minimum Realtime System Profile** – for small embedded realtime systems that require no file system
- **POSIX Realtime Controller System Profile** – for small realtime systems that require support for file and directory systems and asynchronous input/output
- **POSIX Dedicated Realtime System Profile** – for systems that require basic input/output, event management, and memory management
- **POSIX Multi-Purpose Realtime System Profile** – for systems that require comprehensive capabilities for running real-time and non-realtime tasks
- **POSIX Platform Environment Profile** – for general purpose multiuser hosts that do not require realtime or network communications.

There are no security-related POSIX profiles. OSIF security requirements identified in POSIX Security Interface (P1003.6) and DoN AIS Security Program (SECNAVINST 5239.2) must be integrated with system profiles and the resulting security profile must be consistent with the Orange Book. [SPAWAR 93C]

The companion handbook, MIL-HDBK-OSIF will offer guidance in selecting POSIX standards to meet MCCR operating system requirements. The handbook will discuss POSIX standardized profiles, the tailoring of those profiles, and conformance testing.

Status. The MIL-STD-OSIF and MIL-HDBK-OSIF have not been approved, and can only be used for informational purposes. The inherent disadvantage to these documents is that many of the POSIX standards are not yet approved by IEEE. The NGCR Program Office has suspended the development of future MIL-STDs due to the evolutionary nature of commercial standards. A long term replacement for the traditional MIL-STDs is being evaluated. In the interim, NGCR will focus on influencing the POSIX standards development.

The POSIX security standards will not be incorporated into MIL-STD-OSIF and MIL-HDBK-OSIF until they are approved by IEEE. This may occur as early as 1995.

Security Services. The MIL-STD-OSIF security profile will likely reiterate the security services provided by the POSIX Security Interface. It should be noted that both POSIX and MIL-STD-OSIF have undergone substantial evolutionary changes and are not yet final. The security services that may be expected in the MIL-STD-OSIF are:

- Discretionary Access Control
- Mandatory Access Control
- Labels
- Audit.

4.1.2 Database Management System Standards

Guidance documents and standards related to Database Management Systems (DBMSs) are discussed in the order shown on Table 4.1-2. Their ordering was arranged according to following sequence:

- **Evaluation criteria** and guidelines
- **Architectures** that define placement of security services within DBMSs
- **Standards** that specify DBMS language, schema, and remote access
- **Application Programmer's Interfaces (API)** for applications to interface with information resource dictionaries and DBMSs
- **Multilevel/Trusted DBMS security standards.**

4.1.2.1 Trusted DBMS Interpretation of the TCSEC (NCSC-TG-021)

Description. The Trusted Database Management System Interpretation of the TCSEC (TDI) [NCSC 91A] was developed by NCSC in 1991 in order to extend Orange Book security features, assurance requirements, and the evaluation rating structure to trusted applications and trusted DBMSs which support object sharing and require access controls. The TDI specifies security features that enforce accountability and access control, and it specifies criteria for assurance and documentation in the same manner that TCSEC does.

Status. The TDI was published two years ago with a statement that it will be used for at least one year so that NCSC could gain experience and revise the document. It has not been updated or augmented with a Companion Document Series yet, but is being followed extensively and is considered to be fairly stable.

Another NCSC document, the Trusted Database Evaluation Criteria (Gray Book), also provides security guidance for the development of DBMSs. The Gray Book is classified.

Security Services. Secure applications and DBMSs implemented in accordance with TDI criteria will provide some or all of the following security services:

- User Identification and Authentication
- Discretionary Access Control
- Mandatory Access Control
- Labels
- Trusted Path
- Audit
- Object Reuse
- Service Assurance

The TDI is concerned primarily with confidentiality and reliability. It considers integrity of the system, but does not consider data integrity services.

4.1.2.2 Reference Model of Data Management (ISO 10032)

Description. According to the Guide to Open Systems Security, "The Reference Model of Data Management [ISO 93J] describes access control in terms of privileges, provides an architectural model of access control whereby access control data is considered in a similar way to database data, and lists a standardized approach to access control as a technical objective associated with data management standardization. Access control is the only security service supported within the scope of data management, although requirements for other security services external to data management are identified." [ISO 92A]

The basic security requirements are identified as preservation of confidentiality and integrity while maintaining availability. Access control is described in terms of discretionary, mandatory, and role-based mechanisms.

Status. The Reference Model of Data Management is an international standard. The latest version is 1993. Additional security-relevant changes were suggested in December 1993, including the addressal of multilevel security for DBMSs and the handling of multimedia data types.

Security Services. The Reference Model of Data Management addresses the following security service:

- Identification and Authentication
- Discretionary Access Control
- Mandatory Access Control
- Data Integrity
- Data Confidentiality
- Trusted Path
- Audit
- Labels
- Covert Channel Protection
- Service Assurance.

4.1.2.3 Relational Database Standard Query Language (FIPS 127-2)

Description. The Database Language Standard Query Language (SQL) Standard, FIPS PUB 127-2 [NIST 93N], specifies data definition, view definition, diagnostics management, transaction management, connection management, session management, access control, integrity constraints, and support for an international character set. In addition, it specifies two methods of programming language binding (Module and Embedded) for seven of the most common programming languages, and it specifies four conformance levels: Entry SQL, Transitional SQL, Intermediate SQL, and Full SQL. Internal mechanisms provide for discretionary access control and integrity of the database. However, the standard does not consider sensitivity labeling or mandatory access control. Standardization on a single database language is supportive of security in general, particularly in an open environment.

Status. Database Language SQL Version 3, FIPS PUB 127-2, became effective December 3, 1993. SQL and Information Resource Dictionary System (IRDS) are the standards specified by FIPS PUB 151-2, POSIX, to work in parallel to provide the DBMS applications portability profile (APP).

Security Services. The Database SQL Standard supports the following security services:

- Discretionary Access Control
- Data Integrity.

The standard does not consider sensitivity labeling or mandatory access control.

4.1.2.4 Remote Database Access (ISO 9579-1)

Description. The Remote Database Access (RDA) specification [ISO 93H] is used to establish a remote connection between an RDA client, acting on behalf of an application program, and an RDA server, interfacing to a process that controls data transfers to and from the database. The RDA protocol defines a data manipulation language which is used by the RDA server to accept the user request and translate it into the specific DBMS's language to manipulate the data. It allows the interconnection of database applications among heterogeneous environments by providing standard OSI application layer protocols to establish a remote connection. RDA can be specialized to any specific database type.

The RDA specification consists of two parts: part 1 specifies the Generic Model, Service, and Protocol, and part 2 specifies the SQL Specialization. These are the basis for OSI Implementors' Agreements on an RDA SQL Application Service Element (ASE) and its application content.

RDA carries the user identity and authorization identity in the request when an RDA dialogue is being set up with a remote node. The user identity and authorization are authenticated and validated before a dialogue is granted. The format, content, and significance of the security information are implementation-specific and are not dictated by RDA.

Status. The RDA specification became an international standard in 1993 and is a candidate for inclusion in GOSIP Version 3 or 4. The RDA protocol is not complete and has not yet been implemented in industry. However, it is compatible with the open systems philosophy and has been viewed favorably within both industry and the standards bodies. It will likely be widely implemented.

In the future, the RDA model will be harmonized with the Transaction Processing protocol (currently under development within the NIST OSI Implementors' Workshop) so that the RDA specification can be extended to include a distributed database capability.

Security Services. The RDA provides a structure for mechanisms to implement the following security services:

- Identification and Authentication
- Discretionary Access Control
- Mandatory Access Control
- Labeling.

4.1.2.5 Information Resource Dictionary System Services Interface (ISO 10728)

Description. The Information Resource Dictionary System (IRDS) (FIPS PUB 156 and ISO 10027) is a framework that specifies facilities for documenting an organization significant data and data processing resources in data dictionary systems and databases. The Services Interface (ISO 10728) provides an application program interface to the IRDS which allows metadata interchange between application programs and information resource dictionaries (IRDs) and DBMSs.

The standards require IRDSs to provide access control mechanisms and they characterize the criteria for access control decisions.

Status. Both the IRDS framework [NIST 89A] and the IRDS Services Interface [ANSI 92A] are international standards. The IRDS framework, FIPS PUB 156, is currently being updated. IRDS and SQL are the standards specified by FIPS PUB 151-2, POSIX, to work in parallel to provide the DBMS applications portability profile (APP).

Security Services. The IRDS framework and IRDS Services Interface provide for the following security service:

- Discretionary Access Control.

4.1.2.6 MLS/Trusted DBMS Security Standards

Description. A significant feature of relational databases is that they are easily shared by users who have no need or right to view all of the data contained in the database. To allow sharing, access controls must be installed that provide users with the ability to access all of the information to which they are entitled, and no more. Furthermore, it the database contains classified information and some users are cleared to access only information that is classified at a level below the highest classification in the database, a multilevel secure (MLS) DBMS is required to control access based on subject and object sensitivity labels.

Numerous threat scenarios have been described during the course of multilevel DBMS development efforts over the past 10 years which amplify the difficulty of securing a database. Often, mechanisms that will counter such threats also restrict access beyond what is required in the security policy so that some users are not allowed to access information to which they have a legal right. Progress is being made and multilevel DBMSs are within sight. These DBMSs will still have vulnerabilities that, for the time being, will have to be quantified and accepted. In particular, there remains some potential for inference, especially when the database is sparsely populated. Also, the concept that an aggregate of information will be classified at a level which is higher than the classifications of the individual data items has not been solved. While this is an implementation-specific problem, it is a universal problem for all sensitive and classified databases and should be solved with a standard mechanism.

Status. There are currently no formal standards for multilevel or trusted database management systems. There are multilevel DBMSs rated B1, and one rated B2, under the TDI criteria. However, there are none that are rated at the A1 level. Several development efforts have been underway for more than 10 years and products are expected within the next few years.

The International Federation of Information Processing (IFIP) Working Group 11.2 is currently developing standards for secure DBMSs. ANSI and ISO are developing an SQL3 specification with features for managing complex objects in heterogeneous environments. The SQL3 standards are expected in 1996. [NIST 93E]

Security Services. MLS/Trusted DBMSs will provides the following security services:

- Identification and Authentication
- Discretionary Access Control
- Mandatory Access Control
- Labeling
- Data Confidentiality
- Data Integrity.

4.1.3 Graphical User Interface Standards

Guidance documents and standards related to graphical user interfaces (GUI) are discussed in the order shown on Table 4.1-2. Their ordering was arranged according to following sequence:

- **GUI Applications Portability Profiles (APP)**
- **GUI Toolkits** which implement an APP for developing portable applications
- **Application Programmer's Interfaces (API)** for portable graphics programs
- **Interoperability standards** for the interchange of graphics data
- **GUI security standards.**

4.1.3.1 User Interface Component of Applications Portability Profile (X Window) (FIPS PUB 158)

Description. The MIT X Window System is the Federal standard [NIST 90D] for GUIs in the open systems environment. Its client-server architecture allows the X client application to run on one system while the X server runs on another system over a network. Applications built to X Window specifications (using toolkit interfaces) can communicate with users in a distributed environment without being concerned about the underlying display hardware. A user on any machine can access an application on any other machine without concern for where the application is running or whether it is compatible. [SLONE 91]

Status. Version 2, FIPS PUB 158-1, was announced in 1992 is expected to be published soon. It is the standard specified by FIPS PUB 151-2, POSIX, for the GUI applications portability profile (APP).

Security Services. The User Interface Component of the Applications Portability Profile provides no security services. However, display standardization is supportive of security in general, particularly in an open environment. Applications that are built around the X Window user interface will provide implementation-dependent security services.

4.1.3.2 X Window System Graphical User Interface – Part 1: Modular Toolkit Environment (IEEE P1295.1)

Description. The X Window System Graphical User Interface–Part 1: Modular Toolkit Environment, IEEE P1295.1, is a GUI toolkit that supports writing portable applications with GUIs based on X Windows. The X Window GUI Toolkit is based on Open Software Foundation's MOTIF, the *de facto* interface standard. Even vendors with proprietary products, such as DECwindows and SUN OpenView, offer MOTIF capabilities for compatibility.

Status. IEEE P1295.1 is in draft status and is expected to become a standard in 1994.

Security Services. The IEEE P1295.1 GUI toolkit provides no security services. However, applications that are built around the X Window user interface using the GUI toolkit can provide implementation-dependent security services. An example of a system with GUI security services is the Compartmented Mode Workstation which incorporates sensitivity labels to indicate the maximum user sensitivity level for the session and information labels to indicate the sensitivity of the data being accessed. Management information used to display the labels is also used to make access control decisions. However, the display labels do not enforce the access control policy.

4.1.3.3 Uniform Application Program Interface – Graphical User Interface (IEEE P1201.1)

Description. The Uniform Application Program Interface–Graphical User Interface (IEEE P1201.1) is a proposed GUI toolkit for a broad range of non-X-Window technologies. [NIST 93E] It will have the same properties as the X Window GUI Toolkit, except that it will support writing portable applications with GUIs that are not based on X Windows.

Status. A draft of IEEE P1201.1 will be available for evaluation in 1994.

Security Services. IEEE P1201.1, like IEEE P1295.1, will be a GUI toolkit and as such will not provide any security services. However, applications that are built using the GUI toolkit can provide implementation-dependent security services, primarily in the area of security labeling.

4.1.3.4 Graphics Kernel System (FIPS PUB 120-1)

Description. The Graphics Kernel System (GKS), FIPS PUB 120-1 [NIST 91C], is an application programmers interface (API) standard that specifies a toolbox (e.g., library) of subroutines for an application programmer to incorporate within a program. GKS provides the interface for programming two-dimensional (2D) graphics applications in a device-independent manner.

Status. GKS became an international standard (ISO 7942) and was published as FIPS PUB 120 in 1985. Version 2, FIPS PUB 120-1, was published in 1991. A full range of products and tools based on GKS is currently on the market.

Security Services. GKS provides no security services. However, as discussed above, standardization in general is supportive of security, and applications that are developed in an open environment can provide implementation-dependent security services.

4.1.3.5 Programmer Hierarchical Interactive Graphics System (FIPS PUB 153)

Description. The Programmer Hierarchical Interactive Graphics System (PHIGS), FIPS PUB 153 [NIST 88], is another API standard, similar to GKS. PHIGS provides the interface for programming real-time interactive 2D and three-dimensional (3D) graphics applications and hierarchical database structures in a device-independent manner. PHIGS applications include computer-aided design, computer-aided engineering, computer-aided manufacturing, command and control systems, modeling, and simulation.

Status. PHIGS became an international standard (ISO 9592) and was published as FIPS PUB 153 in 1988. A full range of products and tools based on PHIGS is currently on the market.

Security Services. PHIGS provides no security services. However, as discussed above, standardization in general is supportive of security, and applications that are developed in an open environment can provide implementation-dependent security services.

4.1.3.6 Computer Graphics Metafile (FIPS PUB 128-1)

Description. The Computer Graphics Metafile (CGM), FIPS PUB 128-1 [NIST 93P], specifies a file format for graphical data interchange in a device-independent manner. The standard facilitates the transfer of graphical information between different graphical software systems and devices.

Status. CGM became an international standard (ISO 8632) in 1992 and was published as FIPS PUB 128-1 which became effective October 15, 1993. CGM is the standard specified by FIPS PUB 151-2, POSIX, for the graphics data interchange applications portability profile (APP). CGM is a strong candidate for inclusion in GOSIP Version 3.

Security Services. Like the other graphics standards, CGM provides no security services, but is supportive of security in a general sense because applications that are developed in an open environment can provide implementation-dependent security services.

4.1.3.7 Initial Graphics Exchange Specification (FIPS PUB 177)

Description. The Initial Graphics Exchange Specification (IGES), FIPS PUB 177 [NIST 92K], specifies a file format for graphical data interchange in a device-independent manner. Where CGM transfers graphical pictures, IGES transfers a graphical database of geometric, topological, and non-geometric data which can be processed to represent a picture. IGES is used by computer-aided design and computer-aided manufacturing (CAD/CAM) systems.

Status. IGES is an ANSI standard. FIPS PUB 177 was published in November 1992 and is in wide use. No substantial changes are foreseen.

Security Services. Like the other graphics standards, IGES provides no security services directly.

4.1.3.8 Graphical User Interface Security Standards

Description. GUI security implementations, such as the Compartmented Mode Workstation (CMW) typically implement features for sensitivity labeling, information labeling, and trusted path. Documentation is generally classified or restricted and is not available as the basis for standardization.

Status. There currently exist no GUI security standards. With the rapid development of multilevel computer systems and networks, GUI security standards will be needed.

Security Services. GUI security standards will identify the following security services:

- Sensitivity Labeling
- Information Labeling
- Trusted Path.

4.1.4 Backplane Standards

Backplane standardization is an important area with regard to security. Information that is transferred between internal components of a host is transferred over the backplane. Information that is transferred between internal components and external interface devices is also transferred over the backplane. The backplane introduces the risk of corruption, disclosure, and denial of service even when the processors, peripherals, and communications channels are functioning correctly and securely. Standards for two types of backplanes are being developed:

- Traditional bus architecture
- High-Speed network of point-to-point interconnections.

Sample topologies for bus and network backplanes are shown in Figure 4.1-1. It should be noted that there are many different topologies for network backplanes.

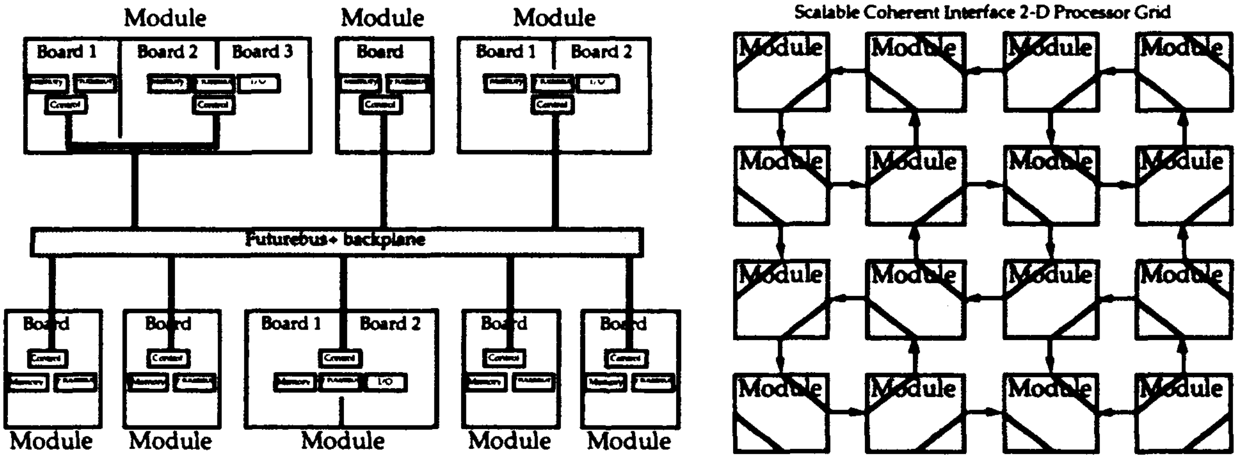

Figure 4.1-1. Bus and Network Backplane Topologies

4.1.4.1 Futurebus+ Recommended Practices (IEEE Std 896.3)

<u>Description</u>. Futurebus+ is a set of standards that provide a backplane architecture for a set of signal lines that constitute a multiple segment bus, and protocols for the interfacing of modules connected to the bus segments. Security considerations are discussed in Part 3, the Recommended Practices. The importance of Futurebus+ is two fold:

- Futurebus+ incorporates Futurebus, VMEbus, and Multibus efforts into a single backplane bus standard
- Futurebus+ supports an interface to the Fiber Distributed Data Interface (FDDI) which is the high-speed LAN technology selected for the SAFENET profile (see section 4.1.5.12).

Examples of modules that may connect to the bus are processors and cache, random access memory, and I/O interface to peripherals and communications. The Futurebus+ Standard contains the following physical layer profiles:

- Profile A – for a general purpose 64 bit or 128 bit bus that can be installed in systems ranging from desktops to small mainframes
- Profile B – for a bus to support I/O modules that interface to peripherals, Ethernet and FDDI channels, and bridges to other buses
- Profile F – for a high-speed bus to support high-speed memory and multimedia subsystems, multi-processor modules with high-speed cache, high-performance I/O modules, and bridges to other buses
- Profile M – for military systems
- Profile T – for telecommunications systems.

Primary security concerns are associated with physical protection and service assurance. For systems having a high level of risk, the standard recommends the chassis be locked and seals be installed to protect the backplane from direct access. Integrity and service assurance are provided through extensive fault management and component redundancy. An optional dual bus architecture can be provided for high performance and high availability. TEMPEST shielding is specified for high risk systems to protect against emanations.

Data confidentiality and integrity mechanisms are recommended for high risk systems to enforce mandatory and discretionary access control policies. Data confidentiality and access control services may be provided through encryption of data transfers over the bus with cryptographic mechanisms embedded in the system modules or bus interface logic. Another mechanism to transfer integrity check value information with the data is the Futurebus+ tag line. Security labels may be applied to the extended message header, the data field, or at the frame level to support mandatory access control decisions. Module identification numbers may be incorporated in the authentication exchange information. Traffic flow security involves generating dummy transmissions to mask the transmission rates among modules, and data padding to mask the duration of data transmissions.

Priority rules for competing modules trying to gain access to the bus are implementation-dependent, and are not mandated by the Futurebus+ standard. Flow control is provided in the Futurebus+ protocol to prevent the loss of information due to problems such as varying buffer sizes.

Status. IEEE developed the initial Futurebus standards (896.1 and 896.2) in 1987. In 1988 and 1989 the VMEbus International Trade Association (VITA) and the Multibus Manufacturers Group (MMG) agreed to join forces with IEEE and merge their VMEbus and Multibus efforts with that of Futurebus to create a single united standard.

IEEE revised the Futurebus standards in 1992 [IEEE 92A AND 92B] and renamed the program Futurebus+ to reflect the universal position. IEEE 896.1 was combined with 896.1a-1993 and became International Standard ISO 10857 in 1994 [ISO 94F]. Unapproved draft Recommended Practices were published in 1992 as P896.3. [IEEE 92C] The draft Futurebus+ Conformance Test was published as IEEE P896.4 in 1993. The draft Military Profile, IEEE P896.5, was also published in 1993.

A military standard (MIL-STD-2205) is being developed, but a draft has not yet been published. It will refer the military community to IEEE 896.5. There are no plans to develop a military handbook as a companion to MIL-STD-2205. However, the Futurebus+ community uses IEEE 896.3, Recommended Practices, as a handbook.

Security Services. The Futurebus+ standard provides guidance for installing mechanisms to provide the following security services:

- Authentication
- Discretionary Access Control
- Mandatory Access Control
- Labeling
- Object Reuse
- Data Confidentiality
- Traffic Flow Confidentiality
- Data Integrity
- Service Assurance
- TEMPEST.

4.1.4.2 High Speed Data Transfer Network

Description. With the development of gigabyte processor chips and parallel processing, a bus architecture has insufficient bandwidth for high-performance computer systems. The high speed data transfer network (HSDTN) introduces a point-to-point interconnection architecture for internal communications between computer modules. [IEEE 93B] It consists of two components:

- Data Channel
- Shared Memory Paradigm.

No single standard has been identified yet for the data channel. The standard developed for the shared memory paradigm is a suite of packet protocols, called *the Scalable Coherent Interface* (SCI), IEEE Std 1596-1992, to form an interconnect system that scales well as the number of attached processors increases, provides a coherent memory system, and that defines a simple *interface* between modules.

The purpose of the SCI is to facilitate assembly of processor, memory, I/O, an bus adapter cards from multiple vendors into massively parallel systems with unidirectional point-to-point transmission throughputs in excess of 1012 operations per second. SCI can connect up to 64,000 nodes and allows interconnection configurations to range from simple rings to complex multistage switching networks. The media may be fiber optic or coaxial cable. In addition, SCI is designed to cope easily with transmission protocols of different speeds.

Transactions are performed by sending packets from a queue in one node to a queue in another. The packet contains address, command, and status information in the header, optional data, and an integrity check value. Some of the fields are reserved for future use and could be assigned for security services. Packets are padded to a standard size which coincidentally supports traffic flow security. Reliability and availability are strongly supported through the use of control and status registers, error detection and isolation, and fault recovery.

An interface has been developed for connecting SCI and Futurebus+ backplanes within a computer. This was done to provide a migration path, but has the side effect of providing future opportunities for expansion.

Status. The HSDTN is still in the development phase. Its data channel component has not been identified. The Scalable Coherent Interface was selected as the shared memory paradigm. The SCI standard has been developed by IEEE in cooperation with CERN in Europe and published in 1992. A standard for the data channel has not been identified. Security for the SCI or the HSDTN has not been considered to the depth that it has for Futurebus+. However, these issues are being addressed.

IEEE Std 1596-1992 is supported by six other documents: 1596.1, SCI Bridges; 1596.2, Kiloprocessors Extensions; 1596.3, Low Voltage Differential Signals; 1596.4, RAM Link; 1596.5, Data Transfer Formats; and 1596.6, SCI Real Time.

There is no military standard for the SCI, and it has not been determined if one will be developed. If one is written, it is expected that it will recommend the use of IEEE 1596 when possible, and the use of IEEE 1596.6 when there is a concern about real-time processing, fault tolerance, and other issues. Currently, IEEE has not published 1596.6. IEEE plans to standardize the Canadian Navy's "SCI Real Time" document published in 1992. There are no plans to develop a military handbook.

Security Services. The SCI establishes point-to-point connections which inherently provides authentication, access control, and data confidentiality without additional mechanisms. However, additional mechanisms are needed when two communicating nodes are not adjacent and an intermediate node must perform store-and-forward services. The SCI protocols include integrity checking. While the SCI standard does not directly discuss security, the mechanisms described support the following security services, though not as well as would be desired:

- Authentication
- Discretionary Access Control
- Service Assurance.
- Data Confidentiality
- Data Integrity

Other services discussed in the Futurebus+ standard could be added to the SCI and HSDTN standards in the future. Those may include:

- Mandatory Access Control
- Labeling
- TEMPEST.
- Traffic Flow Confidentiality
- Object Reuse

4.1.5 Network Standards

Guidance documents and standards related to networks are discussed in the order shown on Table 4.1-2. Their ordering was arranged according to the following sequence:

- **Evaluation criteria and guidelines**
- **Profiles** consisting of selected lists of standards and specifications
- **Architectures** that define placement of security services and mechanisms
- **Frameworks** that define basic concepts for a security mechanism that may be available in many layers
- **Security models** that address implementation of services at particular layers
- **Standards that specialize models** to serve as protocol construction tools
- **Military profiles** for lower layer protocols
- **Lower layer security protocols**
- **Upper layer security protocols and mechanisms.**

Many of the standards related to networks have been finalized in the past year or are still undergoing revision. Most have not yet been widely implemented, and are therefore not stable. Vendors hesitate to implement products based on draft standards because standards often undergo significant revision when being upgraded from draft to international standard status. Even when standards are finalized, they are not stable. Standards bodies are often under tremendous market pressure to have standards produced as soon as possible. Furthermore, as Marshall Rose points out, "Unless OSI implementors begin prototyping during the standards process, then there is very little confidence that the resulting international standard will be workable." [ROSE 90] Stability comes when the standards have been implemented and there is little technological pressure to change them. Major flaws requiring correction may be discovered during implementation.

In the interest of interoperability, the government has established requirements for system designers to implement standards that are accepted Internationally. However, since many of the International Standards are not stable, existing standards that are more widely implemented (e.g., Transmission Control Protocol, Internet Protocol, Security Protocol 3, Security Protocol 4, Simple Network Management Protocol, and others) may be used in the interim.

4.1.5.1 Trusted Network Interpretation of the TCSEC (NCSC-TG-005)

Description. The Trusted Network Interpretation of the TCSEC (TNI) [NCSC 87] was developed by NCSC in 1987 in order to:

- Extend Orange Book security features, assurance requirements, and the evaluation rating structure to networks
- Describe additional security services needed for networks.

The TNI specifies security features that enforce accountability and access control, and it specifies criteria for assurance and documentation, in the same manner that TCSEC does. However, the TNI describes more extensive security features such as communications integrity, transmission security, and service assurance.

A side effect of the TNI should be noted. TCSEC and the TNI require that system developers maintain a security policy for the system which sets the criteria for providing security services. TCSEC and the TNI also require the developers to verify that the top level specification complies with the security policy. In order to verify compliance, the security policy must be stated mathematically for higher level evaluation classes, e.g., in a security model. Models generally refer to a lattice of security levels which may be DoD classification levels, integrity levels, or something more comprehensive which incorporates both.

The models that are used for host systems are not adequate for networks, particularly for multilevel networks, because they are too restrictive. The Bell-LaPadula model is an access control model that is not supportive of communications between subjects operating at different levels. It is suitable for host systems where users operating at different security levels have little or no need to share information. In a network, hosts that operate at different levels may need to communicate extensively. Less restrictive models are required. The Honeywell Secure Communication Processor (SCOMP), for example, was verified using a variation of the Feiertag-Levitt-Robinson security model, which is based on flow control. The Goguen-Meseguer model is an early example of a non-interference model based on information theory which can be applied to networks. The Clark and Wilson model is an integrity model which complements the confidentiality aspects of other models. The Biba integrity model is the inverse of the Bell and LaPadula model in that it states that data items exist at different levels of integrity, and that the system should prevent lower level data from contaminating higher level data. [CLARK 87] Various authentication models have been developed. Two examples are the Sidhu model and the Varadharajan model. [MUFTIC 93]

The point to this discussion is that each secure system implementation requires a unique security policy, and accordingly, a unique security model. The NCSC has published A Guide to Understanding Security Modeling in Trusted Systems which is intended to aid developers in understanding modeling requirements in both the host system and the network environments.

Status. The TNI was published seven years ago, and has not changed since. It is considered as stable as the Orange Book.

Security Services. Networks implemented in accordance with TNI criteria will provide some or all of the following security services:

- User Identification and Authentication
- Peer-Entity Authentication
- Data Origin Authentication
- Discretionary Access Control
- Mandatory Access Control
- Labels
- Service Assurance
  - Continuity of Operations
  - Protocol-Based Protection
  - Network Management
- Trusted Path
- Audit
- Non-Repudiation
- Object Reuse
- Data Confidentiality
- Traffic Confidentiality
- Selective Field Integrity
- Selective Routing

4.1.5.2 Government Open Systems Interconnection Profile (FIPS 146-1)

Description. The Government Open Systems Interconnection Profile (GOSIP) [NIST 91B] defines a common set of data communications protocols that enable systems developed by different vendors to interoperate and the users of different applications on those systems to exchange information. GOSIP is based on implementation agreements developed by the NIST/IEEE-sponsored Open System Environment (OSE) Implementors' Workshop (OIW), and on national and international standards. Use of GOSIP protocols is mandatory for Federal Government procurements.

Version 1, issued in 1988, supported Message Handling System (MHS) electronic mail, File Transfer, Access, and Management (FTAM) applications, and protocols for interconnection of X.25, 802.3, 803.4, 802.5 network technologies. Version 2, issued in 1991, added the Virtual Terminal application and protocols for end system to intermediate system connection, connection-oriented services, connectionless services, and Integrated Services Digital Network (ISDN) technologies.

Versions 2 discusses security only as an option. It refers extensively to ISO 7498-2 for placement of security services. GOSIP states that access control and non-repudiation services may be implemented only at layer 7, and authentication, confidentiality, and integrity services may be implemented in layers 3, 4, and 7. GOSIP defers security services at layer 2 until the IEEE 802.10 Standard for Interoperable LAN and MAN Security (SILS) is approved. FIPS PUB 113 is referenced for data authentication, and FIPS PUB 171 is referenced for key management using ANSI X9.17, the Financial Institution Key Management standard.

Version 3, to be issued soon, is expected to include the following functions, protocols, and network technologies:

- Protocols for Security at Layers 2, 3, and 4
- Fiber Distributed Data Interface (FDDI)
- Frame Relay
- Intermediate System-Intermediate System (IS-IS) Routing
- Inter-Domain Routing Protocol (IDRP)
- Connectionless Upper Layer Service
- Network Management
- X.500 Directory Service Applications
- X-Windows Over OSI
- Remote Database Access (RDA)
- Security enhancements to mail applications.

Status. GOSIP Version 2 has been mandated for use by Federal Government agencies since 1992. GOSIP Version 3 will reference the services and protocols contained in the Industry and Government Open Systems Specification (IGOSS). Both GOSIP Version 3 and IGOSS were scheduled for release in late 1993. GOSIP Version 3 will be mandated in 1995.

Security Services. GOSIP recommends optional applications and protocols to provide some or all of the following security services:

- Authentication
- Confidentiality
- Integrity
- Access Control
- Non-Repudiation
- Key Management.

4.1.5.3 Government Network Management Profile (FIPS PUB 179)

Description. The Government Network Management Profile (GNMP), FIPS PUB 179 [NIST 92C], specifies the common management information exchange protocol and services, specific management functions and services, and the syntax and information required to support monitoring and control of the network and system components and their resources. GNMP, as GOSIP, is based on NIST OIW implementation agreements, and on national and international standards. The goal of network management is to provide increased network performance, accessibility, and integration.

GNMP and GOSIP are interrelated profiles that cross-reference each other. GNMP is the standard reference for all Federal Government agencies to use when acquiring Network Management functions and services for computer and communications systems and networks. The Network Management Specification for DoD Communications (MIL-STD-2045-38000) builds on GNMP and augments GNMP with military-unique requirements. GNMP and the MIL-STD are companion documents for use when specifying military network management product procurements.

GNMP identifies five Specific Management Functional Areas (SMFAs): configuration management, fault management, performance management, security management, and accounting management. GNMP specifies the Common Management Information Protocol (CMIP) (ISO 9596-1, 1991) for exchange of management commands and information between two open systems. CMIP is an application layer protocol that specifies the structure of the management messages and how they are transferred from one open system to another. The Common Management Information Service (CMIS) (ISO 9595, 1991) specifies the service interface to management information service users. The network manager manages the managed objects that represent these protocols and services.

CMIP and CMIS are international standards, but are not yet widely installed. The Simple Network Management Protocol (SNMP) was developed by the Internet Engineering Task Force (IETF) as an interim protocol to provide some interoperability. SNMP is intended to be upward compatible with CMIP and is installed on many systems. CMIP is growing in popularity wherever OSI is embraced. [MICHAEL 93] GNMP's view of SNMP in the future is that SNMP will remain useful as an internetwork management protocol that fits into a network management architecture for the purpose of managing sets of routers.

Status. Concepts for network management were first standardized when the ISO Open Systems Interconnection Reference Model (OSI RM) Part 4, Management Framework, became an international standard (ISO 7498-4) in 1989. GNMP builds on the framework and is being developed in three phases so that it will progress as technology progresses. FIPS PUB 179, published in December 1992 is the initial version. Version 2 will expand the network management functions and may include stronger access control and other security functions. Version 2 is scheduled for publication in mid-1994. Version 3, the final planned version, will primarily be a reference to IGOSS, and will be issued two to three years after Version 2. Versions 2 and 3 will be backward-compatible with existing implementations.

Security Services. Version 1 of GNMP provides the following security services:

- Peer-Entity Authentication
- Security Audit and Alarm
- Discretionary Access Control.

Two modes are provided for authentication. Mode 1 requires use of usernames and passwords for authentication. Mode 2 provides additional security by using a hash function applied to the password. The Secure Hash Algorithm (SHA) and other hash algorithms, such as Message Digest 5 (MD5), are suggested. A timestamp may also be included so that the password hashes to a different value each time.

The following services, not included in GNMP Version 1, are planned for future versions:

- Data Origin Authentication
- Connectionless Confidentiality
- Connectionless Integrity
- Non-Repudiation.

4.1.5.4 Network Management for DoD Communications (MIL-STD-2045-38000)

Description. The Network Management for DoD Communications (MIL-STD-2045-38000) [DoD 93A] specifies the requirements for DoD network management product procurements. MIL-STD-2045-38000 directs procurement officials to the FIPS PUB 179 (GNMP), and is a companion document to GNMP in that it provides guidance for DoD's implementation of GNMP. Network management assists in providing security services for service assurance and penetration resistance.

GNMP network management is intended to be a complete profile, specifying all that is necessary to assure interoperable network management system products. It includes consideration for configuration management, fault management, performance management, security management, and accounting management. MIL-STD-2045-38000 adds detail concerning requirements and functionality is areas such as the human-machine interface, automated analysis, network management system database characteristics, and performance requirements.

Status. MIL-STD-2045-38000 supersedes MIL-STD-1813 [DoD 91] which was never finalized. The latest version of the preliminary working draft of MIL-STD-2045-38000 was published in January 1993. Since January 1993, the draft standard has undergone considerable change and will be published as another working draft in 1994, probably under the same identification number.

The support document to MIL-STD-2045-38000 is the Military Handbook (MIL-HDBK-1351) [DoD 93B] which augments the MIL-STD with much detail about the current state of protocols and standards. The preliminary working draft of MIL-HDBK-1351 was published in late-1993 and is undergoing considerable change. However, it is in a more stable state than is the MIL-STD. The intent of the MIL-HDBK is to serve as a *living document* that evolves as the standards and GNMP evolve.

Security Services. MIL-STD-2045-38000 specifies requirements for the following security services:

- User Authentication
- Access Control
- Security Audit
- Key Management.

4.1.5.5 OSI Reference Model Security Architecture (ISO 7498-2)

Description. ISO 7498 describes the Basic Reference Model for Open Systems Interconnection (OSI). Part 2, Security Architecture, became an international standard in 1989. It prescribes security controls needed to protect the information exchanged between application processes. It provides a general description of security services and mechanisms and defines where they should be placed within the Reference Model.

Status. ISO 7498-2 is the basis for ISO frameworks and security models, and is the reference for developing protocols needed to implement security services. ISO 7498-2 is well established and is referenced by GOSIP, GNMP, and the TNI.

ISO standards are reviewed every five years to determine if they should be updated. ISO 7498-2 was renewed without change in early 1994. It was reviewed and there were no Defect Reports from any national body, so it will stand for another five years. The IEEE 802.10, Standard for Interoperable Security (SILS) working group, proposed enhancements to the document domestically, but could not gain sufficient support within ANSI for the United States to submit a Defect Report. The basis of their proposal was to allow additional security services beyond confidentiality to be supported at the Data Link Layer. Opponents suggested that the Secure Data Exchange Protocol (SDE) which operates at layer 2 is for LANs only, whereas the overall OSI security architecture supports generic internetworks by placing the services at layers 3 and 4.

The European Computer Manufacturers Association (ECMA), a standards body similar to ANSI, has developed a model that deals with security in the context of complete open systems, rather than just communications. The document is ECMA 138, Security in Open Systems, Data Elements and Service Definitions. However, ECMA 138 addresses only authentication and access control. The ECMA model is more closely aligned with the ISO authentication and access control services. In addition, the terminology is not consistent with ISO 7498-2. ECMA 138 concepts will not be incorporated into ISO 7498-2, nor will ECMA 138 compete with ISO 7498-2. However, it's concepts of security domains, interdomain facilities, and Privilege Attribute Certificates are being adopted in other standards such as the Integrated Services Digital Network (ISDN). [NIST 91A]

Security Services. ISO 7498-2 identifies the following security services:

- Access Control
- Peer-Entity Authentication
- Data-Origin Authentication
- Connection Confidentiality
- Connectionless Confidentiality
- Selective Field Confidentiality
- Traffic Flow Confidentiality
- Connection Integrity with Recovery
- Connection Integrity without Recovery
- Connectionless Integrity
- Selective Field Connection Integrity
- Selective Field Connectionless Integrity
- Non-Repudiation with Proof of Origin
- Non-Repudiation with Proof of Delivery

4.1.5.6 Security Frameworks for Open Systems (ISO 10181)

Description. Security Frameworks for Open Systems are being developed jointly as International Telecommunications Union, Telecommunications Sector (ITU-T, formerly CCITT) Recommendations and as a multipart International Standard. [ISO 92B, 93A, 93B, 93C, 93K, 93L, and 94E] The frameworks address security services by defining the means of providing protection for systems, objects within systems, and interactions between systems. This includes databases, distributed applications, open distributed processing, and open systems interconnection (OSI). Frameworks define basic security concepts, possible classes of mechanisms, services for those classes of mechanisms, functional requirements for protocols, and general management requirements.

Security frameworks are not concerned with specific implementations or methodologies for mechanisms. Other standards can use the frameworks by incorporating concepts and providing specific security services and mechanisms.

The International Standard, ISO 10181, will consist of the following parts:

- Part 1: Security Frameworks Overview
- Part 2: Authentication Framework
- Part 3: Access Control Framework
- Part 4: Confidentiality Framework
- Part 5: Integrity Framework
- Part 6: Non-Repudiation Framework
- Part 7: Security Audit Framework
- Part 8: Guide to Open Systems Security.

Status. Each part of the security frameworks is a separate document. The status of the individual documents is as follows:

- Part 1: Security Frameworks Overview (CD 10181-1.2): Failed second committee draft ballot in 1993 and requires some changes before progressing to draft international standard (DIS) status. This framework will progress to DIS status after all other frameworks are stable, probably in July 1994.
- Part 2: Authentication Framework (DIS 10181-2): The DIS was balloted in late 1993. The authentication framework is expected to become an International Standard in early 1994.
- Part 3: Access Control Framework (CD 10181-3.2): This was advanced to DIS status in January 1994 and went out for six month ballot. It is expected to become an international standard in 1995.
- Part 4: Confidentiality Framework (DIS 10186-4): The first committee draft (CD) ballot passed in June 1993 and the framework advanced to DIS status. International comments are being incorporated by ANSI (the editor is from NIST). Because of instability, it will probably not become an international standard until 1996.
- Part 5: Integrity Framework (DIS 10186-5): Same editor and status as the Confidentiality Framework.
- Part 6: Non-Repudiation Framework (CD 10181-6): The committee draft is currently undergoing major changes and will require another round of CD balloting before progressing to DIS status.
- Part 7: Security Audit Framework (CD 10181-7.2): The second committee draft ballot failed in September. The framework requires major changes and must be reballoted again before progressing to DIS status.
- Part 8: Guide to Open Systems Security (working draft 10181-8): The working draft was revised in May 1992 and has not progressed to CD status.

Security Services. The frameworks define the means for other standards to provide the following security services:

- Peer-Entity Authentication
- Data Origin Authentication
- Connection Integrity Without Recovery
- Connection Integrity With Recovery
- Selective Field Connection Integrity
- Connectionless Integrity
- Selective Field Connectionless Integrity
- Non-Repudiation With Proof of Origin
- Non-Repudiation With Proof of Delivery
- Key management.
- Discretionary Access Control
- Mandatory Access Control
- Confidentiality Labels
- Integrity Labels
- Connection Confidentiality
- Connectionless Confidentiality
- Selective Field Confidentiality
- Traffic Flow Confidentiality
- Security Audit

4.1.5.7 Security Labels Framework for the Internet (RFC 1457)

Description. The security labels framework [RFC 93A] is intended to help protocol designers determine what security labeling they should support. It identifies integrity labels and sensitivity labels which support data integrity and data confidentiality, respectively.

Operating systems label the data they process. These security labels are not part of the data, but attributes of the data. Since the security label is an attribute of the data, it should be bound to the data by the integrity security service or other mechanism that can preserve the binding.

The Internet Protocol Security Option (IPSO), described in MIL-STD-1777, was developed in 1983 to provide a way for hosts to send security level, compartmentation, handling restriction code, and user group parameters through subnetworks. IPSO was revised (RIPSO) and commercialized (CIPSO), and NSA has attempted to uniform labeling for commercial and defense requirements with the Common Security Label (CSL) approach. The labels framework extends these efforts by considering integrity, and by being applicable to protocols at all layers.

The framework discusses trade-offs to be made when determining how a particular network will perform security labeling. It allows both explicit and implicit labels to be used, and discusses methods that explicit labels can be implemented in the data link layer, the network layer, the transport layer, the session layer, the presentation layer, and the application layer. The framework allows security labels to be either connection-oriented or connectionless. Hybrid combinations of all of the above are also permitted.

Status. The labels framework is a memo which holds no status as an Internet standard, ISO standard, or DoD standard. However, the author, Russ Housley, is intimately involved in the label standardization efforts being accomplished by the IEEE 802.2 and 802.10 Working Groups, as well as the Standard Security Label for GOSIP being developed by NIST. The concepts of the labels framework are indicative of the standards that will follow.

Security Services. The labels framework supports the following security services:

- Discretionary Access Control
- Mandatory Access Controls
- Labels
- Data Confidentiality
- Data Integrity.

4.1.5.8 OSI Directory – Part 8: Authentication Framework (ISO 9594-8)

Description. The OSI Directory – Part 8: Authentication Framework (ISO 9594-8) is equivalent to the CCITT X.509 recommendation. The X.500 Directory System is a collection of open systems which cooperate to form a distributed database known as the Directory Information Base (DIB) for the internetwork. All users and hosts with appropriate access permissions can read and modify the directory. Two security services are recommended in X.509: an Access Control Framework and an Authentication Framework. Users are granted access to the DIB based on their access control rights, defined by the implementation-specific access control policy. Access control security services are also implementation-specific.

The Authentication Framework provides Entity Authentication for the Directory, applications, and system users. It specifies the structure of the authentication information, states assumptions on how the information is created and input into the Directory, describes how the information can be obtained, and defines uses for the information in performing authentication and other security services supported by authentication.

The Authentication Framework establishes two levels of authentication that could be implemented: Simple Authentication, which uses userid and password, and Strong Authentication, which uses public-key cryptography to form authentication certificates. Certificates are created by a Certification Authority and are held in the Directory as attributes in a manner that causes them not to lose their level of trust. No unique capabilities are required of the Directory in order to store or communicate user certificates in a secure manner.

Status. The Authentication Framework became an International Standard in 1990. The other parts of the Directory standard, ISO 9594, are:

- Part 1 – Overview of Concepts, Models, and Services
- Part 2 – Model
- Part 3 – Abstract Service Definition
- Part 4 – Procedures for Distributed Operations
- Part 5 – Protocol Specifications
- Part 6 – Selected Attribute Types
- Part 7 – Selected Object Classes.

All of the parts of 9594 are technically aligned with Recommendation X.500.

Security Services. The Authentication Framework provides the following security service:

- Entity Authentication.

4.1.5.9 OSI Lower Layers Security Model (Technical Report)

Description. Security Frameworks (discussed in section 4.1.5.5 above) each describe a general security service available in many layers. Models, on the other hand, address the implementation of services within particular layers and address the interaction between these layer services. They provide the specifics for protocols to follow.

The Lower Layers Security Model [ISO 93I] provides for the establishment of Security Associations (SAs) at layers 1 to 4 through the exchange of SA protocol data units (PDUs), or through out-of-band mechanisms. While lower layer security PDUs will follow a common general structure identified in the Model, they will not be identical due to format restrictions imposed by the protocol layers. However, security PDUs will have the following common aspects:

- Integrity Check Value (ICV) appended to the PDU
- Separate padding fields for traffic flow confidentiality, integrity, and encipherment
- Sequence numbering for integrity
- Flexibility in the encoding of fields.

The Model also defines the protection quality of service (QOS) parameter used to request or *indicate the security protection required or provided at an N-layer. Examples* of QOS parameters (not specifically mentioned in the Model) are speed requirements, reliability requirements, acceptable error rates, priority, and acceptable transmission delay times.

Status. The Lower Layers Security Model is currently in working draft status to become a Technical Report. It is being edited and is expected to be reballoted in July 1994 and be published as an International Technical Report late in 1994.

Security Services. The Lower Layers Security Model provides the structure for services to be provided by protocols such as the Secure Data Exchange Protocol (SDE), Network Layer Security Protocol (NLSP), or Transport Layer Security Protocol (TLSP). The Model specifically discusses the following security services:

- Connection Confidentiality
- Connectionless Confidentiality
- Traffic Flow Confidentiality
- Connection Integrity With Recovery
- Connection Integrity Without Recovery
- Peer-Entity Authentication
- Access Control
- Selective Routing
- Security Labeling
- Key Management.

4.1.5.10 OSI Upper Layers Security Model (ISO 10745)

Description. The Upper Layers Security Model is concerned with development of application-independent services and protocols in order to minimize the need for application-specific application service elements (ASEs) to contain internal security services. [ISO 94A]

The model specifies:

- Security aspects of communication in the upper layers
- Upper layers support of security services, as defined in the frameworks
- Positioning and relationships of security services and mechanisms in the upper layers, in accordance with ISO 7498-2 and ISO 9545
- Interactions among upper layers, and between upper layers and lower layers, in providing and using security services
- Upper layer requirements for security information management.

The model does not specify:

- Security service definitions
- Security protocol specifications
- Security techniques and mechanisms, their requirements, or their protocol requirements
- Provisions for security which are not concerned with OSI communications.

Status. The Upper Layers Security Model, to be assigned as ITU-T Recommendation X.803, became an international standard in November 1993 when the final text was accepted. It will be published as ISO / IEC 10745 in mid-1994.

Security Services. The Upper Layers Security Model provides the structure for services to be defined for the session, presentation, and application layers. The Model specifically discusses the following security services:

- Connection Confidentiality
- Connectionless Confidentiality
- Selective Field Confidentiality
- Connection Integrity With Recovery
- Connection Integrity Without Recovery
- Connectionless Integrity
- Selective Field Integrity
- Entity Authentication
- Data Origin Authentication
- Access Control
- Security Labeling
- Non-Repudiation, Origin
- Non-Repudiation, Delivery
- Key Management.

4.1.5.11 Generic Upper Layer Security Standard (DIS 11586)

Description. The Generic Upper Layer Security (GULS) Standard [ISO 93D, 93E, 93F, 93G] specializes some of the application layer concepts of the Upper Layers Security Model (ISO 10745) to permit the exchange of security-related information between application processes in a distributed environment. GULS defines generic facilities to support construction of Upper Layer security protocols. These generic security facilities do not in themselves provide security services, but are construction tools for protocols which will provide security services for the upper layers. GULS facilities include:

- A set of notational tools to support the abstract syntax specification of selective field protection requirements, and to support the specification of *security exchanges* and *security transformations*
- A service definition, protocol specification, and PICS proforma for an application service element to support security services provided in the Application Layer
- A specification and PICS proforma for security transfer syntax, associated with Presentation Layer support for security services in the Application Layer.

GULS consists of six parts, including what was previously the Security Exchange Application Service Element (SE-ASE) being developed by ISO. A service element (SE) is a primitive defined at the interface between two adjacent layers. An application service element (ASE) is a set of functions that support application programs. An ASE represents a type of work that the user expects to be performed, such as security exchanges, along with the elements needed to perform that work. The GULS parts are:

- Part 1: Overview, Models, and Notation
- Part 2: Security Exchange Service Element (SESE) Service Definition
- Part 3: SESE Protocol Specification
- Part 4: Protecting Transfer Syntax Specification
- Part 5: SESE Protocol Implementation Conformance Statement (PICS) Proforma
- Part 6: Protecting Transfer Syntax PICS Proforma.

Status. Parts 1 and 4 of the GULS standard being developed by ANSI were progressed from CD status at the ISO meeting in June 1993 and were published as draft international standards. They were distributed for ballot, with the ballot closing in the spring 1994. Parts 3 and 4 are in Final DIS Text status. All four are expected to advance to international standard status in mid-1994. The Protocol Implementation Conformance Statement (PICS) Proformas, parts 5 and 6, have not been developed yet.

The IEEE 802.10 (SILS) committee is using GULS as the key management infrastructure. The Open System Environment Implementors' Workshop (OIW) is assessing GULS for a variety of applications, including management and directory services.

The Corporation of Information Management (CIM), with support from NSA, is developing the Technical Architecture Framework for Information Management (TAFIM) which will include the DoD GULS Security Architecture (DGSA) as Volume 6. The DGSA was started by the Center for Information Systems Security (CISS, previously the Defense Information System Security Program (DISSP)). A draft of the DGSA (Volume 6 of the TAFIM) will be available in early 1994.

Security Services. GULS facilities will support protocols which provide the following security services required by applications:

- Entity Authentication
- Data Origin Authentication
- Traffic Flow Confidentiality
- Connection Confidentiality
- Connectionless Confidentiality
- Selective Field Confidentiality
- Non-Repudiation
- Discretionary Access Control
- Mandatory Access Control
- Labeling
- Connection Integrity
- Connectionless Integrity
- Selective Field Integrity
- Key Management.

4.1.5.12 Survivable Adaptable Fiber Optic Embedded Network (SAFENET) Standard (MIL-STD-2204)

Description. The Survivable Adaptable Fiber Optic Embedded Network (SAFENET) Standard, MIL-STD-2204 [SPAWAR 92C], provides requirements for the implementation of fiber optic local area networks for use in support of Naval mission critical computer resources. SAFENET is based on the Fiber Distributed Data Interface (FDDI) token ring technology. The SAFENET Standard provides for three network profiles:

- OSI profile - based on OSI protocols that conform to OSI Reference Model
- Lightweight profile - high performance transport and network layer protocols
- Combined profile - includes all SAFENET-defined protocols and services.

The following protocols and services are common to all three SAFENET profiles:

- Fiber Distributed Data Interface Protocol (FDDI)
- Logical Link Control Protocol (LLC)
- Connectionless Network Protocol (CLNP)
- Connectionless Transport Protocol (CLTP)
- ES-IS Routing Exchange Protocol
- IS-IS Intra-Domain Routing Protocol (optional in the lightweight profile)
- SAFENET Time Service (STS).

The following protocols are being added:

- Transmission Control Protocol (TCP)
- Internet Protocol (IP).

The SAFENET Network Development Guidance Military Handbook, MIL-HDBK-818-1 [SPAWAR 92D], includes an informative chapter on Security Guidance for developing secure SAFENET profiles. The Handbook discusses generic threats and generic services that should be implemented to counter the threats. The security architecture is driven by the threat exposure of the system, the security services that must be provided to counter those threats, and available security mechanisms to support those services [GRUMMAND 92]. The SAFENET Handbook suggests following ISO standards where possible to ensure open system interconnection. DoD protocols (TCP/IP) are included because they are widely implemented and stable, whereas the ISO standards are neither widely implemented nor yet stable. The Handbook discusses following GOSIP and SDNS when they are compatible with ISO standards. It also suggests use of

NLSP, TLSP, GULS, and OSI Network Management standards when they are mature and become international standards.

Status. Drafts of the SAFENET Standard, MIL-STD-2204, and SAFENET Handbook, MIL-HDBK-818-1 [SPAWAR 92D] were published in October 1992. The SAFENET Working Group continues to meet approximately six times per year. The latest drafts were distributed in January 1994. Final comments on the drafts are being accepted through February 1994 and the documents are expected to be finalized and published in the fall of 1994. The standard and handbook will be revised as technology and international standards progress sufficiently to merit update.

Security Services. The SAFENET Handbook requires no specific security services, but discusses potential services that should be implemented:

- Identity Based Access Control
- Rule Based Access Control
- Labeling
- Peer-Entity Authentication
- Data Origin Authentication
- Security Audit
- Connection-oriented Confidentiality
- Connectionless Confidentiality
- Traffic Flow Confidentiality
- Connection-oriented Integrity
- Connectionless Integrity
- Non-Repudiation of Origin
- Non-Repudiation of Receipt
- Service Availability.

4.1.5.13 Standard for Interoperable LAN / MAN Security (IEEE 802.10)

Description. Packet switched networks (PSNs) and wide area networks (WANs) were the architectural models used to develop ISO 7498-2 in 1989. Local area networks have since introduced new vulnerabilities associated with subnetworks and routing that were not present in the Data Link Layer of PSNs and WANs because of their point-to-point nature. The IEEE 802.10 Standard for Interoperable LAN and MAN Security (SILS) [IEEE 93A] is being developed to expand security services to protect LANs, even though security services exist at higher layers in the protocol stack. SILS consists of four parts:

- 802.10 Clause 1 – SILS Model
- 802.10 Clause 2 – Secure Data Exchange (SDE) Protocol
- 802.10 Clause 3 – Key Management Protocol
- 802.10 Clause 4 – Security Management.

Clause 1 provides an overview for security of local area networks and metropolitan area networks, defines terms, and provides an architecture which describes the relationship of each of the security protocols to the OSI Basic Reference Model (ISO 7498-2).

Clause 2 defines the Secure Data Exchange (SDE) Protocol to be implemented at the Data Link Layer, as part of the logical link control (LLC) sublayer. SDE augments standard LLC and media access control (MAC) communications protocols without replacing those protocols. An SDE-specific PDU encapsulates the LLC PDU and has optional elements and fields to satisfy a broad range of potential security applications. SDE requires no change to the existing upper-layer protocols in the stack. SDE will operate in LANs and MANs where not all stations use SDE. The SDE PDU has a clear header portion which includes a unique Link Service Access Point (LSAP) address to distinguish the SDE PDU from unprotected LLC PDUs.

SDE provides data confidentiality through encipherment. Connectionless integrity is provided through the use of an integrity check value (ICV). Data origin authentication is achieved through the use of the integrity service, or through the use of key management and the placement of a Station ID in the SDE protected header. Access control is provided by key management or system management. Access control decisions are based on the use of security associations. Access control is dependent on both integrity and authentication services.

SDE is not applicable to MANs using IEEE 802.6 isochronous and connection-oriented protocols (Distributed Queue Dual Bus Subnetworks), nor is it applicable to integrated services using the proposed P802.9 Integrated Services Interface at the Physical Layer. [IEEE 93A]

Clause 3 establishes a structure for key management to provide keying material and association attributes, represented as managed objects in the security management information base (SMIB), needed by security protocols at all layers. The Generic Upper

Layer Security (GULS) Standard services will be used to support SILS key management. The Security Exchange Service Element (SESE) defined in the GULS standard will support the key management attribute negotiation phase. Clause 3 allows asymmetric key management via X.509 certificates, use of the symmetric key management approach described in ANSI X9.17, and manual keying. Clause 3 will also address multicast key management.

Clause 4 describes management functions and protocols that support the security services provided in other clauses.

Status. The Standard for Interoperable LAN and MAN Security was published by IEEE in February, 1993. This initial version contains only Clause 2, the SDE protocol. The other three clauses will be added in future versions. A standard has been drafted by NSA and NIST which would add SDE to the SDNS suite of protocols. It will be called Security Protocol 2 for LANs (SP2L) within SDNS. [NIST 92F]

Clause 1 is currently undergoing considerable revision and will likely continue to do so until the other clauses are completed.

Clause 3 is controversial because one group feels key management belongs only in layer 7 while another group would like the option of installing key management at other layers so NLSP and TLSP could potentially perform key management internally. An agreement has been reached that recommends, but does not require, that key management be performed at layer 7. The first draft was presented to the SILS Working Group in November 1993. ISO has not drafted a proposal for a layer 7 key management protocol. The SILS Working Group would like to complete Clause 3 as quickly as possible in order to submit the document to ANSI for potential use as the ISO standard.

Clause 4 is based on the Common Management Information Protocol (CMIP), Common Management Information Service (CMIS), Simple Network Management Protocol (SNMP), and Simple Management Protocol (SMP). The first draft was presented to the SILS Working Group in November, 1993.

A Protocol Implementation Conformance Statement (PICS) Proforma will be developed when other efforts are close to completion. Discussions concerning the format of the SDE PDUs, security association ID values, placement of a security label in the protected header [IEEE 93E], and bootstrap SAIDs for key management are already underway.

Security Services. SILS provides the following security services:

- Access Control
- Data Origin Authentication
- Labeling (future)
- Data Confidentiality
- Connectionless Integrity
- Key Management.

4.1.5.14 Secure Data Network System (NISTIRs 90-4250, 90-4262, 90-4259)

Description. The Secure Data Network System (SDNS) was developed by the National Security Agency (NSA) in 1989 and published by NIST in 1990. [NIST 90A, 90B, 90C] SDNS provides an architecture and several protocols which are overlaid on the OSI communications protocol stack. NIST grouped NSA's original 10 documents into three documents for publication:

- NISTIR 90-4250 – SDNS Protocols
  - SDN.301 – Security Protocol 3 (SP3)
  - SDN.401 – Security Protocol 4 (SP4)
  - SDN.701 – Message Security Protocol (MSP) (for electronic mail)
  - SDN.702 – Directory Specifications for use with MSP
- NISTIR 90-4262 – Key Management Documents
  - SDN.601 – Key Management Profile
  - SDN.902 – Key Management Protocol - Definition of Service
  - SDN.903 – Key Management Protocol - Specifications for Protocol
  - SDN.906 – Key Management Protocol - Traffic Key Attribute Negotiation
- NISTIR 90-4259 – Access Control Documents
  - SDN.801 – Access Control Concept Document
  - SDN.802 – Access Control Specification

The SDNS protocols all work in a somewhat similar fashion by encapsulating Protocol Data Units (PDUs) in security envelopes. SDNS protocols augment standard communications protocols by adding security services without replacing the standard protocols. A protected header is appended in front of the PDU. The protected header optionally contains security labels, sequence numbers, NSAP addresses, or CLNP headers, depending on the specific protocol. An Integrity Check Value (ICV), computed from the protected header and the PDU, is added behind the PDU. The PDU, protected header, and ICV are optionally encrypted. A clear header is then prepended to the protected header so that the key can be identified.

The SP3 protocol provides connectionless network service with confidentiality, integrity, or both. SP3 also provides routing flexibility in internetworks. Connection-oriented network services are being added to SP3 to protect systems that do not utilize the ISO Connectionless Network Protocol (CLNP). SP3 can support host-to-host, host-to-gateway, and gateway-to-gateway services. The SP4 protocol provides host-to-host data protection for transport connections or for connectionless transmissions. With connection-oriented protection, each transport connection is individually protected with a different cryptographic key. SP4 can also be used to protect multiple host-to-host connections between a pair of end systems with a single cryptographic key for all host-to-host connections at a given classification level.

MSP was developed to support secure electronic mail transmissions when using the X.400 Message Handling System (ISO 8505-1). MSP provides connectionless confidentiality, connectionless integrity, data origin authentication, non-repudiation with proof of origin, access control for message transfer, and signed receipt request. When used in non-MHS applications, MSP provides connectionless confidentiality, connectionless integrity, user-to-user authentication, non-repudiation with proof of origin, user-to-user access control, and signed receipt request. The Directory System Specification for MSP augments the X.500 Directory System (ISO 9594) with support for key management functions.

MSP can be used with the ANSI conventions for Electronic Data Interchange (EDI) to provide secure exchange of EDI messages by encapsulating the message and adding a security header before submitting the message to the X.400 Message Transfer System. EDI is the computer-to-computer interchange of messages representing business documents. The primary application of EDI in the Federal Government is in procurements, including the receipt of bids and the issuance of purchase orders. Vendor payments may be combined with notification of payment via EDI.

The security protocols are heavily dependent on cryptographic key management and access control services. Key management in the application layer provides for the generation, distribution, and updating of traffic encryption keys (TEKs) for use by security protocols in any layer. The SDN.903 Key Management Protocol specification describes the services provided to the Key Management Application Process (KMAP) to support applications in a distributed open systems environment. Some management capabilities for authentication and access control are provided by the KMAP. [NIST 90B]

The access control documents describe the SDNS access control and authentication services. A trusted distribution algorithm, operating in conjunction with a trusted central authority, provides a means for an authenticated exchange of identity and attribute data between communicating peers. A means for local authorities to represent additional identity and attribute data without central authority involvement is provided. These capabilities support rule-based access control (RBAC) and identity-based access control (IBAC) mechanisms.

<u>Status</u>. SDNS was published in 1990 and has remained stable. Currently, NIST is considering adding the Transport Layer Security Protocol (TLSP) and Network Layer Security Protocol (NLSP) to SDNS. A specification has been drafted by NSA and NIST to include the IEEE 802.10 Secure Data Exchange (SDE) protocol in SDNS. Within SDNS, it will be called the Security Protocol 2 for LANs (SP2L). [NIST 92F]

Security Services. The SDNS protocols provide the following security services:

- Peer-Entity Authentication
- Data-Origin Authentication
- User-to-User Authentication
- Rule-Based Access Control
- Identity-Based Access Control
- Connection-oriented Confidentiality
- Connectionless Confidentiality
- Connection-oriented Integrity
- Connectionless Integrity
- Non-Repudiation with Proof of Origin
- Non-Repudiation with Proof of Delivery
- Key Management.

4.1.5.15 Network Layer Security Protocol (ISO 11577)

Description. The Network Layer Security Protocol (NLSP) [ISO 94B] provides the security services at Layer 3 which are not provided by standard communications protocols. Is does not replace standard communications protocols, but augments them. NLSP can be implemented in end systems and intermediate systems to provide end-to-end encapsulation or link encapsulation of higher level PDUs. Other primary functions beyond encapsulation are padding and connection authentication.

NLSP provides the option of performing an encipherment key or integrity key exchange. This would allow key management to be removed from the application layer. NLSP will also work with key management being performed for it externally. Before secure communication can be accomplished, a security association must be established in band or out of band and all association attributes must be agreed upon.

NLSP operates optionally at various subnetwork layers. For connection mode communications, NLSP operates above a subnetwork independent convergence protocol or subnetwork access protocol such as X.25.

For connectionless mode communication, NLSP can provide host-to-host service by being used as a subnetwork independent convergence protocol (SNICP) and operating above a connectionless network protocol which is also a SNICP. Interdomain routing protocol (IDRP) exchanges can be protected by placing NLSP below IDRP but above the connectionless network protocol. Intradomain routing exchanges cannot be protected by NLSP because it does not support multi-peer communications.

Status. NLSP became an international standard in November 1993 when the final text was accepted. It will be published in mid-1994. NLSP is being considered for inclusion in the Secure Data Network System (SDNS).

Security Services. NLSP, in conjunction with key management mechanisms and a connection-oriented or connectionless network protocol, provides the following security services:

- Peer-Entity Authentication
- Data Origin Authentication
- Discretionary Access Control
- Mandatory Access Control
- Labels
- Connection Confidentiality
- Connectionless Confidentiality
- Traffic Flow Confidentiality
- Connection Integrity Without Recovery
- Connectionless Integrity
- Key Management.

4.1.5.16 Transport Layer Security Protocol (ISO 10736)

Description. The Transport Layer Security Protocol (TLSP) [ISO 94C] can support all of the security services identified for the transport layer in the ISO RM Security Architecture (ISO 7498-2) through use of cryptographic mechanisms and security labeling. TLSP uses encapsulation of transport protocol data units (TPDUs) in conjunction with encipherment and an integrity check function to provide host-to-host connection or connectionless confidentiality and integrity services. Transport Protocol Class 4 (TP4) is capable of using checksums and sequence numbers to provide minimal connection oriented integrity service when TLSP is not needed to provide other security services. TLSP is capable of providing much stronger integrity assurance than TP4 through the use of the Secure Hash Algorithm (SHA), Message Digest (MD5), Data Encryption Standard (DES), or other mechanisms.

Encapsulation is performed by TLSP after all transport protocol processing is performed and prior to multiplexing and assigning the network connection. The integrity check function may or may not be cryptographically based, depending on user requirements. A security label can be associated with each encapsulated TPDU and security padding can be used to support cryptographic algorithm requirements for both confidentiality and integrity. Connection establishment PDUs can be exchanged to perform peer-entity authentication at the transport layer.

Status. TLSP became an international standard in November 1993 and will be published in mid-1994. It is being considered for inclusion in the Secure Data Network System (SDNS). An amendment to extend TLSP to permit peer entities to exchange the information needed for Security Association (SA) establishment and rekeying was also accepted in November 1993. [ISO 94D]

Security Services. TLSP, in conjunction with a connection-oriented or connectionless transport protocol, provides the following security services:

- Peer-Entity Authentication
- Data Origin Authentication
- Discretionary Access Control
- Mandatory Access Control
- Labels
- Connection Confidentiality
- Connectionless Confidentiality
- Connection Integrity With Recovery
- Connection Integrity Without Recovery
- Connectionless Integrity
- Key Management.

4.1.5.17 Standard Security Label for the GOSIP (Proposed FIPS PUB)

Description. The Standard Security Label for the Government Open Systems Interconnection Profile (SSL) [NIST 93R] specifies the security label for the GOSIP. GOSIP security labels carry information used by protocol entities to determine how to handle unclassified but sensitive data communicated between open systems. Information on a security label can be used to control access, specify protective measures, and determine additional handling restrictions required by a communications security policy.

The standard specifies the syntax for the labels and relies on a Computer Security Objects Register to provide the semantics. The separation of the label syntax from its semantics enables a single label format to support multiple security pclicies and facilitates cross-domain communications. Given the inherent differences in layer functionality the security label defined in the document is expressed both as an abstract label syntax specification for the OSI Application Layer and as an encoding optimized for the use at the Network Layer. The Application and Network Layers are the initial targets of GOSIP security. GOSIP will call for the use of this standard when optional security protocols at these layers require the use of security labels.

The label presented in the SSL defines security tags that may be combined into tag sets to carry security-related information. Five basic security tag types allow security information to be represented as bit maps, attribute enumerations, attribute range selections, hierarchical security levels, or as user-defined data.

Status. The draft Proposed FIPS PUB was published in September 1993 with the requirement that comments be returned by March 29, 1994. The standard is expected to be published as a FIPS PUB in late 1994.

Security Services. Security labeling provides or supports the following security services:

- Labeling
- Mandatory Access Control
- Audit
- Accountability.

4.1.5.18 Presentation Layer Confidentiality, Integrity, and Cryptography

Description. Amendments to the connection oriented presentation service definition (ISO 8822) and protocol (ISO 8823) are being developed to provide confidentiality and integrity services at the presentation layer in accordance with the confidentiality and integrity frameworks.

Another potential amendment would add cryptographic techniques to the presentation protocol in order to support the confidentiality and integrity amendments, and to provide peer-entity authentication at the presentation layer. This item will conform to the Upper Layers Security Model (ISO 10745) [ISO 94A] and the authentication framework (DIS 10181-2) [ISO 93A].

Status. The connection oriented presentation service definition and protocol amendments can be finalized in parallel with related efforts currently underway:

- The authentication framework is a draft international standard, and was expected to progress to international standard status late in 1993 or early 1994
- A future ISO standard governing upper layers authentication services is currently in working draft status and will support the cryptographic techniques amendment
- The confidentiality and integrity frameworks are still in committee draft status and are likely to progress to draft international standard status in 1994.

Security Services. The amendments provide the following security services at the presentation layer:

- Connection Integrity
- Selective Field Connection Integrity
- Connection Confidentiality
- Selective Field Connection Confidentiality
- Peer-Entity Authentication.

4.1.5.19 Message Digest Algorithms (RFCs 1319 and 1320)

Description. Message digest algorithms (e.g., hash algorithms) compute a fixed size representation of an input stream. Message digest algorithms have different performance characteristics and employ different computational techniques, making each suitable for different applications.

The MD2 Message Digest Algorithm (RFC 1319, RSA Data Security Inc., April 1992) [RFC 92A] employs traditionally accepted computational techniques and yields a relatively slow output. MD4 employs non-traditional computational techniques to enhance its speed in systems with native 32-bit arithmetic. The MD5 Message Digest Algorithm (RFC 1320, RSA Data Security Inc., April 1992) [RFC 92B] is based on the techniques of MD4, but provides additional security features to counter proposed attacks at the expense of slightly reduced speed. MD5 is still considerably faster than MD2.

Message digests will be used in Privacy-enhanced Electronic Mail (PEM) to provide message integrity. When the message digest is sealed with an asymmetric algorithm using the sender's private key, a digital signature is formed to provide authentication, and to support non-repudiation.

Status. MD2, MD4, and MD5 were developed for use over Internet and are referenced in the OIW Implementation Agreements. MD4 and MD5 are the basis for the Secure Hash Algorithm (SHA).

Security Services. Hash algorithms support mechanisms that provide the following security services:

- Data Integrity
- Data Origin Authentication
- Non-Repudiation.

4.1.5.20 Secure Hash Standard (FIPS PUB 180)

Description. The Secure Hash Standard (SHS) [NIST 93H] specifies a secure hash algorithm (SHA) for computing a condensed representation of a message or data file. The Secure Hash Algorithm (SHA) is based on principles similar to those used in the MD4 and MD5 message digest algorithms. The SHA produces a 160-bit message digest which can be used to provide data integrity. However, the primary purpose of the SHA is to produce a message digest that is input to the Digital Signature Algorithm (DSA) to generate or verify a digital signature over the original message. In order to produce fixed size message digests, the SHA performs message padding.

Status. FIPS PUB 180 was published in May 1993 and became effective in October.

Security Services. The Secure Hash Algorithm provides, or supports mechanisms that provide, the following security services:

- Data Integrity
- Data Origin Authentication
- Non-Repudiation.

4.1.5.21 Digital Signature Standard (Proposed FIPS PUB)

Description. The Digital Signature Standard (DSS) defines a public key cryptographic system that will specify a digital signature algorithm (DSA) for generating and verifying digital signatures over messages and data file. The DSA randomly generates a private key. Using this key and a mathematical process defined in the standard, the public key is then generated.

The DSA can be used in electronic mail systems, in legal systems where the integrity of a time stamp is needed, in electronic fund transfers, in Electronic Data Interchange (EDI) transactions, and for the secure distribution of software.

To generate a signature on a message, the owner of the private key first applies the SHA, as defined in the FIPS PUB 180 to produce the 160-bit message digest. The owner of the private key then applies it to the message digest using the techniques specified in the DSA to produce a 320-bit digital signature. Any party with access to the public key, message, and signature can verify the signature using the DSA.

The verifier can provide the message, digital signature, and signer's public key as evidence to a third party that the message was, in fact, signed by the claimant. Given the evidence, the third party can also verify the signature to provide non-repudiation.

Status. The DSS was proposed by NIST in August 1991 and is expected to be published in 1994.

Security Services. The DSS provides, or supports, the following security service:

- Data Origin Authentication
- Non-Repudiation.

The DSS does not provide data confidentiality. To provide confidentiality, the signer could first apply symmetric encryption to the message and then sign it using the DSA.

4.1.5.22 Message Oriented Text Interchange System (ISO 10021)

Description. The ISO Message Oriented Text Interchange System (MOTIS) [ISO 90C] is equivalent to the 1988 version of the CCITT X.400, called the Message Handling System (MHS). MOTIS is the application layer protocol which supports electronic mail for open networks. The 1984 version of X.400 did not consider security. Optional security extensions are provided in the 1988 version and accordingly, in MOTIS.

Security is achieved through the inclusion of security elements in the exchanged messages by cooperative users, or by adding information in the MHS envelope. MOTIS defines how to transfer relevant security parameters, but does not provide rules for generation and interpretation of the parameters.

An example of a MOTIS security exchange mechanism is one that requires the recipient to return a token to the sender that can only be generated when the message is correctly received. Once issued, the recipient cannot repudiate proof of delivery. A weakness in the mechanism is that no third party is used to mediate disputes. Furthermore, generation of the proof is at the discretion of the recipient.

Access control, based upon mutual user authentication, can be provided. Data confidentiality and data integrity, as well as sequence integrity are also provided by MOTIS for mutually cooperative users.

Status. ISO 10021 is an international standard. Other standards are being developed to provide stronger security mechanisms that are always invoked and that do not rely on cooperative users.

Security Services. MOTIS provides the :ollowing security services for cooperating users:

- Peer Entity Authentication
- Data Origin Authentication
- Probe Origin Authentication
- Discretionary Access Control
- Proof of Submission
- Proof of Delivery
- Non-Repudiation with respect to Origin
- Non-Repudiation with respect to Delivery
- Data Confidentiality
- Data Integrity
- Message Sequence Integrity
- Message Security Labeling.

4.1.5.23 Privacy Enhancement for Internet Electronic Mail (RFCs 1421, 1422, 1423, 1424)

Description. The Internet Engineering Task Force (IETF) published four documents that define the Privacy-enhanced Electronic Mail (PEM) protocol, its ancillary infrastructure, cryptographic algorithms to implement PEM, and initialization procedures for joining the Internet PEM infrastructure. [RFC 93B, 93C, 93D, 93E] The latest versions of the four documents are:

RFC 1421 – Part I:	Message Encryption and Authentication Procedures
RFC 1422 – Part II:	Certificate-Based Key Management
RFC 1423 – Part III:	Algorithms, Modes, and Identifiers
RFC 1424 – Part IV:	Key Certification and Related Services.

PEM employs cryptographic techniques at the application layer to provide the security services. An integrity check value (ICV) is computed for the message, using a message digest algorithm, and the ICV is transmitted with the message to provide message integrity. The message digest is sealed with an asymmetric algorithm using the senders private key which forms a digital signature to provide message origin authentication and non-repudiation with respect to origin. The message is then symmetrically encrypted for confidentiality and integrity. The key is encrypted using the recipient's public key and is transmitted with the message to enable decryption. Certificates are used to acquire public keys in order for both the originator and the intended recipient to verify the identity of the other.

PEM is designed to be selectively used by users and selectively deployed on end systems without interfering with users and hosts that are not implementing it. PEM certificate-based techniques are well suited for other applications that will certainly be identified as PEM becomes familiar to the Internet user community.

Status. RFCs 1421, 1422, 1423, and 1424 were published in 1993 as Proposed Standards and are currently being reviewed for inclusion into the Multipurpose Internet Mail Extensions (MIME) specifications. Four prototypes have been developed and used over Internet. Expansion of the user base outside the United States has been nearly impossible due to export controls on cryptographic algorithms. The prototypes have identified areas for improvement of the RFCs, particularly with respect to ease of use so that user errors are minimized.

Security Services. PEM protocols include the following security services:

- Message Integrity
- Message Origin Authentication
- Non-Repudiation of Origin
- Message Confidentiality
- Key Management.

There are several services which PEM does not address:

- Access Control
- Routing Control
- Traffic Flow Confidentiality
- Non-Repudiation of Delivery
- Duplication detection, replay prevention, or other stream-oriented services.

4.1.5.24 Key Management Using ANSI X9.17 (FIPS PUB 171)

Description. ANSI X9.17, the Financial Institute Key Management standard [NIST 92D], is in wide use today. It uses the Data Encryption Standard (DES) to provide key management. FIPS PUB 171 is a standard based on X9.17 for government agencies to follow when managing keying material. The standard cannot be used as an OSI key management protocol because it does not use ASN.1 notation nor make use of the Association Control Service Element (ACSE) to establish an application association as required to conform with ISO standards. When used in conjunction with ANSI X9.17, FIPS PUB 171 provides a key management system for:

- A point-to-point environment in which each party to a key exchange shares a key encrypting key which is used to distribute other keys between the parties
- A key distribution center (KDC) environment in which each party shares a key encrypting key with a center who generates keys for distribution and use between pairs of parties (such as is used in Kerberos)
- A key translation center (KTC) environment in which each party shares a key encrypting key with a center who translates keys generated by one party which will be distributed to another party who is the ultimate recipient.

Status. FIPS PUB 171 was published in 1992 to provide symmetric key management. Due to the proliferation of commercial products developed around DES, it is likely that this standard will be useful for many years to come. Future standards will provide for asymmetric key management based on public key encipherment.

Security Services. FIPS PUB 171 provides key management support for mechanisms that provide the following security services:

- Authentication
- Confidentiality
- Integrity.

4.1.6 Project Support Environment Standards

The Project Support Environment (PSE) is a unique area. Standardization in the other areas directly affect the types of services installed on the host or network system. Security services cannot be placed in the PSE. However, that is not to say that security is not an issue. In order to develop trusted software for other areas of standardization, security must be considered and mechanisms must be developed and installed in the PSE. The security guidelines and standards below discuss relevant issues. While many of the guidelines that can be applied to the PSE are well established, there are no well established standards. This area is undergoing considerable growth and is not stable.

4.1.6.1 NCSC Guidelines

Description. The NCSC has published many guidelines to help software developers understand the TCSEC, TNI, and TDI requirements and to suggest methods for meeting those requirements. Some important NCSC documents [NCSC 88, 89, 91, 92] are:

- Guide to Understanding Security Modeling in Trusted Systems, 1992
- Guide to Understanding Design Documentation in Trusted Systems, 1988
- Guidelines for Formal Verification Systems, 1989
- Guide to Understanding Configuration Management in Trusted Systems, 1988
- Guide to Understanding Trusted Distribution in Trusted Systems, 1988
- Guide to Understanding Trusted Recovery in Trusted Systems, 1991
- Guide to Writing Security Features User's Guide for Trusted Systems, 1991
- Guide to Understanding Trusted Facility Management, 1989

These documents, and others, form the Rainbow Series published by NCSC. Vendors who are developing secure products and systems are advised to follow these publications in order to understand and meet the evaluation criteria requirements.

Status. The Rainbow Series is well established and is being followed by all vendors who are developing secure products and systems. These documents will continue to be followed even when the Federal Criteria is adopted.

Security Services. NCSC guidelines provide no direct security services, but support the development of systems that provide all of the services described in the TCSEC (Orange Book), the TDI (Purple Book), and TNI (Red Book).

4.1.6.2 Portable Common Tools Environment Standard

Description. Numerous standards exist for specific areas of the project support environment, commonly referred to by NIST as the Integrated Software Engineering Environments (ISEE), such as programming languages and computer aided software engineering (CASE) tools. However, the PSE has no central base international standard. The European Computer Manufacturers Association (ECMA) published Standard ECMA-149 *Portable Common Tools Environment (PCTE): Abstract Specification* in 1990.

The North American PCTE Initiative (NAPI), consisting of NIST, DoD, and the Object Management Group (OMG), has accepted the ECMA reference model and supports development of the PCTE Standard, but would like to resolve some issues in the ECMA standard before it is accepted as an international standard.

Status. ECMA plans to enhance the ECMA-149 Standard slightly and submit it to ISO in 1994 to become an international standard. The PCTE Standard is one to two years from becoming an international standard, and may evolve considerably after that by incorporating improvements discovered as vendors begin to use the new standard.

Security Services. The PCTE Standard will provide no direct security services, but will support the standardized development of systems that provide all of the services described in the TCSEC, TDI, and TNI.

4.1.6.3 Project Support Environment Security Standards

Description. Federal policy is moving toward allowing procurements to specify industry developed standards along with ANSI, IEEE, and ISO standards. At the same time, there is concern over the need for open systems in software development. As a result, NIST, in cooperation with the NGCR Project Support Environment Working Group, will convene a special interest group to develop open systems Integrated Software Engineering Environment (ISEE) profiles, implementation agreements, and conventions for using such environment integration standards and specifications.

Status. The first Integrated Software Engineering Environment Special Interest Group (ISEE-SIG) meeting will be held at the OSI Implementors' Workshop (OIW) sponsored by NIST in March 1994. Security standards have not been placed on the agenda.

Security Services. If a PSE security standard were to be developed, it would provide no direct security services, but would support the standardized development of systems that provide all of the services described in the TCSEC, TDI, and TNI.

4.2 Security Functions and Services

As discussed in Section 3, some areas of standardization require security services only to support security functions in other areas. Examples are labeling to support access control, trusted path to support authentication, and object reuse to support data confidentiality and integrity. The graphical user interface provides no primary security functions, but provides labels to support access control. Adequate security support for Naval and other agency missions will be provided when the security services are provided in all of these areas.

	Primary Functions								Support Services			
Areas of Standardization	Identification & Authentication	Discretionary Access Control	Mandatory Access Control	Audit and Accountability	Service Assurance	Data Confidentiality	Data Integrity	Non-Repudiation	Labeling	Object Reuse	Trusted Path	Key Management
Operating System	•	•	•	•	•				•	•	•	
Database Management System	•	•	•	•	•	•	•		•	•	•	
Graphical User Interface			•			•	•		•		•	
Backplane	•	•	•		•	•	•		•	•		
Network	•	•	•	•	•	•	•	•	•	•	•	•
Project Support Environment	•	•	•	•		•	•		•	•	•	

Figure 4.2-1. Primary Security Functions and Support Services

The current standardization efforts discussed in Section 4 provide support for security functions and services to meet all of the needs identified in Figure 4.2-1 above. While there are no security functions or services listed for the project support environment (PSE), the services for host operating systems, DBMSs, backplanes, and GUIs apply with respect to the host computers used for software development. In addition, software configuration management and secure distribution of software are functions of the PSE. Integrity, confidentiality, and service assurance mechanisms must be in place during distribution. These may be incorporated in the communications assets or in manual distribution methods.

Focusing on the network area of standardization, Figure 4.2-2 identifies some of the standardization efforts that specifically provide security services that should be used for Naval and other agency missions.

	Primary Functions								Support Services			
Guidance Documents and Standards	Identification & Authentication	Discretionary Access Control	Mandatory Access Control	Audit and Accountability	Service Assurance	Data Confidentiality	Data Integrity	Non-Repudiation	Labeling	Object Reuse	Trusted Path	Key Management
TNI and GOSIP Guidance	•	•	•	•	•	•	•	•	•	•	•	•
Security Frameworks	•	•	•	•		•	•	•	•			•
Generic Upper Layer Security (GULS) Standard	•	•	•			•	•	•	•			
SAFENET Standard	•	•	•	•	•	•	•	•	•			
Protocols and Protocol Suites	•	•	•			•	•	•	•			•
Application Layer Standards	•	•	•	•	•	•	•	•	•			•

Figure 4.2-2. Primary Network Standards that Provide Security Services

As mentioned earlier, in the interest of interoperability, the Government has established requirements for implementation of standards that are accepted internationally. However, many of the standards related to networks are still undergoing revision even if they have been finalized. They are not stable because they have not yet been widely implemented. Major flaws may be discovered during implementation and require correction. Since many of the International Standards are not stable, existing standards that are more widely implemented may be specified in procurements in the interim.

This Page Intentionally Left Blank

Section 5

Security Services and Mechanisms

This Page Intentionally Left Blank

5.0 Security Services and Mechanisms

Sections 1 and 2 of this report discussed the rapid advances being made in computing and networking technologies and their importance to the Navy and other government agencies. Section 3 sketched out a model for a generic computer network that included host computers, local area networks, network switching elements, tactical transmission media, and interfaces to strategic communications systems. The model was developed as a reference for visualizing the need for security services and the placement of security mechanisms.

Section 4 synopsized the current status of security standardization in the areas of operating systems, database management systems, graphical user interfaces, networks, and the project support environment, for it is these areas that security services must be installed in order to provide secure host computers, networks, network switching elements, tactical transmission media, and strategic system interfaces.

This section will discuss generic security mechanisms that implement the security services described in Section 4. The mechanisms, listed in Figure 5.0-1, are categorized according to the following security services:

- Authentication
- Access Control
- Audit and Accountability
- Confidentiality
- Integrity
- Non-Repudiation
- Service Assurance.

Authentication

- Peer Address Checking
- Authentication Exchange
  - Passwords
  - Supporting Devices
    - Hand-held devices
    - Smart cards
    - Biometric readers
  - Challenge-Response
    - Symmetric Encipherment
    - Asymmetric Encipherment
- Certification Authority
- Continuity of Authentication

Access Control

- System-Oriented Access Control
  - Object Reuse
  - Trusted Path
  - Connection Timeout
- Discretionary Access Control
  - Access Control Lists
  - Capabilities
  - Authentication Server
- Mandatory Access Control
  - Security Labels
  - Routing Control

Audit and Accountability

- Audit Mechanism
- Alarm Mechanism

Non-Repudiation

- Digital Signature
- Notary Service

Confidentiality

- Physical Protection
  - Isolation
  - Selective Routing
- Information Hiding
  - Symmetric Encipherment
  - Asymmetric Encipherment
  - Traffic Padding
- Partial Accessibility
  - Internal Fragmentation
  - Data Scattering

Integrity

- Error Detection
  - Error Detection Codes
  - Integrity Check Values (ICV)
  - Message Digests
- Encryption for Integrity
  - Cryptographic Seal
  - Digital Signature
- Sequence Protection
  - Sequence Numbers
  - Cryptographic Chaining
  - Timestamps
  - Reflection Bits
  - Source Addresses

Service Assurance

- Redundant Components
- Fault Tolerance
- Priority Processing

Figure 5.0-1. Generic Security Mechanisms

5.1 Mechanisms that Provide Authentication

Authentication, the act of verifying the identity of a subject or claimant to allow access or communication exchange, is necessary to be performed within a host computer by the operating system, database management system, application programs, and backplane, and within the network for communications. By confirming the identity of a subject, authentication supports access control, accountability, and integrity services.

In some cases authentication is virtually nonexistent. An example of weak authentication would be for an operating system, DBMS, or network to accept the subject's simple assertion of identity with no credentials as proof. The inclusion of passwords and personal identification numbers (PINs) still provide weak authentication. Another example of very weak authentication is in the area of backplanes. The backplane may accept the context (e.g. the module's address) as sufficient evidence for authentication. Generally, on a network an authentication exchange is required to strengthen the level of trust. Trusted third parties, called *certification authorities,* can act as authorizing entities to provide information to be used to support mutual authentication among entities on a network. Hand-held user authentication devices, smart cards, and biometric readers may be necessary in environments where a high level of individual authentication is needed.

5.1.1 Peer Address Checking

Upon receipt of a message or protocol data unit (PDU) over a network, the peer address associated with the cryptographic key can be verified by comparing it to the source address of the message or PDU to provide data origin authentication.

5.1.2 Authentication Exchange Mechanisms

Authentication usually involves an exchange of messages between the claimant and the trusted computing base (TCB) or verifier who decides whether to accept the proof of identity based on the subject's credentials. Simple authentication involves the transmittal of a secret credential, such as a password, which is mapped to the claimant. Simple authentication is generally sufficient for user's to authenticate themselves to operating systems or DBMSs. However, in a distributed environment, a node that authenticates itself to another node must use stronger mechanisms than simple passwords. If not, the second node can masquerade as the first node when attempting to gain access to a third node. Additionally, the password could be intercepted by an eavesdropper.

Authentication mechanisms are considered to be *strong* when the claimant is not required to transmit the secret credential. Examples of strong authentication are challenge/response protocols using encipherment.

5.1.2.1 Passwords

Simple authentication using passwords is generally sufficient for users to log onto host computers when the users and host computers are located inside a controlled environment, the user identities have been established, the computer configurations are controlled, and the risk of leakage is low. For access within a network, the claimant should use a different password for each potential verifier to prevent an untrustworthy verifier from masquerading as the claimant. Unique one-time passwords can be used each time a claimant authenticates itself to the same verifier so that a wiretapper cannot acquire useful passwords.

5.1.2.2 Supporting Devices

Hand-held user authentication device. Authentication can be strengthened without requiring encryption by using support devices. A hand-held user authentication device can be programmed to store a long list of one-time passwords. The device requires no special hardware to be connected to a terminal. It is transparent to the terminal and to any intermediate node, communicating the authentication exchange directly to the authenticating node. Hand-held devices can also incorporate cryptography to provide strong authentication.

Smart cards. Smart cards can be used for personal authentication to support public key cryptography and can support signatures that contain more than a hundred digits. The card contains the user's private key and a secret code, called a *personal identification number (PIN).* The card also contains a processor capable of calculating the digital signature. A variation is based on a challenge that is implicit in the time of day. A new response is calculated every 30 to 60 seconds and a hash of the current time is supplied with the PIN. Smart card solutions requires card readers attached to terminals and workstations.

Biometric readers. Authentication of human claimants can be further strengthened by verifying biometric characteristics (e.g., fingerprint, retina, saliva) or other various non-forgeable possessions of the entity.

5.1.2.3 Challenge-Response Protocol Using Symmetric Encipherment

With symmetric encipherment, the claimant and verifier share a secret key and the rules for a challenge-response authentication protocol. The challenge-response protocol is dependent on the key distribution process to establish the tools for communication. The claimant requests to establish communications with the verifier. The verifier sends a unique number, called a *nonce,* to the claimant to begin the challenge-response exchange. The claimant must return the nonce to the verifier encrypted with the secret key that only these two parties know. The verifier authenticates the claimant by decrypting the nonce and verifying that it matches the original nonce. In addition to performing authentication, challenge-response exchanges protect against replay of previously authenticated messages. Mutual authentication is provided when the claimant also generates a nonce for the verifier to encrypt and return.

5.1.2.4 Challenge-Response Protocol Using Asymmetric Encipherment

An authentication exchange can also be made using asymmetric encipherment. Encryption and decryption can be performed in either order. If a message is signed with a decryption private-key, anyone with the corresponding encryption public-key can verify the source, assuming the private-key is kept secret.

An asymmetric authentication exchange, similar to that which uses symmetric encipherment, can be added. The claimant requests to establish communications with the verifier. The verifier sends a codeword to the claimant encrypted with the claimant's public key. The claimant decrypts the codeword with his private key, then encrypts the codeword again with his private key and returns it to the verifier. The verifier decrypts it with the claimant's public key to complete the exchange. There are plans to use this protocol in smart cards.

Incorporation of a reusable codeword leaves the exchange vulnerable to future replay by a potential masquerader. A nonce should be used in place of a codeword to guarantee the freshness of the challenge and to prevent such masquerading. Timestamps and synchronization of clocks can also be added to guarantee freshness. Mutual authentication is supported using either the codeword or nonce. Three-way authentication handshakes can also be used for multi-party mutual authentication.

5.1.3 Certification Authority

Trusted third parties are used to provide mutual authentication among a large population of entities on a network. Each trusted certification authority maintains information about a limited number of entities. A common method of third party authentication is for the trusted authority to produce an authentication certificate upon request from a claimant, seal it with it's private key, and to deliver it to the verifier. The certificate can also be stored in the Directory until it is needed. The certificate contains the method used to obtain it, the claimant's distinguished identifier, a cryptographic key (either symmetric or asymmetric) to be used by both the claimant and the verifier, and the identification of the algorithm to be used with the key. Since creation of the certificate involves encryption, an untrusted directory authority can store certificates without fear of corruption because modification would cause calculations on the value to yield an invalid certificate. The Directory could lose, but not forge or modify, a certificate.

5.1.4 Continuity of Authentication

Authentication that is performed when a communications session is established provides assurance of identity at that instant. To provide assurance of continuity of the authentication, the authentication service should be linked with a data integrity service. Use of a nonce, timestamp, and synchronization methods are examples of services that will prevent future reuse of authentication exchange messages by a masquerader. During connection-oriented communications, repeating authentication exchanges from time to time will strengthen the assurance, but will not be fully effective for communications occurring during intervals between authentication exchanges.

5.2 Mechanisms that Provide Access Control

There are two types of access control: physical and technical. Physical access controls provide isolation to prevent tampering and are applied to backplanes, dedicated stand-alone computers, the project support environment, and occasionally to network cabling. Technical access controls are implemented in hardware and software (e.g., Discretionary Access Controls based on identities, Mandatory Access Controls based on sensitivity levels, and encryption). If computers are networked, the perimeter of the physical control zone must be extended to enclose all components of the network. If the computer or network is shared, and one or more subjects require confidentiality or integrity assurance, technical access controls must be applied. In addition, if a portion of the computer (e.g., a remote terminal) or the network is located outside the physical control zone, technical access controls must be applied.

Most computers are shared or connected to networks that are shared. Therefore, most computers now require technical access control mechanisms. These mechanisms must reside in the host operating system and in the network management software, as well as in any shared DBMS. If the host is to operate in the multi-level security mode, technical access control mechanisms may be required for the backplane as well.

System-oriented access control mechanisms are used to reduce vulnerabilities associated with the design of the system. Examples of these are object reuse and trusted path. System-oriented access controls are not concerned with the rights of individual claimants, but with the ability of the host computer or network to limit access to information contained in the system. Other technical access control mechanisms determine specific access rights by evaluating the identity of an entity and information about the entity and about the object to which access is requested.

Access control can only be provided within the context of a defined security policy. The security policies for most systems or networks base access on the identity of the subject, membership in particular groups, and ownership of files. This is called discretionary or identity-based access control. In addition, all military and some commercial security policies also require that the subject's sensitivity label dominate the sensitivity label of the object for which access is requested. This is called mandatory or rule-based access control.

5.2.1 System-Oriented Access Control Mechanisms

Storage objects (e.g., buffers, pages of memory, disk sectors, magnetic tape) and communications paths between claimants and TCBs or verifiers hold sensitive information for which access must be controlled. The information in these objects and paths does not, at the time of system possession, belong to individual subjects, but to the system. Therefore, access is not based on subject identity, but on system ownership, and the operating system requires a unique type of access control. In addition, the system must limit the likelihood that unauthorized users can gain access through channels allocated to authorized users.

5.2.1.1 Object Reuse

Storage objects are intended to retain user data temporarily and to make that data available upon demand. After the information has been read out of the storage object and provided to the owner, the storage object can be reallocated for storage of another subject's data. However, a copy of the original subject's data remains in the storage object unless it has been purged. A browser or scavenger can gain unauthorized access to the residue. Furthermore, a storage object could become an information transfer channel, called a covert storage channel, between disjoint users. Therefore, all storage objects require purging upon deallocation. [DoD 85]

This mechanism is implemented by operating systems in host computers and intermediate nodes in a network. It is also implemented by applications and databases where the operating system has allocated a storage object to the application or DBMS, and the application or DBMS controls write and read actions on the object.

5.2.1.2 Trusted Path

A bidirectional trusted path is needed between a claimant and the TCB or verifier for use when a positive TCB-to-user connection is required (e.g., identification and authentication, change security level). [DoD 85] The trusted path is established through use of a trusted process that cannot be influenced (or spoofed) by untrusted software, rather than through an untrusted process operating as the user's agent. [GASSER 91] Within host systems, trusted paths are supported by hardware such as *'special'* signals from a physical key (e.g., the break key) and dedicated channels that cannot be simulated or spoofed.

To extend the trusted path to a network, the reference monitor which mediates all accesses on the host must be extended across the network. This is done by providing secure gateways and remote servers that the host can trust, since the host cannot trust other unknown hosts on the network. Specific implementations can partition the functions of gateways so that they cannot be mimicked in hosts. The result is a trusted path that, in theory, is as secure as one on a single stand-alone host, but which is dependent on multiple network components (many of which are not under a single organization's ownership and control) for maintaining a secure state.

5.2.1.3 Connection Timeout

Timeouts are installed on hosts to logout a user when there is no activity at a terminal for a prespecified period. It reduces the possibility that a user has inadvertently left the terminal unattended. Timeouts are also installed on networks to clear a connection when a node remains in a dormant mode for a prespecified period. Timeouts are intended to reduce the possibility that unauthorized persons can carry out operations for which they have no privilege.

5.2.2 Discretionary Access Control Mechanisms

Discretionary access control mechanisms determine the type of access that a subject can have to a storage or communications object (e.g., file, program, storage device, terminal, channel, etc.). Information for making access decisions is maintained in a database owned and controlled by the operating system or network manager. DBMSs and application programs may also control access to their storage objects and may thus maintain their own security management information base. Two discretionary access control mechanisms are generally used: access control lists and capabilities.

5.2.2.1 Access Control Lists

An access control list (ACL) is associated with an object and represents the set of subjects, or groups, that are authorized to access that object along with the types of accesses they are permitted. Discretionary access decisions are based on the identity of the subject or group to which the subject belongs. ACLs are easy to locate and maintain because they are linked to the storage object. ACLs are generally sufficient for discretionary access control decisions made within stand-alone hosts by the operating system or DBMS. ACLs are less effective in networks because the claimants whose identities appear on the ACL cannot usually be authenticated through direct interaction.

5.2.2.2 Capabilities

Capabilities are similar to ACLs except they are associated with a subject and represent the set of objects that the subject is authorized to access along with the type of access that is permitted. Since capabilities are not associated with objects, they are not as readily available and are more difficult to maintain. Capabilities act as tickets which give authorizations for subjects to access objects. They must therefore be protected from forgery or modification.

5.2.2.3 Authentication Server

One method for preventing forgery of capabilities is to use an on-line trusted authentication server that delivers capabilities to claimants upon demand. In order to gain access to an object, the claimant transmits the capability to the verifier who then confirms it's authenticity with the authentication server prior to granting access. While capabilities cannot be forged, they can be copied. To eliminate unauthorized copying, the claimant must notify the authentication server each time it copies the certificate and passes the copy to another entity; and the server must validate that a claimant is a valid holder of the capability by checking to see that the claimant is on the list.

5.2.3 Mandatory Access Control Mechanisms

Mandatory access control mechanisms determine the type of access that a subject may have to an object based on the subject's attributes, rather than its identity. Within the military, attributes generally involve only classification levels and categories. Examples of attributes that might be implemented in commercial systems are integrity identifiers or perhaps job classifications or roles. Mandatory access controls can be implemented within operating systems, application programs, DBMSs, and networks. The subject's attributes are examined to verify that they dominate (i.e., their access privilege set *includes)* the object's attributes prior to allowing access.

5.2.3.1 Security Labels

The primary support mechanism for enforcing mandatory access control policies is the use of security labels that indicate the sensitivity or protection level of the information. Security labeling by itself does not provide data security. Labeling must be implemented in conjunction with other mechanisms. The term *'security labels'* is a broad category that includes both sensitivity labels and integrity labels. This discussion centers on sensitivity labels to support mandatory access control mechanisms. However, integrity labels can also be applied to indicate what measures the data requires for protection from modification and destruction.

In a multi-level host, operating systems can bind upper and lower labels to subjects to indicate the range of information they are permitted to access, and to objects holding information (e.g., files, buffers, channels, terminals, and storage devices). In the future, backplanes may support operating systems by assigning labels to modules and mitigating access based on those labels.

DBMSs can bind labels to data at the file level, the record level, the attribute level (e.g., column), the entry level, or any combination. The graphical user interface can bind sensitivity labels to the display screen to indicate the highest sensitivity permitted for the user during the session. The graphical user interface can also bind information labels (which indicate the sensitivity level of the file being accessed) to individual display windows to indicate the highest sensitivity of information available for display in that window. If a user were logged on at the Secret level (display sensitivity label) and had two files open, the information labels for the windows might be Secret and Confidential (they cannot be higher than the level indicated by the sensitivity label). The user must not be able to cut and paste from the Secret file to the Confidential file. If the user later logs on for a Confidential session, the user must not be able to open the Secret file. Therefore, both the sensitivity label and the information label are used to support mandatory access control decisions.

Just as a host must securely bind sensitivity labels to the data with which they are associated, so must a network. Network management can also associate labels with nodes and communications channels. The security label also indicates, either explicitly or implicitly, the security authority responsible for creating the binding. The identification of the security authority must also be bound to the data.

5.2.3.2 Routing Controls

Routing controls are actions taken within networks to direct, throttle, or delete messages based on their contents and sensitivity labels. Routing control is the choosing or avoidance of specific networks, links, or relays. [NCSC 87] It provide confidentiality of communications without encryption by preventing sensitive messages from being sent through portions of the network where they may be intercepted by untrusted components of the network. [GASSER 91]

Routing controls can be implemented wherever a device is in a position to intercept communications between nodes. Usually routing controls are implemented in intermediate systems at the Network Layer. Additional functions of routing controls include providing access control by filtering out unauthorized requests for resources, and providing availability and cost control by keeping out excess traffic from unwanted sources. [GASSER 91]

Routing control mechanisms can be categorized as being either discretionary or mandatory. Discretionary routing control mechanisms identify the network components that are to be used or avoided based either on their general characteristics or on their specific identities. Mandatory access control mechanisms in hosts and network components may also be called upon to make routing decisions based on the sensitivity labels of traffic and network components. In a heterogeneous internetwork, and in subnetworks as well, some links may only handle a single level of data, while others can handle multiple levels. [SSI 92]

5.3 Mechanisms that Provide Audit and Accountability

Security audit is the journaling of security-relevant events to an audit trail, and the analysis and reporting of those events. The audit mechanism includes event detection, the journaling process, and alarms. A security alarm is a response to events or thresholds that must be immediately reported to a security alarm administrator. Analysis and reporting are management functions that are not actually part of the audit mechanism. The audit mechanism should journal:

- **Authentication results**, whether positive or negative
- **Accesses to objects and channels**, to allow the review of subject access histories and object or channel patterns of access
- **Repeated attempts to bypass** protection mechanisms by both authorized users and outsiders (whether successful or unsuccessful)
- **Use of privileges** beyond what a subject normally has that are acquired when the subject assumes a privileged role (e.g., programmer, administrator)
- **System failures** or events that indicate a potential for component failure or loss of data.

5.4 Mechanisms that Provide Confidentiality

Information is represented as data items such as files, bit streams, or messages during processing, storage, and transmission. Information may be derived from a data item in the following ways [ISO 92D]:

- Directly from the value of the data item
- From knowing whether the data item exists
- From attributes of the data item (e.g., creation date, owner, function, size, address, location, frequency, etc.)
- From dynamic variations of data and attribute representations.

Confidentiality mechanisms protect against disclosure by protecting the representation of the information and it's attributes from disclosure, and by protecting the representation rules from disclosure. There are three types of confidentiality mechanisms:

- Mechanisms that provide physical access protection:
  - Isolation and physical protection
  - Selective routing
- Mechanisms that hide the data:
  - Symmetric encipherment
  - Asymmetric encipherment
  - Traffic padding
- Mechanisms that make the data only partially accessible while in storage or transmission, such that the data cannot be completely recreated from the limited amount of data that could be collected:
  - Internal fragmentation
  - Data scattering (e.g., frequency hopping).

5.4.1 Confidentiality Through Physical Protection

Physical protection of computer and communications assets is necessary to protect against eavesdropping, modification, and sabotage. Isolation is commonly used without encipherment to provide confidentiality within a host computer.

5.4.1.1 Isolation and Physical Protection

Physical protection mechanisms such as isolation, locks, seals and other intrusion detectors are used to protect host computer and communication assets from tampering. Each computer in the network must be protected to ensure its integrity. This includes protecting the network interfaces and the modules that reside in the backplane, assuming the computer is using a backplane architecture. Authentication and access control mechanisms are used to isolate and mediate access to files within each host. The military also uses physical isolation of cable runs to protect networks whether or not other technical confidentiality mechanisms are used. Protected distribution systems can be used to secure individual cables and enable detection of wiretapping. The project support environment should be isolated from operational systems and both should be protected through physical measures.

5.4.1.2 Selective Routing

The use of physically secure sub-networks, relays, and links and the avoidance of others is an important method of providing confidentiality in networks. Routing control mechanisms can be either discretionary, where links are specified by the sender, or mandatory, where routing decisions are based on sensitivity labels. It allows the avoidance of known and potential passive monitoring and active wiretapping threats.

5.4.2 Confidentiality Through Information Hiding

Information hiding is the primary technical mechanism for providing confidentiality. Encipherment is used to accomplish information hiding so that an adversary cannot read traffic that is intercepted. Traffic padding is also used to camouflage the message length, and thus the message type, before the message is enciphered. Information hiding can be applied within operating systems, within applications, within databases, within backplanes, within networks, and in the project support environment. It can be applied to data elements, data records, or entire data files, and to selective fields or entire messages. Positive side effects are that it strongly supports authentication, access control, and data integrity services.

5.4.2.1 Symmetric Encipherment

Symmetric encipherment transforms plaintext into ciphertext through the use of an encryption algorithm and a secret key that is shared by two parties. Encipherment involves a combination of substitution and transposition operations. The same key is used to decrypt the ciphertext back to plaintext. Since both parties share the same key, symmetric encipherment is also called *secret key* or *one-key encipherment*, and because it has been used for decades, it is sometimes called *conventional encipherment*.

Symmetric encipherment is appropriate for uses within a host computer to encrypt files, records, and data elements, and for protection of individual communications channels in a network. In addition to providing confidentiality through information hiding, symmetric encipherment will support integrity if the algorithm provides error extension such that a wiretapper could not determine what effect a change to the file or message would have.

When symmetric encipherment is used to provide point-to-point protection in a network, a different encryption key should be used for each channel to ensure that only the two entities that are communicating over the channel have access. Pairwise keying also supports authentication. In addition, it conveys an authorization to communicate. Symmetric encipherment without other mechanisms present does not support non-repudiation because a receiver cannot prove that it did not send the message to itself.

End-to-end protection can be provided in a network by application entities or end-to-end communication protocol entities through pairwise keying. When cryptonets are formed by allowing multiple parties to hold the same key, limited forms of access control and confidentiality are provided, but authentication cannot be provided because encipherment by itself is insufficient to permit identification of the cryptonet member that the host is communicating with.

5.4.2.2 Asymmetric Encipherment

Asymmetric encipherment involves an encryption process that uses one key, called a *public key*, and a decryption process that uses another key, called a *private key*. The sender encrypts a message with the *receiver's public key* and the receiver decrypts the message using the *receiver's private key*. Public keys cannot be used to infer private keys and therefore require no protection from compromise and can be widely distributed. Private keys are not shared and must be protected from compromise. Asymmetric encipherment is also called *public key* or *two-key encipherment.*

Asymmetric encipherment provides confidentiality but is limited due to the fact that it is processing intensive and can only be used to encrypt small amounts of data, such as symmetric encipherment keys. Integrity is not supported because asymmetric encipherment does not provide error extension. Authentication is not supported because it provides no assurance that the sender provided it's true identity. Non-repudiation is not supported for the same reason. Asymmetric encipherment is the basis for digital signatures which can provide both authentication and non-repudiation as discussed in Section 5.6.

5.4.2.3 Traffic Padding

Traffic analysis is a compromise in which analysis of message length, frequency, and protocol control information (such as address) results in information disclosure through inference. [NCSC 87] Traffic flow confidentiality is concerned with masking the frequency, length, and origin-destination patterns of communications between protocol entities. Traffic padding provides traffic flow confidentiality. Traffic padding is only effective when it is used in conjunction with encryption. There are two general approaches to traffic padding:

- Padding individual data units to a fixed length to conceal message size
- Generating dummy data units to conceal the amount of traffic on the channel between any particular source and any particular destination.

Care must be taken to prevent the introduction of covert channels through traffic padding. This is done by requiring that specific characters be used for padding. At the same time, the padding characters should be sufficiently varied to thwart cryptanalysis.

5.4.3 Confidentiality Through Partial Accessibility

Contextual mechanisms provide confidentiality by making the data only partially accessible while in storage or transmission so the data cannot be completely recreated by an eavesdropper.

5.4.3.1 Internal Fragmentation

Information that is fragmented and distributed is of less value than when it is all available to an intruder. When data is transmitted in a prespecified format and the field names and encoding rules are not transmitted with the data values, the information is less vulnerable.

5.4.3.2 Data Scattering

Frequency hopping techniques are used to provide confidentiality. The sender and receiver change frequencies rapidly, sending small portions of a message during each burst. The eavesdropper must copy all channels or must change frequencies along with the sender and receiver in order to intercept the entire message. Encryption prevents the eavesdropper from knowing the channel identity where the next burst will be sent. Using a large number of channels prevents the eavesdropper from intercepting them all. Sending small bursts and changing channels quickly prevents the eavesdropper from tuning in on the correct channel in time to intercept much of the burst.

5.5 Mechanisms that Provide Integrity

Integrity mechanisms detect unauthorized modifications of data in storage (files, records) and in transit (messages, fields). These may be accidental, caused by hardware error or noise on the channel, or intentional, such as active wiretapping. It is access controls, not integrity mechanisms, that are intended to prevent unauthorized modifications. Integrity mechanisms are responsible for detecting such occurrences in time that they can be corrected without having a serious impact on operations. Integrity mechanisms and access controls are strongly supported by confidentiality mechanisms, particularly encryption. Integrity mechanisms can be grouped into the following categories:

- Error Detection
- Encryption for Integrity
- Message Sequence Protection.

5.5.1 Error Detection

The operating system, backplane, network, and project support environment all use forms of error detection to provide assurance that data has not been corrupted.

5.5.1.1 Error Detection Codes

In host systems, error detection is typically done through the use of vertical and longitudinal parity checks on data transfers between the backplane, microprocessors, memory, buffers, cache, interfaces, and other components. For software being delivered from the project support environment, it is generally provided by linear checksums and cyclic redundancy checks (CRCs). Communication protocols use non-secure error detection codes for integrity. When error detection codes are used for communication in conjunction with encryption that includes error extension, an adversary cannot modify the PDU and the check values to hide the fact that modification has occurred.

5.5.1.2 Integrity Check Values

For communications integrity, integrity check values (ICVs), computed as a cryptographic function of the information bits in a data unit, are appended to the data by security protocols and both are sent to the destination. This causes the ICV to be cryptographically bound to the data. The destination then recomputes the ICV with the data received to determine if it matches the received ICV. ICVs are suitable for integrity of bulk data communications. One ICV specified by ANSI uses symmetric encipherment based on the Data Encryption Standard and requires that both parties know the secret key.

5.5.1.3 Message Digests

A message digest is a short fixed-length value that is calculated against the message using a well known one-way hash algorithm. No secret key is needed to compute the message digest and it is computationally infeasible to find another data unit that produces the same hash value. These two properties essentially make the hash value as unique as the data unit. Both the sender and verifier use the well known one-way hash algorithm to determine the message digest. Message digests are not intended for integrity of bulk data communications. Their primary use is in conjunction with digital signatures.

Using a digital signature, the source signs the hash value of the data unit with its private key. This serves to bind the hash value to the data unit. It then sends the data unit and the signed hash value to the destination. The destination recomputes the hash using the plaintext data unit, verifies the signed hash with the public key (producing the plaintext hash) and compares this plaintext hash with the recomputed hash to see if they match. [SSI 92]

Public key cryptography is slow and calculating digital signatures over the entire message is time consuming. Calculating a message digest is fast, and a signature of the message digest is as valid as a signature of the entire message. [GASSER 91] Calculating one-way hash values against passwords is also useful in providing integrity during authentication.

5.5.2 Encryption for Integrity

Encryption is a strong measure for supporting detection of password and message modifications. Several cryptographic mechanisms are used for integrity.

5.5.2.1 Cryptographic Seals

Cryptographic sealing is a special case of applying an ICV. Cryptographic sealing is based on encipherment and provides integrity by appending a cryptographic check value to the data to be protected. Integrity is assured by virtue of the fact that only two entities (or a limited number of entities in the case of a cryptonet) share the key.

5.5.2.2 Digital Signatures

Digital signatures, described in Section 5.6, are based on asymmetric encipherment and provide integrity by appending cryptographic check values to the data to be protected. Integrity is assured by virtue of the fact that only one entity knows the private key and can sign the data, and that the receiving entity reliably knows the sending entity's public key.

5.5.3 Sequence Protection

Connection integrity services can detect message deletion (including the special case of truncation), duplication, insertion, reordering, and replay. [SSI 92] Mechanisms that support these services include:

- Sequence Numbers
- Cryptographic Chaining.

Sequence numbering and cryptographic chaining have limited capabilities in protecting against replay. As is discussed below, replay can be detected within a sequence period, but may not be detected if it occurs after a recycle when the sequence numbers are reused. A mechanism that offers strong protection against replay is:

- Timestamps.

A special case of replay, called reflection, occurs when a sender receives a message back. Two mechanisms protect against reflection:

- Reflection Bits
- Source Addresses.

5.5.3.1 Sequence Numbers

Consecutive sequence numbers are transmitted with data units and are represented by a field fixed in size using modular arithmetic. A receiver can thus detect missing or duplicate data units or data units that are received out of order. Replay can be detected within a sequence period, but may not be detected if it occurs after a recycle when the sequence numbers are reused. This vulnerability can be addressed in several ways: 1) the data units can also include the date and time they were generated (timestamp); 2) the connection can be released when the sequence numbers are exhausted and a new connection can then be established with a new connection identifier; and 3) if the data units are encrypted, the session key can be changed when the sequence numbers are exhausted. This causes the combination of the sequence numbers with either the timestamp, connection identifier, or key to be unique for each data unit.

Integrity mechanisms should be used to protect sequence numbers from being modified and to bind them to the data units. To prevent truncation of sequences of data units prior to releasing a connection, a control data unit can be sent to identify the sequence number of the final data unit transmitted.

5.5.3.2 Cryptographic Chaining

With cipher block chaining, the ciphertext output for a block of data is transmitted to the receiver and is also used to transform the input of the next block. Ciphertext blocks must be received in the proper sequence for decryption to be accomplished.

5.5.3.3 Timestamps

Including a timestamp with a data unit is effective in protecting against replay, provided all parties can measure time with sufficient accuracy. As with sequence numbers, ICVs and encipherment should be used to protect timestamps from being modified.

5.5.3.4 Reflection Bits

Two cooperating entities that share a unique key can establish a protocol that uses a single bit to indicate on which end of the connection a message originated. If an entity receives a message that the reflection bit indicates it sent, the entity discards the message. As with other integrity protection mechanisms, the reflection bit must be protected from modification.

5.5.3.3 Source Addresses

The source address field is used in the same manner that a reflection bit is used, except that it can be used on a cryptonet where a group of entities share a secret key.

5.5.4 Integrity Recovery Mechanisms

Integrity mechanisms that provide sequence protection enable receivers to detect when a protocol data unit is lost. Communications protocols incorporate mechanisms that use that ability to recover lost data units. Examples are:

- Stop-and-Wait Protocols - sender transmits a data unit, sets a retransmission timer, and waits for an acknowledgment. If an acknowledgment (ACK) is not received before the timer times out, the sender retransmits.
- Go-Back-N Protocols – sender sets a timer and begins transmitting data units without waiting for acknowledgments. Any time an ACK or negative acknowledgment (NAK) is received, the timer is reset. If an ACK is received, all data units have been successfully received up to an indicated data unit. If a NAK is received, it will indicate which data unit to begin retransmission from. If the timer expires before an ACK or NAK is received, all data units since the last ACK will be retransmitted.
- Selective Repeat Protocols – sender sets a timer and begins transmitting data units without waiting for acknowledgments. Any time an ACK or NAK is received, the timer is reset. If an ACK is received, all data units have been successfully received up to an indicated data unit. An NAK indicates a data unit that was not received or that contained errors and requires retransmission. Only that data unit will be retransmitted. If the timer expires before an ACK or NAK is received, all data units since the last ACK will be retransmitted.

5.6 Mechanisms that Provide Non-Repudiation

Non-repudiation mechanisms are used in networks to provide proof of the origin or of the delivery of data. It counters false denial by an originator that the data has been sent and false denial by a recipient that the data has been received.

Digital Signatures are used to provide non-repudiation. A digital signature establishes the source of data and protects against forgery by other parties including the destination. [SSI 92] Non-repudiation services may require the existence of a trusted third-party, called a notary, who authenticates the evidence, verifies its integrity, and arbitrates disputes that arise as a result of repudiated messages. [ISO 93B]

5.6.1 Digital Signatures

A digital signature based on asymmetric encipherment uses the sender's private key to sign the message and the sender's public key to verify the signature. Any receiver who can obtain the sender's public key can verify the signature. The digital signature can be computed against the entire message. However, because asymmetric encipherment is processing intensive, a message digest is usually computed for the message, and the digital signature is computed against the message digest.

In order to serve as a non-repudiation service with respect to origin, the destination must store the signed data unit and its source's corresponding public key for future reference so it can show that the received plaintext being contested is produced with that public key. However, the sender can later claim that it's private key had been compromised and someone else must have sent the message. Non-repudiation using merely a digital signature is therefore only effective when the entities trust each other. A robust non-repudiation service requires the use of a trusted notary service.

5.6.2 Notary Service

A notary service is provided by a trusted third-party, called a notary or arbitrator, to verify that a data unit has been sent by the sender, that it has been received at the destination, and that neither party has since modified it. The sender typically employs either an encipherment of the data unit or the production of a cryptographic checkfunction of the data unit, using its private key. [NCSC 87] In order for the notary to provide non-repudiation with respect to origin, the sender must route the signed message to the notary service who then verifies the signature, timestamps the data unit, appends its own signature, and forwards the data unit to the destination. The notary stores the document or the signature of the document with a timestamp. Ideally, the data unit is encrypted so the notary is not able to read its content. [MUFTIC 93]

In order to provide non-repudiation with respect to delivery, the receiver must sign the message upon receipt and return it to the notary as an acknowledgment which could be used later by the notary to prove delivery.

5.7 Mechanisms that Provide Service Assurance

Service assurance is provided by a number of mechanisms including redundancy, fault tolerance, and priority processing.

5.7.1 Redundant Components

A primary mechanism that is useful both within a host and across a network is redundancy. Dual processors, spare components (e.g., mirrored hard disks, redundant disk controllers, etc.), mirrored databases, dual homing to network access points, dual networks, and transmission groups consisting of multiple physical links and alternate routes are examples of redundancy that strongly supports system availability.

5.7.2 Fault Tolerance

Error detection, fault detection, error recovery, and fault recovery within applications, DBMSs, operating systems, and networks support continuity of operations. Distributed processing and the use of subnetworks help to assure that a mission can be met with reduced resources when individual components are inoperable. Routing control mechanisms described in Section 5.2.3.2 for network access control support service assurance by allowing specific subnetworks, relays, or links to be selected or avoided. Network management software can identify network components that are out of service or temporarily saturated. The integrity recovery mechanisms described in Section 5.5.4 support service assurance within a network by helping to guarantee that lost or corrupted data units are identified and retransmitted.

5.7.3 Priority Processing

Denial of service involves both loss of information and delay of information. Military systems often incorporate priority processing so that more perishable information is processed first. Priorities can be assigned to processes within a host and messages being transmitted over a network to improve response times of the higher priority information.

This Page Intentionally Left Blank

Section 6

Additional Factors Concerning Placement of Services

This Page Intentionally Left Blank

6.0 Additional Factors Concerning Placement of Services

This section discusses factors concerning the choice and placement of network security mechanisms that must be considered when evaluating the following architectural alternatives for secure computer and communications systems:

- Designing a multilevel system versus designing separate system high or dedicated systems at unclassified and single-classification levels
- Placement of security services in particular areas of standardization
- Implementation of security services in application processes versus implementation in the communication protocols
- Placement of communication security protocols in host computers versus placement in external devices
- Using distributed versus centralized security mechanisms.

6.1 Multilevel Security

Current technology requires that separate classified and unclassified networks be developed and maintained independently because the programmatic risk to develop computers that can be trusted to maintain the necessary separation is too great. Currently, any exchange of information between classified and unclassified networks must be processed manually or through a trusted multilevel guard. Command Centers assimilate battle information from classified and unclassified sources which are closely related, yet must copy information from the *low* system to the *high* system in order to process and display the information together. Classified databases often mirror exact copies of unclassified databases, but include additional classified records inserted independently. Concurrency of the classified database becomes an issue when records are added or deleted from the unclassified database. Additionally, network designers do not currently have the latitude to interface classified shipboard networks to Internet or commercial B-ISDN. Navy personnel must access these wide area networks through their unclassified systems and must find other means for communicating classified information to organizations connected to only these networks. The development of an MLS system would thus allow for information to be exchanged more efficiently and reliably between users at different clearance levels.

The primary classified shipboard network is commonly designated to handle Unclassified, Sensitive but Unclassified, Confidential, and Secret data. All personnel having access to the classified network are cleared for access to Secret information even though many only require access to Confidential information. Additional systems are installed for the handling of Unclassified through Top Secret and Sensitive Compartmented Information (SCI). Personnel with clearances and a need-to-know are granted access to information on those networks.

When MLS-capable computers, DBMSs, and networking products are commercially available, system engineers will be able to design internetworks of commercial and government systems operating at various classified and unclassified levels. Development of fully-capable multilevel systems is an expensive and time-consuming process. However, the benefit is that only one network will be necessary to support all shipboard operations and to allow interconnection to virtually any strategic communications system. It has been claimed that a significant cost-benefit can be realized by clearing personnel only to the level needed and by installing only one shipboard network. Decision-makers are aware of these benefits and are funding research and development efforts in all associated areas of standardization. Until such time that these products become readily available, which will probably be at least 10 years, designers must include security mechanisms in the physical facilities, host computers, and networks to safeguard classified information.

In summary, the major factors to consider when choosing between using an MLS system versus using separate dedicated or system high systems is that when an MLS system is used, the overall performance and reliability of the network is improved while reducing its operational cost, but the developmental cost and programmatic risk associated with an MLS system is significantly higher.

6.2 Areas of Standardization

Both the host computer and the network must provide security services. The security services in question are *Authentication, Access Control, Audit and Accountability, Confidentiality, Integrity, Non-Repudiation, and Service Assurance.* Operating systems are responsible for performing identification and authentication, access control, and audit and accountability for the host computer and they must provide appropriate levels of confidentiality, integrity, and reliability based on their implementation-specific security policies. Applications and DBMSs may also be designed to perform many of these services to meet implementation-specific requirements. The network provides, or may provide, services in addition to what is provided in the host computer.

Design trade-offs must be based on the level of security demanded by the environment, and the capability available in the operating system, DBMS, network, and applications. Designers must assess the capabilities of both the host and the network while keeping the goals of the total system in perspective before establishing specific security requirements for either the host computers or the network. System functional goals might be achieved if the necessary security features are found in either the computer architecture or the network capabilities. Lacking these, operational flexibility cannot be extended. As more security services are designed into operating systems, DBMSs, and networks, more options will be available to system developers. Emphasizing the implementation of security within the network can reduce the risk of supporting security within operating systems, DBMSs, and applications, but reduces the flexibility with which differing network technologies can be supported.

With respect to access control within a host computer, there is a trade-off on whether to modify the operating system to produce a security kernel or to develop a separate physically isolated kernel. The latter approach can reduce the programmatic risk associated with developing a secure operating system as well as providing a more efficient operating system, but the resultant system is more costly due to the greater component count.

The LOCK architecture [SAYDJ 87, SAYDJ 89, SECCOMP 91A, and SECCOMP 91B] is an example of an access control mechanism which has a coprocessor that connects to the bus to implement a separate isolated reference monitor from that in the operating system. LOCK monitors all exchanges over the bus. It implements a security kernel in a commercial off-the-shelf product while minimizing the modifications that a system developer must make to a target system. It implements the reference monitor concept by virtue of the fact that it meets the following criteria:

- Always invoked – the LOCK processor is always invoked before the primary processor so that it can monitor all activity on the system, even during startup
- Tamperproof – it is not part of the operating system and, in fact, is physically isolated and uses a separate coprocessor. Also, LOCK maintains a separate access control database
- Easily verifiable – the LOCK code is small and clearly identifiable.

Design decisions can also be made in terms of the extent to which security functionality is incorporated within the graphical user interfaces versus the operating system and applications. Graphical user interfaces implement labeling to support access control decisions based on services provided in the operating system and application programs. GUI security implementations, such as the Compartmented Mode Workstation (CMW) may implement features for sensitivity labeling, information labeling, and trusted path. However, the GUI cannot enforce an access control policy. The direction of GUI standards discussed in Section 4 indicate a lack of need for GUI security services.

Trade-offs can be made regarding the extent to which security functionality is incorporated in the backplane versus the operating system. Mechanisms embedded in the backplane can be more robust, but are also more expensive. Access Control for the backplane may consist of identifying which modules are allowed to exchange information based on hardware addresses. This minimal level of access control assumes that access to the backplane is physically controlled so that an external listening device (e.g., logical analyzer) cannot be attached. Audit and Accountability is generally not necessary because the operating system controls all traffic on the backplane. This may change as parallel processing technology advances. Confidentiality of data on the backplane is provided as a consequence of using access control. However, multilevel systems must provide assurance that confidentiality will be maintained internally. Richer discretionary and mandatory access control policies may potentially be enforced by the backplane architecture, thereby reinforcing this functionality in the operating system. Therefore, mandatory access control and confidentiality services may be implemented in the backplane in the future. Integrity is a service that is typically implemented in the backplane and memory management hardware for the sake of speed and convenience. The Futurebus+ standard provides authentication, access control (both discretionary and mandatory), confidentiality, integrity, and service assurance services in the backplane. In addition, it supports labeling and object reuse.

6.3 Security in Applications versus Communication Protocols

Additional factors must be considered when designers are assessing whether to place security services in application processes or communication protocols. All of the security services can be implemented by application processes above layer 7, or in OSI layers 6 and 7, or even lower, as suggested by ISO 7498-2. The security services in question are Authentication, Access Control, Audit and Accountability, Confidentiality, Integrity, Non-Repudiation, and Service Assurance. It is possible for applications, or preferably the security kernel that supports them, to authenticate the remote users desiring access and to base access decisions on that authentication. The security kernel or application process can also maintain their own audit trail, perform confidentiality and integrity services, and verify that messages they send are delivered. When data is exchanged between hosts that use the same local representation for data, encipherment can be implemented in application processes. This could improve throughput and delivery times, since the translation function normally performed by the presentation layer is processing intensive and requires significant transmission overhead as well. The inclusion of security functionality within the application processes could expand the use of available NDI software. Of course, for interoperability, all the NDI software would have to perform the same functions and do so in the same manner. The approach also facilitates the use of NDI operating systems because the operating system would not have to exchange security information with communication protocols.

While it is possible for individual applications to provide some of the security services, it may be more efficient to develop one set of security services and place those services in the OSI stack rather than developing individual mechanisms for each application process. For that reason, it is preferable that communication protocols provide these services. When the environment demands, or when communication protocols are insufficient, the application programs may provide the security services. In the past, engineers developing applications have not fully trusted the communications support and have included acknowledgments, sequence numbers, security labels, integrity check values, and many other countermeasures in their design to provide security services for their data. As indicated in Section 4, standards bodies are developing guidelines, profiles, frameworks, models, and protocols that address security services in networks at all layers. Applications are beginning to be designed with interfaces by which they can request security services from the communications infrastructure. Until such time that protocol standards are complete and stable, a combination is most effective.

When security is to be implemented in the communications protocols, there are trade-offs to be made within the OSI layers. Considerations described in the SBIR Phase I report [SSI 92] include:

- Users associated with an application process can be authenticated at the application layer.
- Application layer protocols also represent information resources (processing and storage resources) associated with the host environment for which access control decisions can be made.
- A non-repudiation service can only be implemented at the application layer. The direct unarbitrated signature commonly used today provides only limited protection. A robust non-repudiation service requires the use of a trusted notary to:
  - Securely store records of the transaction to furnish a proof to an adjudicator if a dispute arises.
  - Support non-repudiation with proof of delivery by forwarding a test message to the receiver immediately before sending the real message to see if it is ready to receive and if the communications channel is functioning. Sending the test message does not ensure that the receiver actually gets the real message that follows, but it does make it more probable.
  - Provide an accurate time reference for time stamping data and recording when the data was submitted to the time stamping service.
- There are two candidate layers for providing selective field confidentiality and integrity — the presentation and application layer. To provide these services, it is necessary to know the structure of the data that is being processed. This information is made available to the presentation layer by the application layer. The presentation layer converts a local data representation of a host to a common OSI transfer syntax which allows heterogeneous hosts to interoperate. At all of the lower layers, the structure of the SDU is ignored.
- When data is exchanged between hosts that use different local representations for data, encipherment should not be implemented within the application layer, since the local data representations becomes unintelligible to the presentation layer which cannot convert them to the OSI transfer syntax. Hosts developed by different vendors generally have major differences in how they represent data locally. This applies to both simple data structures ("big endian" versus "little endian" problem, for example) and complex data structures (vectors, matrices, etc.).
- If data confidentiality is implemented using encipherment in any of the upper four OSI layers (transport through application layer), true end-to-end encryption (E3) is provided between hosts across a network or internetwork.

- Access control decisions can be made with a finer level of granularity using access control information from the upper OSI layers than the lower layers. Making access control decisions in the upper OSI layers amounts to deciding if protocols or application processes within particular network components are allowed to communicate. At the network and data link layers, deciding if protocol entities can transfer data or establish a connection amounts to deciding if their associated network components are authorized to communicate. At the physical layer, access control decisions can only be made for network components that are directly connected to a physical link (cryptonets implemented at the physical layer, for example, can be used to control which stations can exchange data on a LAN segment).

- The service access point (SAP) addresses associated with layers 4 through 7 identify particular protocols or application processes within the hosts, but do not identify the hosts themselves. Authentication of these SAP addresses provides a finer level of granularity towards authenticating application processes.

- All OSI layers have communications resources (i.e., protocol entities) that can be protected from unauthorized access. Between adjacent layers, an access control decision can be made to determine if the services requested by the service user from the service provider are authorized. Between correspondent protocol entities within the same layer, an access control decision can be made to determine if they are authorized to exchange data for a connectionless service or to establish a connection for a connection-oriented service.

- A limited form of access control can be supported through the use of cryptonets (a group of entities that share the same key) at any layer.

- At the top of layer 3 (network layer), a Subnetwork-Independent Convergence Protocol (SNICP) can support either link or end-to-end encryption. When the SNICP encipherment/decipherment entities lie within hosts, true end-to-end encryption is provided. When one entity lies in a host and the other in a gateway (or if both lie in gateways), link encryption is provided.

- Encipherment at the data link layer can provide either link or end-to-end encryption for a collection of LANs connected through bridges.

- Encipherment at the physical layer for LANs and WANs, and the data link layer for WANs, provides link encryption.

- An authentication service is related to the general services provided by protocols in almost every OSI layer, since all of these protocols provide some kind of identification information that relates to the protocol entities. The one exception is the physical layer which does not support the use of headers or trailers, or consequently any entity identification information. Authentication can still be supported at the physical layer by using symmetric encipherment with pairwise keys.

- Since correspondent entities at the physical layer and the data link layer for WANs lie across a physical link and are generally not collocated with the application processes they support, they cannot generally be used to authenticate the application processes.
- As one moves up the bottom three layers of the OSI RM, the degree of confidentiality protection generally improves, since there are more situations in which relays are denied the potential to monitor traffic. The degree of protection is equivalent for the top four layers from the perspective of link versus end-to-end encryption.
- In moving up the lower three OSI layers, the strength of an authentication mechanism improves, since there are more networking situations in which the source and destination network components that support an application process are truly being authenticated, rather than intervening components, such as intermediate systems.
- Lowering the layer in which encipherment is provided, causes more upper layer headers to be encrypted before transmission over a physical link and therefore provides greater protection against traffic analysis. The physical layer can protect idle periods as well. At the physical layer, full period encryption can be provided so that no traffic is discernible. The physical layer can also sometimes be protected with intrusion resistant media so that outsiders cannot monitor transmissions (traffic flow or content) without being detected.
- The physical layer provides the best combination of link encryption and traffic flow confidentiality. The data link layer can provide end-to-end encryption for a collection of LANs connected through bridges. The network layer can provide end-to-end encryption for an internetwork consisting of LANs and WANs. The upper four layers steadily decrease in desirability from a traffic flow confidentiality perspective, but all provide true end-to-end encryption. Some environments require super encryption, i.e., end-to-end encryption provided in the upper layers for data confidentiality and link encryption provided in the lower layers for traffic flow confidentiality.
- Traffic flow confidentiality can be supported to some extent through the generation of spurious traffic followed by encipherment. The traffic padding function can be implemented above the encipherment function within the same layer or across different layers. If spurious traffic is transferred between hosts at layers 3 through 7, the traffic will be distributed naturally across links or subnetworks. The top of the network layer (SNICP sublayer) is the lowest layer at which spurious traffic can be generated for exchange between hosts on an internetwork of LANs and WANs and eliminates the need to process real headers for dummy traffic at higher layers (service requests to generate dummy traffic could however be generated at the higher layers). A negative side effect to traffic padding, particularly when it is accomplished end-to-end, is that it can cause congestion. If spurious traffic is introduced at the data link layer, all address information contained in the upper layer headers will be

hiuden. However, a traffic analyst may still be able to detect some spurious traffic by correlating the traffic levels among different links.

- Error detecting codes can be used to thwart active wiretapping threats when used with encipherment algorithms that provide error extension. An encipherment mechanism with error extension has the property that when a pattern of errors is introduced in the ciphertext, a larger range of bits will potentially be in error in the corresponding plaintext. Depending on the encipherment technique used, the position of errors occurring within this range may be completely unpredictable or it may be possible to know with certainty where one or more errors will occur. If an error detecting code is generated before going through an encipherment algorithm that provides error extension, wiretappers can change the ciphertext bits at will, but they cannot predict all of the plaintext bits that will be changed as a result. In general, the error detection code can be implemented above the encipherment function within the same layer or across different layers.

Thus, where security services are placed in the various layers affects the strength of the security mechanism, the throughput/delivery time, the cost of the security mechanisms, and programmatic risk.

6.4 Communications Security in Hosts versus External Devices

For economic reasons, commercial networks typically place security services in higher layers and on devices resident on the host computer. For security reasons, military networks often place security services in front end devices where access can be strictly limited. The trade-off is cost versus the degree of physical protection.

Communications security services that are implemented in software can be widely distributed and installed on existing systems without additional hardware. These mechanisms are the least secure, and incur a processing penalty by competing for CPU cycles. Therefore, security mechanisms implemented in software within hosts process traffic more slowly than secure front ends. Communications security services that are implemented in chips or on circuit boards can also be produced economically and be distributed and installed relatively easily. These are more secure because they require that an attacker have physical access. Hosts with embedded security mechanisms that are implemented in hardware also process traffic faster than either hosts with mechanisms implemented in software or front-end security devices, and generally incur less programmatic risk to develop. Communications security services that are implemented in external devices such as security card devices and secure front-ends are the most expensive to implement and the most physically protected from attack.

An additional factor that influences the decision on where to implement COMSEC services is the type of external WAN interfaces that are desired. In order for classified hosts to communicate over untrustworthy networks, such as commercial B-ISDN or Internet, end-to-end encryption is required, either internally or within front-end devices.

6.5 Distributed versus Centralized Security

Security functionality can be implemented primarily within hosts (distributed) or primarily within a security server (centralized).

Direct key distribution provides an example of distributed security functionality. In this approach, two entities that want to establish security associations initially share the same Key Encryption Key (KEK) delivered out of band using a physical distribution mechanism. The source generates a session key, encrypts it with the KEK, and then sends it to the destination. It is then decrypted at the destination using the KEK. Traffic can then be exchanged between the entities using the session key.

The use of a Key Distribution Center (KDC) provides an example of centralized security functionality. With this approach, each entity in the network initially shares a master key with the KDC delivered to them out of band, using a physical distribution mechanism. If 'A' wants to establish a security association with 'B', it requests that the KDC establish a session key for this association. The KDC generates two copies of the session key and encrypts one in the master key for A, and the other in the master key for B. The KDC sends both to A. A decrypts the session key using its master key, and sends the other encrypted session key to B. B then decrypts the session key using its master key. A and B can then exchange data using the session key.

Several fundamental factors must be considered when deciding whether to implement centralized or distributed security functionality. In general, distributed security mechanisms require less overhead and are more efficient than centralized security mechanisms. They are also less vulnerable to denial of service attacks because disabling the security server would disrupt all service in a centralized system. On the other hand, distributed systems are more costly since a greater number of components throughout the network must incorporate additional trustworthy security functionality.

This Page Intentionally Left Blank

Section 7

Summary

This Page Intentionally Left Blank

7.0 Summary

The primary objective of this study was to assess the status of security standardization for host computers, networks, and the project support environment. For host computers, the areas of standardization to be assessed included operating systems, database management systems, graphical user interfaces, and backplanes.

To better understand why security standards are needed, and in order to identify the types of standards that are needed to support the development of secure computer and network systems, the early sections reviewed the state of automation technology and the Naval environments for data processing and communications.

Section 1 provided background information concerning technological advances. That background information is summarized in Section 7.1 below. Section 2 described Naval communications environments as discussed in related studies, and Section 3 developed a generic computer network model based on those studies. The communications environment that the Naval studies describe and the resulting model are summarized in Section 7.2 below.

Having acquired the necessary background for assessing the security standards, Section 4 began the primary objective of reviewing security guidance documents and standards in each of the areas of standardization, with an emphasis on network standards. The findings are summarized in Section 7.3 below.

A variety of security mechanisms can be implemented to provide security services in networks. Many of the standards describe or refer to specific mechanisms. Section 5 summarized the network security mechanisms that are available for implementation. Section 6 discusses additional factors that system designers should be aware of when choosing appropriate network security mechanisms and deciding where to place those mechanisms. The security mechanisms and additional factors are summarized in Section 7.4 below. Section 7.5 outlines briefly the direction for further research in future SBIR-II tasks.

7.1 Technological Advances

The area of networking and distributed processing is evolving faster than any other area of automation. As a result of these advances, an insatiable demand for even greater capabilities has developed. The user community has joined developers in envisioning new uses for systems, has become convinced that the developers will succeed in devising new products and technologies to meet their expectations, and have assured the developers that there is a market for those products and technologies. Developers have responded, and will continue to respond, to that demand with more powerful, more reliable, and more secure communications technologies and products.

The most significant improvement is bandwidth. Fiber optic media has emerged as the technology of the future, because it can support broad bandwidths at reasonable costs. Fiber Distributed Data Interface (FDDI) incorporates dual fiber optic rings to provide high bandwidth local area network communications. The Distributed Queue Dual Bus (DQDB) subnetwork of a metropolitan area network incorporates dual fiber optic rings to provide the Switched Multi-megabit Data Service (SMDS). The Broadband Integrated Services Digital Network (B-ISDN) incorporates cell-relay-based Asynchronous Transfer Mode (ATM) and Synchronous Optical Network (SONET) to provide high-performance multimedia wide area network communications.

Multimedia capabilities are the next step being demanded by the user community. Providers are responding by establishing teams consisting of representatives with backgrounds in telephony, cable broadcasting, and digital transmissions. Multimedia capabilities will change the way the Navy accomplishes its missions. Multimedia is identified as the basis for the Command Global Information Exchange System (GLOBIXS) network of the Copernicus architecture. Interactive video applications and video conferencing are expected to become common activities.

Network technology is evolving in other ways. Besides migrating to fiber, enterprise hubs, which introduce switched buses, are emerging. There are significant speed and security benefits associated with switched buses that cannot be realized on the traditional contention-based broadcast LAN.

The wireless LAN is another technology that will arise due to the success of the portable computer and the cellular telephone. Commercial production of wireless LANs is still several years off, but demand has created a market and that market is motivating developers. Wireless LANs will provide additional flexibility for Government agencies, but pose new challenges with respect to security.

From a security perspective for the military, the most important development efforts are in the area of multilevel processing. Standards bodies and system developers are well aware of the need to label subjects and objects and to base access control decisions on those labels. The mechanisms developed for the processing of military-oriented security labels will be capable of processing commercial security labels as well. Automation will someday (probably no less than 10 years) be capable of allowing cleared and uncleared users to share the same resources across multilevel networks. It has been claimed that the military would realize a significant cost savings by not having to clear all users to the highest level and by not having to install as many computers and telecommunications systems. The user community would also have more freedom to operate automated systems in less secure environments because they would be assured that the computers and networks can provide the necessary security internally.

7.2 The Naval Environment

Studies concerning communications security and Naval communications systems were reviewed in order to fully understand the Naval environment. First, two reports on generic security services and mechanisms were reviewed in order to understand the threats which may be brought to bear against Naval computer and communications assets, and to help assess the general categories of security mechanisms that may be successful in limiting harm from those threats. They were the *Information Security Report for MCCR System Developers,* produced by the Next Generation Computer Resources Security Task Group (NSTG), and *Security in Distributed Systems,* by Morrie Gasser. Next, studies concerning the architecture and security implications for four Naval systems were reviewed. They were:

- Battle Management Command and Control System
- Submarine Command System
- Integrated Interior Communications and Control (IC)2
- Copernicus, and supporting communications systems.

The NSTG report considered security services for host computers (i.e., operating system, DBMS, graphical interface, and backplane), networks, and the project support environment that could be implemented to counter specific threats identified in the report. It also identified system and protocol standards that could be specified in order to provide the needed security services.

The Gasser paper recognized the similarities between networks and host computer systems and discussed common security threats and generic services. The report identified very similar threats to those which were identified by NSTG.

While studying the specific Naval systems, required security services were identified. The services generally conformed to those discussed by the first two studies. This means that Naval systems typically require the types of security services that apply to all networked or distributed systems. Furthermore, the specific mechanisms that are required for the Navy systems are those that are commonly used. Figure 7.2-1 summarizes the security services and mechanisms suggested in the various studies and also indicates that standardization efforts have addressed provisions for all of the identified services and mechanisms.

	Services						Security Mechanisms																	
Security Requirements	Identification and Authentication	Confidentiality	Integrity	Access Control	Non-Repudiation	Service Assurance (Availability)	Discretionary Access Mechanisms	Mandatory Access Mechanisms	Labeling	Integrity Check Value	Audit and Accountability	Object Reuse	Trusted Path	Encryption	Key Management	Network and Security Management	One-Way Hash Algorithm	Digital Signatures	Certification Authorities	Challenge-Response Protocol	Sequence Numbers	Timestamping	Redundancy	Selective Routing
MCCR INFOSEC Study	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•								•
Distributed Systems Security	•	•	•	•	•	•	•	•	•	•				•			•	•	•	•	•	•	•	•
Integrated Interior C & C System	•	•	•	•		•	•	•	•		•	•	•	•	•	•							•	
Battle Management System	•	•	•	•	•	•	•	•	•	•	•			•		•								
Submarine Combat System	•	•	•	•	•	•	•	•	•	•	•			•		•								
Copernicus Security Requirements	•	•	•	•	•	•	•	•	•	•	•			•	•	•								
Provided by Standards	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•

Figure 7.2-1. Required vs. Provided Security Services and Mechanisms

Based on the findings of the reviews, a generic computer network model was developed as a tool to support the identification and placement of appropriate security services and mechanisms. The model (illustrated in Figure 3.0-1 in Section 3) consists of the following components:

- Host computers
- Local area networks
- Network switching elements
- Tactical transmission media
- Strategic communication system interfaces.

The areas of standardization were related to the model, so that security services needed in each area could be correlated to the model. Figure 7.2-2 shows the general categories of security functions needed in the areas of standardization, and shows in which network components the security functions are needed.

The Project Support Environment (PSE) is a unique area. Standardization in the other areas directly affect the types of services installed on the host or network system. Security services cannot be placed in the PSE. However, in order to develop trusted software for other areas of standardization, security must be considered and mechanisms developed for other areas must be installed in the PSE hosts and network components. Identification of industry-developed standards for the PSE will be initiated by the Integrated Software Engineering Environment Special Interest Group (ISEE-SIG) at the OSI Implementors' Workshop (OIW) sponsored by NIST.

	Primary Security Functions								Support Services			
Areas of Standardization	Identification & Authentication	Discretionary Access Control	Mandatory Access Control	Audit and Accountability	Service Assurance	Data Confidentiality	Data Integrity	Non-Repudiation	Labeling	Object Reuse	Trusted Path	Key Management
Operating System Host computers Network switching elements Strategic Communication System Interfaces	•	•	•	•	•				•	•	•	
Database Management System Host computers Network switching elements Strategic Communication System Interfaces	•	•	•	•	•	•	•		•	•	•	
Graphical User Interface Host computers			•			•	•		•		•	
Backplane Host computers	•	•	•		•	•	•		•	•		
Network Local area networks Tactical transmission media	•	•	•	•	•	•	•	•	•	•	•	•
Project Support Environment	•	•	•	•		•	•		•	•	•	

Figure 7.2-2. Security Functions Needed in Network Components

7.3 Status of Security Standardization

Standards for operating systems are well established. The DoD Trusted Computer System Evaluation Criteria, commonly known as the *Orange Book,* was developed in 1983 and has been widely followed and emulated. However, it should be noted that the Orange Book provides guidance for implementing secure stand-alone computers and does not include the network interfaces needed to make host computers useful in a networked environment.

The Federal Criteria, expected to be published as a FIPS PUB in 1994, is intended to replace the Orange Book. The Portable Operating System Interface (PC IX) Security Interface is still in draft status, but is fairly complete in defining sets of open system security interfaces. The Navy is developing operating system profiles with the goal that they will be POSIX-compliant when they are completed. While the operating system area of standardization is perhaps the most well established, it is in a state of transition and uncertainty.

Vendors have been attempting to define database security and develop multilevel secure database management systems for almost as long as the Orange Book has been in existence. However, standards for secure DBMSs are not well established. Security guidance documents were not introduced until 1991, and are still general in nature. Shared databases are much harder to secure than shared file systems because ownership of data elements cannot always be easily defined, there is a risk of compromise through inference, and aggregate issues have not been solved. On the other hand, technologies for defining access to databases are being standardized. This will facilitate improvements in security standardization.

There currently exist no graphical user interface security standards. However, there are well established standards on how graphical data is presented and how systems and applications interface with the graphical user interface regardless of platform or location on a network. GUI security implementations, such as the Compartmented Mode Workstation (CMW) typically implement features for sensitivity labeling and information labeling to support enforcement of access control policies. With the development of multilevel computer systems and networks, GUI security standards are needed.

Standards which describe security services for backplanes are in their infancy. The recommended practices for Futurebus+, a backplane which incorporates a traditional bus architecture, were published in 1992. Considerations for security services in the Futurebus+ recommended practices are impressive. The alternative architecture which will eventually emerge to replace the contention-based bus architecture is the High Speed Data Transfer Network, a system of dedicated point-to-point unidirectional transmission lines connecting processors, memory, and interface channels. It is particularly well suited for massively parallel computers. Standards that are being developed for the shared memory paradigm component of the High Speed Data Transfer Network do not directly address security, but do include mechanisms that support implementation of security services within the backplane.

Security standardization for networks is also relatively new, though there is a significant commitment in this area within industry and government. Standards that describe protocols which include security services are being adopted by standards bodies and are beginning to be used. Most have not yet been widely implemented, and are therefore not stable. Vendors hesitate to implement products based on draft standards because standards often undergo significant revision when being upgraded from draft to international standard status. Even when standards are finalized, they are not stable. Stability comes when the standards have been implemented and there is little technological pressure to change them. Major flaws requiring correction may be discovered during implementation. Since many of the International Standards are not stable, existing standards that are more widely implemented (e.g., TCP, IP, SP3, SP4, SNMP, and others) may be used in the interim.

Desired security services, identified in the Navy case studies, have been discussed by standards committees and are being incorporated into standards. In the past five years, the following guidance documents and standards related to networks have been developed:

- **Evaluation criteria and guidelines**
- **Profiles** consisting of selected lists of standards and specifications
- **Architectures** that define placement of security services and mechanisms
- **Frameworks** that define basic concepts for a security mechanism that may be available in many layers
- **Security models** that address implementation of services at particular layers
- **Standards that specialize models** to serve as protocol construction tools
- **Military profiles** for lower layer protocols
- **Lower layer security protocols**
- **Upper layer security protocols and mechanisms.**

7.4 *Security Mechanisms and Placement Factors to Consider*

Security mechanisms that are needed in networks are categorized according to the following security services, as shown in Figure 7.4-1:

- Authentication
- Access Control
- Audit and Accountability
- Confidentiality
- Integrity
- Non-Repudiation
- Service Assurance.

Authentication may be necessary to be performed within a host computer by the operating system, database management system, application programs, and backplane, and within the network for communications. By confirming the identity of a subject, authentication supports access control, accountability, and integrity services.

In some cases authentication is virtually nonexistent. For example, the backplane may accept the context (e.g. the module's address) as sufficient evidence for authentication. Another example of weak authentication would be for an operating

Authentication

- Peer Address Checking
- Authentication Exchange
  - Passwords
  - Supporting Devices
    - Hand-held devices
    - Smart cards
    - Biometric readers
  - Challenge-Response
    - Symmetric Encipherment
    - Asymmetric Encipherment
- Certification Authority
- Continuity of Authentication

Access Control

- System-Oriented Access Control
  - Object Reuse
  - Trusted Path
  - Connection Timeout
- Discretionary Access Control
  - Access Control Lists
  - Capabilities
  - Authentication Server
- Mandatory Access Control
  - Security Labels
  - Routing Control

Audit and Accountability

- Audit Mechanism
- Alarm Mechanism

Non-Repudiation

- Digital Signature
- Notary Service

Confidentiality

- Physical Protection
  - Isolation
  - Selective Routing
- Information Hiding
  - Symmetric Encipherment
  - Asymmetric Encipherment
  - Traffic Padding
- Partial Accessibility
  - Internal Fragmentation
  - Data Scattering

Integrity

- Error Detection
  - Error Detection Codes
  - Integrity Check Values (ICV)
  - Message Digests
- Encryption for Integrity
  - Cryptographic Seal
  - Digital Signature
- Sequence Protection
  - Sequence Numbers
  - Cryptographic Chaining
  - Timestamps
  - Reflection Bits
  - Source Addresses

Service Assurance

- Redundant Components
- Fault Tolerance
- Priority Processing

Figure 7.4-1. Generic Security Mechanisms

system, DBMS, or network to accept the subject's simple assertion of identity with no credentials as proof. Generally, however, an authentication exchange is required to strengthen the level of trust. Trusted third parties, called *certification authorities*, can act as authorizing entities to provide information to be used to support mutual authentication among entities on a network. Hand-held user authentication devices, smart cards, and biometric readers may be necessary in environments where a high level of individual authentication is needed.

There are two types of access control mechanisms: physical and technical. Physical access controls provide isolation to prevent tampering and are applied to backplanes, dedicated stand-alone computers, the project support environment, and occasionally to network cables. If computers are networked, the perimeter of the physical control zone must be extended to enclose all components of the network. If the computer or network is shared or partially located outside the physical control zone, technical access controls must be applied. Technical access control mechanisms must reside in the host operating system and in the network management software, as well as in any shared DBMS. If the host is to operate in the multi-level security mode, technical access control mechanisms may be required for the backplane as well.

System-oriented access control mechanisms are used to reduce vulnerabilities associated with the design of the system. Examples of these are object reuse and trusted path. System-oriented access controls are not concerned with the rights of individual claimants, but with the ability of the host computer or network to limit access to information contained in the system. Access control can only be provided within the context of a defined security policy. The security policies for most systems or networks base access on the identity of the subject, membership in particular groups, and ownership of files. This is called discretionary or identity-based access control. In addition, some security policies also require that the subject's sensitivity label dominate the sensitivity label of the object for which access is requested. This is called mandatory or rule-based access control.

Security audit and alarm mechanisms are needed in the control software of operating systems and networks, and require input from DBMSs and applications.

Non-repudiation mechanisms are used in networks to provide proof of the origin or delivery of data. They counter false denial by an originator that the data has been sent and false denial by a recipient that the data has been received.

Digital Signatures are used to provide non-repudiation. A digital signature establishes the source of data and protects against forgery by other parties including the destination. Non-repudiation services may require the existence of a trusted third-party, called a notary, who authenticates the evidence, verifies its integrity, and arbitrates disputes that arise as a result of repudiated messages.

Confidentiality mechanisms protect against disclosure by protecting the representation of the information and its attributes from disclosure, and by protecting the representation rules from disclosure. They are implemented in all of the areas of standardization except the GUI, and are implemented in all of the components of the Navy generic computer network model. There are three types of confidentiality mechanisms:

- Mechanisms that provide physical access protection:
  - Isolation and physical protection
  - Selective routing
- Mechanisms that hide the data:
  - Symmetric encipherment
  - Asymmetric encipherment
  - Traffic padding
- Mechanisms that make the data only partially accessible while in storage or transmission, such that the data cannot be completely recreated from the limited amount of data that could be collected:
  - Internal fragmentation
  - Data scattering (e.g., frequency hopping).

Integrity mechanisms detect unauthorized modifications of data in storage (files, records) and in transit (messages, fields). These may be accidental, caused by hardware error or noise on the channel, or intentional, such as active wiretapping. It is access controls, not integrity mechanisms, that are intended to prevent unauthorized modifications. Integrity mechanisms are responsible for detecting such occurrences in time that they can be corrected without having a serious impact on operations. Integrity mechanisms and access controls are strongly supported by confidentiality mechanisms, particularly encryption. There are three types of integrity mechanisms:

- Error Detection
- Encryption for Integrity
- Message Sequence Protection.

Service assurance is provided by mechanisms such as redundancy, fault tolerance, and priority processing.

System designers must consider the level of security demanded by the environment, and the capabilities available in the operating system, DBMS, network, and applications. As more security services are designed into operating systems, DBMSs, and networks, more options will be available to system developers. Factors concerning the choice and placement of network security mechanisms must be considered when evaluating the following architectural alternatives for secure computer and communications systems:

- Designing a multilevel system versus designing separate system high or dedicated systems at unclassified and single-classification levels
- Placement of security services in particular areas of standardization
- Implementation of security services in application processes versus implementation in the communication protocols
- Placement of communication security protocols in host computers versus placement in external devices
- Using distributed versus centralized security mechanisms.

Multilevel operations is a primary technological issue for most of the areas of standardization. Current technology requires that separate classified and unclassified networks be developed and maintained independently because technology cannot be trusted to maintain the necessary separation. Any exchange of information between classified and unclassified networks must be processed manually or through a trusted multilevel guard. When MLS-capable computers, DBMSs, and networks are commercially available, system engineers will be able to design internetworks of commercial and government systems operating at various classified and unclassified levels. The benefit is that only one network will be necessary to support all operations of the organization and to allow interconnection to virtually any strategic communications system.

In assessing whether Authentication, Access Control, Audit and Accountability, Confidentiality, Integrity, Non-Repudiation, and Service Assurance should be provided by the host computers or the network, the answer for most systems is a combination. While it is possible for application processes and security kernels on host computers to provide some of the security services, it may be more efficient to develop one set of security services and place those services in the OSI stack rather than developing individual mechanisms for each application process. When the environment demands, or when communications protocols are insufficient, the application programs and security kernels may provide the security services. Operating systems are responsible for performing identification and authentication, access control, and audit and accountability, and they must provide appropriate levels of confidentiality, integrity, and reliability based on their implementation-specific security policies. Applications and DBMSs may also be designed to perform many of the services to meet implementation-specific requirements.

There are security design options concerning backplanes provided physical access is controlled so that external listening devices cannot be attached. This may change as parallel processing and multilevel technologies advance. While applications and hosts have not been able to place their trust in networks of the past, the trend is toward providing full-service networks with interfaces for applications to specify the services needed.

For economic reasons, commercial networks typically place security services in higher layers and on devices resident on the host computer. For security reasons, military networks often place security services in front end devices where access can be strictly limited. The trade-off is cost versus the degree of physical protection. Communications security services that are implemented in software can be widely distributed and installed on existing systems without additional hardware. These mechanisms are the least secure, and incur a processing penalty by competing for CPU cycles. Therefore, security mechanisms implemented in software within hosts process traffic more slowly than secure front ends. Communications security services that are implemented in chips or on circuit boards can also be produced economically and be distributed and installed relatively easily. These are more secure because they require that an attacker have physical access. Hosts with embedded security mechanisms that are implemented in hardware also process traffic faster than either hosts with mechanisms implemented in software or front-end security devices, and generally incur less programmatic risk to develop. Communications security services that are implemented in external devices such as security card devices and secure front-ends are the most expensive to implement and the most physically protected from attack.

An additional factor that influences the decision on where to implement COMSEC services is the type of external WAN interfaces that are desired. In order for classified hosts to communicate over untrustworthy networks, such as commercial B-ISDN or Internet, end-to-end encryption is required, either internally or within front-end devices.

Security functionality can be distributed (implemented primarily within hosts) or centralized (implemented primarily within a security server). Direct key distribution is an example of distributed security functionality. The use of a Key Distribution Center (KDC) is an example of centralized security functionality. Several fundamental factors must be considered when deciding whether to implement centralized or distributed security functionality. In general, distributed security mechanisms require less overhead and are more efficient than centralized security mechanisms. They are also less vulnerable to denial of service attacks because disabling the security server would disrupt all service in a centralized system. On the other hand, distributed systems are more costly since a greater number of components throughout the network must incorporate additional trustworthy security functionality.

7.5 Further Research

Internetworking capabilities are becoming increasingly expected for the conduct of Government organization missions. Applications are being developed to meet that demand. Operating systems, DBMSs, and graphical user interfaces are migrating toward distributed processing. Network technology is evolving faster than any other area of automation. Multimedia and wireless technologies are becoming a reality and they introduce security challenges. Fortunately, the industry has recognized that applications and operating systems are dependent on the network to provide security services and is responding with network security standards for mechanisms and interfaces to provide those services to the hosts. It is the standards that can allow the system designers to achieve the elusive goal of interoperability.

The impact of this trend, with respect to the generic computer network model, is that multilevel hosts, networks, and switching elements are needed to allow full connectivity. In addition, all three components must provide the standard security services in a manner that application designers can select which services they need to use and can have confidence that the services will be reliable. These two requirements are independent. Reliable security services must be provided, regardless of the status of multilevel technologies; and multilevel capabilities must be pursued, regardless of the status o‚ standard security service mechanisms.

Further research efforts and related activities that will occur in Tasks 4, 5, and 6 of this SBIR Phase II effort include:

- Identify architectural alternatives for network security products that implement security services and mechanisms to satisfy security requirements (including an architecture to support end-to-end encryption at Layer 2 in a LAN/WAN internetwork)
- Compare the alternative architectures with respect to performance, cost, and security risk imposed by the threat
- Estimate the number of products required to meet near-term and far-term security requirements
- Survey the market to assess what network security products currently exist or are being developed, highlighting those that support current or emerging security standards. Examples are:
  - SPAWAR Embeddable INFOSEC Product (EIP)
  - Motorola Network Encryption System (NES)
  - Motorola CANEWARE Front End and CANEWARE Control Processor
  - OSF Distributed Computing Environment (DCE)
  - Boeing MLS LAN Secure Network Server

  - Verdix Secure LAN (VSLAN)
  - Xerox Encryption Unit (XEU)
  - GTE Tactical End-to-End Device (TEED)
  - Kerberos Authentication Service Products
  - Multilevel Information Systems Security Initiative (MISSI) Products (including Appliqué devices and the Secure Computing LOCK Secure Network Server)
  - Asynchronous Transfer Mode (ATM) Encryption Devices
  - Devices that support privacy-enhanced electronic mail (PEM)

- Develop functional design documentation for additional network security products that are needed to support required security architectures

- Identify market opportunities for the additional network security products and provide briefings to vendors who have experience in developing INFOSEC products to stimulate an interest in developing these products.

Appendices

This Page Intentionally Left Blank

Appendix A

Acronyms

This Page Intentionally Left Blank

Appendix A

Acronyms

ACK	Acknowledgment
ACL	Access Control List
ACSE	Association Control Service Element
ADP	Automated Data Processing
AIS	Automated Information System
ANSI	American National Standards Institute
API	Application Programmer's Interface
APP	Applications Portabi!ity Profile
ASE	Application Service Element
ATM	Asynchronous Transfer Mode
AUTODIN	Automatic Digital Network
B-ISDN	Broadband Integrated Services Digital Network
CAD/CAM	Computer-Aided Design / Computer-Aided Manufacturing
CASE	Computer-Aided Software Engineering
CCC	CINC Command Complex
CCR	Commitment, Concurrency and Recovery
CCITT	International Telegraph and Telephone Consultative Committee
CD	Committee Draft
CGM	Computer Graphics Metafile
CINC	Commander in Chief
CIPSO	Commercial Internet Protocol Security Option
CISS	Center for Information Systems Security (Previously DISSP)
CLNP	Connectionless Network Protocol
CLTP	Connectionless Transport Protocol
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CMW	Compartmented Mode Workstation
COMPUSEC	Computer Security
COMSEC	Communications Security
COTS	Commercial off-the-shelf

Appendix A – Acronyms (continued)

CRC	Cyclic Redundancy Check
CSL	Common Security Label
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSS	Communications Support System
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DAC	Discretionary Access Control
DBMS	Database Management System
DCS	Defense Communications System
DDN	Defense Data Network
DES	Data Encryption Standard
DGSA	DoD GULS Security Architecture
DIA	Defense Intelligence Agency
DIB	Directory Information Base
DIS	Draft International Standard
DISSP	Defense Information System Security Program
DMS	Defense Message System
DoD	Department of Defense
DODIIS	DoD Intelligence Information System
DON	Department of the Navy
DQDB	Distributed Queue Dual Bus
DSA	Digital Signature Algorithm
DSE	Distributed Computing Environment
DSS	Digital Signature Standard
DSSCS	Defense Special Security Communications System
E3	End-to-End Encryption
ECMA	European Computer Manufacturers Association
EDI	Electronic Data Interchange
EHF	Extremely High Frequency
EIP	Embeddable INFOSEC Product
ELF	Extremely Low Frequency
ES	End System
ES-IS	End System to Intermediate System

Appendix A – Acronyms (continued)

FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standards
FTAM	File Transfer, Access and Management
FTS2000	Federal Telephone System 2000
Gbps	Gigabits Per Second
GKS	Graphics Kernel System
GLOBIXS	Global Information Exchange Systems
GNMP	Government Network Management Profile
GOSIP	Government OSI Profile
GUI	Graphical User Interface
GULS	Generic Upper Layer Security
HF	High Frequency
HSDTN	High Speed Data Transfer Network
IBAC	Identity-Based Access Control
(IC)^2	Integrated Interior Communications and Control System
ICV	Integrity Check Value
IDRP	Inter-Domain Routing Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	Internet Engineering Task Force
IFIP	International Federation of Information Processing
IGES	Initial Graphics Exchange Specification
IGOSS	Industry and Government Open Systems Specification
INFOSEC	Information Security
IPSO	Internet Protocol Security Option
IRD	Information Resource Dictionary
IRDS	Information Resource Dictionary System
IS	International Standard
ISDN	Integrated Services Digital Network
ISEE	Integrated Software Engineering Environment
IS-IS	Intermediate System to Intermediate System

Appendix A – Acronyms (continued)

ISO	International Standards Organization
IT	Information Technology
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union (formerly CCITT)
ITU-T	ITU, Telecommunications Sector
KDC	Key Distribution Center
KEK	Key Encrypting Key
KMAP	Key Management Application Process
KMP	Key Management Protocol
KTC	Key Translation Center
LAN	Local Area Network
LLC	Logical Link Control
LPE	Low Probability of Exploitation
LPI	Low Probability of Interception
LSAP	Link Service Access Point
MAC	Mandatory Access Control
MAC	Media Access Control
MAN	Metropolitan Area Network
Mbps	Megabits Per Second
MCCR	Mission-Critical Computer Resources
MD4	Message Digest Algorithm 4
MD5	Message Digest Algorithm 5
MDA	Message Digest Algorithm
MHS	Message Handling System
MIME	Multipurpose Internet Mail Extensions
MISSI	Multilevel Information Systems Security Initiative
MLS	Multi-Level Security
MMG	Multibus Manufacturers Group
MOTIS	Message-Oriented Text Interchange System
MSP	Message Security Protocol
NAK	Negative Acknowledgment
NAPI	North American PCTE Initiative

Appendix A – Acronyms (continued)

NCSC	National Computer Security Center
NDI	Non-Developmental Item
NES	Network Encryption System
NGCR	Next Generation Computer Resources
NIST	National Institute of Standards and Technology
NLSP	Network Layer Security Protocol
NOFORN	Not For Foreign Release
NRaD	Naval Research and Development
NRL	Naval Research Laboratory
NSA	National Security Agency
NSC	DODIIS Network Support Center
NSE	Network Switching Element
NSTG	NGCR Security Task Group
NSWC	Naval Surface Warfare Center
NUSC	Naval Undersea Systems Center
NUWC	Naval Undersea Warfare Center
OIW	OSE Implementors' Workshop
OMG	Object Management Group
OSE	Open System Environment
OSF	Open Software Foundation
OSI	Open Systems Interconnection
OSIF	Operating System Interface
OSI RM	OSI Reference Model
PCI	Protocol Control Information
PCTE	Portable Common Tools Environment
PDU	Protocol Data Unit
PEM	Privacy-enhanced Electronic Mail
PHIGS	Programmer's Hierarchical Interactive Graphics System
PICS	Protocol Implementation Conformance Statement
PIN	Personal Identification Number
POSIX	Portable Operating System Interface
PSE	Project Support Environment

Appendix A – Acronyms (continued)

PSN	Packet Switched Network
QOS	Quality of Service
RBAC	Rule-Based Access Control
RDA	Remote Database Access
RDBMS	Relational Database Management System
RFC	Request for Comments
RIPSO	Revised Internet Protocol Security Option
RSA	Rivest, Shamir, and Adelman
SA	Security Association
SAFENET	Survivable Adaptable Fiber Optic Embedded Network
SAP	Service Access Point
SATCOM	Satellite Communications
SBIR	Small Business Innovative Research
SCI	Scalable Coherent Interface
SCI	Sensitive Compartmented Information
SCOMP	Secure Computer Processor
SDE	Secure Data Exchange Protocol
SDNS	Secure Data Network System
SDU	Service Data Unit
SE	Service Element
SE-ASE	Security Exchange – Application Service Element
SESE	Security Exchange Service Element
SHA	Secure Hash Algorithm
SHF	Super High Frequency
SHS	Secure Hash Standard
SILS	Standard for Interoperable LAN / MAN Security
SMDS	Switched Multi-megabit Data Service
SMFA	Specific Management Functional Area
SMIB	Security Management Information Base
SMP	Simple Management Protocol
SNICP	Subnetwork-Independent Convergence Protocol
SNMP	Simple Network Management Protocol

Appendix A – Acronyms (continued)

SONET	Synchronous Optical Network
SP2L	Security Protocol 2 for LANs
SP3	Security Protocol 3
SP4	Security Protocol 4
SPAWAR	Space and Naval Warfare Systems Command
SQL	Standard Query Language
SSL	Standard Security Label for GOSIP
STS	SAFENET Time Service
TADIXS	Tactical Data Information Exchange System
TAFIM	Technical Architecture Framework for Information Management
TCB	Trusted Computing Base
TCC	Tactical Command Center
TCP / IP	Transmission Control Protocol / Internet Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TDI	Trusted DBMS Interpretation of TCSEC
TEED	Tactical End-to-End Device
TEK	Traffic Encryption Key
TIS	DODIIS TCP/UDP/IP Transport Interface Software
TLSP	Transport Layer Security Protocol
TNI	Trusted Network Interpretation of TCSEC
TPDU	Transport Protocol Data Unit
TRANSEC	Transmission Security
TS	Top Secret
UHF	Ultra High Frequency
UPS	Uninterruptible Power Supply
VHF	Very High Frequency
VITA	VMEbus International Trade Association
VSLAN	Verdix Secure LAN
WAN	Wide Area Network
WWMCCS	Worldwide Military Command and Control System
XEU	Xerox Encryption Unit

This Page Intentionally Left Blank

Appendix B

References

This Page Intentionally Left Blank

Appendix B

References

[ANSI 88A] American National Standards Institute, *Digital Hierarchy – Optical Interface Rates and Formats Specifications,* ANSI T1.105-1988, ANSI T1X1.5, 1988.

[ANSI 88B] American National Standards Institute, *Digital Hierarchy – Optical Parameters,* ANSI T1.106-1988, ANSI T1X1.5, 1988.

[ANSI 89] American National Standards Institute, *Addendum to ANSI T1.105-1988, Digital Hierarchy – Optical Interface Rates and Formats Specifications,* (Phase 2 SONET), ANSI T1X1.5, 1989.

[ANSI 92A] American National Standards Institute, *Information Resource Dictionary System (IRDS) Services Interface*, ANSI Standard X3.185-1992 (ISO 10728), 1992.

[ANSI 92B] American National Standards Institute, *Frame Relay Bearer Service Architectural Framework and Service Description,* draft standard T1.606, 1992, (aligned with CCITT Q.922).

[BAILEY 93] B. Bailey, "Trends in Networking," *Handbook of Local Area Networks – 1993-94 Yearbook,* Auerbach Publications, 1993, pp. S-259 – S-266.

[BARKER 89] L. K. Barker, "Network Management and Diagnostics for Secure LANs," *Local Area Network Security, Lecture Notes in Computer Science 396, Springer-Verlag*, 1989, pp. 139-152.

[BLACK 91] U. D. Black, OSI – *A Model for Computer Communications Standards*, Prentice Hall, Englewood Cliffs, New Jersey, 1991.

[BLACK 92A] U. D. Black, *Network Management Standards – The OSI, SNMP and CMOL Protocols*, McGraw-Hill, New York, New York, 1992.

[BLACK 92B] U. D. Black, *TCP/IP and Related Protocols*, McGraw-Hill, New York, New York, 1992.

[BLACK 93] U. D. Black, *Computer Networks – Protocols, Standards, and Interfaces*, Second Edition, Prentice Hall, Englewood Cliffs, New Jersey, 1993.

Appendix B – References (continued)

[CCITT 91] The International Telegraph and Telephone Consultative Committee (CCITT), *Broadband Integrated Services Digital Network (B-ISDN) Asynchronous Transfer Mode (ATM) Functional Characteristics*, Recommendation I.150, 1991.

[CCITT 92] The International Telegraph and Telephone Consultative Committee (CCITT), *ISDN Data Link Layer Specification for Frame Mode Bearer Services,* Recommendation Q.922, 1992.

[CLARK 87] D. D. Clark and D. R. Wilson, "A Comparison of Commercial and Military Computer Security Policies," *Proceedings of the 1987 IEEE Symposium on Security and Privacy*, April 1987.

[COMER 91] D. E. Comer, *Internetworking With TCP/IP, Volume I: Principles, Protocols, and Architecture*, Second Edition, Prentice Hall, Englewood Cliffs, New Jersey, 1991.

[DoD 85] Department of Defense, *Trusted Computer System Evaluation Criteria (TCSEC)*, DoD 5200.28-STD, December 1985.

[DoD 91] Department of Defense, *Military Standard – Network Management for DoD Communications,* MIL-STD-1813, unapproved working draft, June 10, 1991, (superseded by MIL-STD-2045-38000 [DoD 93A]).

[DoD 93A] Department of Defense, *Military Standard – Network Management for DoD Communications,* MIL-STD-2045-38000, (supersedes MIL-STD-1813 [DoD 91]), unapproved working draft, January 4, 1993.

[DoD 93B] Department of Defense, *Military Handbook – Network Management for DoD Communications,* MIL-HDBK-1351, unapproved working draft, undated, approximate publication date: November 1993.

[FRAME 90] Frame Relay Consortium: DEC, Northern Telecom Inc., and StrataCom Inc., *Frame Relay Specification with Extensions Based on Proposed T1S1 Standards, Revision 1,* Document Number 001-208966, September 18, 1990.

[GASSER 91] M. Gasser, *Security in Distributed Systems*, 1991.

[GOSIP 93] The GOSIP Institute, *Internet 2000: A Protocol Framework to Achieve a Single Worldwide TCP/IP/OSI/CLNP Internet by Year 2000*, A White Paper, Version 3.0, June 4, 1993.

Appendix B – References (continued)

[GRUMMAN 92] Grummand Data Systems, *Secure SAFENET Communications*, June 30, 1992.

[HALSALL 92] F. Halsall, *Data Communications, Computer Networks and Open Systems*, Third Edition, Addison-Wesley Publishing Company, Reading, Massachusetts, 1992.

[HEALY 89] E. M. Healy, "SONET Overview and Standards Status," *Proceedings of the IEEE SONET Symposium*, November 1989.

[HEBRAWI 93] B. Hebrawi, *Open Systems Interconnection – Upper Layer Standards and Practices*, McGraw-Hill, New York, New York, 1993.

[IEEE 88] Institute of Electrical and Electronics Engineers, *IEEE Standard Portable Operating System Interface for Computer Environments (POSIX)*, IEEE Std 1003.1-1988, August 22, 1988.

[IEEE 90] Institute of Electrical and Electronics Engineers, *IEEE Standard for Distributed Queue Dual Bus (DQDB) Subnetwork of a Metropolitan Area Network (MAN)*, IEEE Standard 802.6, 1990.

[IEEE 92A] Institute of Electrical and Electronics Engineers, *Standard for Futurebus+ — Logical Protocol Specification*, IEEE Standard 896.1-1991, March 10, 1992. (Amended in 1993. Became ISO 10857 in 1994.)

[IEEE 92B] Institute of Electrical and Electronics Engineers, *Standard for Futurebus+ — Physical Layer and Profile Specification*, IEEE Standard 896.2-1991, April 24, 1992.

[IEEE 92C] Institute of Electrical and Electronics Engineers, *Standard for Futurebus+ — Recommended Practices*, Unapproved Draft IEEE Standard P896.3/D4.1, IEEE Computer Society, October 1992.

[IEEE 92D] Institute of Electrical and Electronics Engineers, *Draft Standard for Information Technology -- Portable Operating System Interface (POSIX) -- Part 1: System Application Program Interface (API) Amendment #: Protection, Audit and Control Interfaces,* Unapproved Draft IEEE P1003.6.1/D13, November 1992.

[IEEE 92E] Institute of Electrical and Electronics Engineers, Draft Standard for *Information Technology -- Portable Operating System Interface (POSIX) -- Part 2: Shell and Utilities – Amendment #: Protection and Control Utilities*, Unapproved Draft IEEE P1003.6.2/D13, November 1992.

Appendix B – References (continued)

[IEEE 93A] Institute of Electrical and Electronics Engineers, *IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS)*, IEEE Standard 802.10-1992, February 5, 1993.

[IEEE 93B] Institute of Electrical and Electronics Engineers, *IEEE Standard for Scalable Coherent Interface (SCI)*, IEEE Standard 1596-1992, August 2, 1993.

[IEEE 93C] Institute of Electrical and Electronics Engineers, *IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS) Clause 3 -- Key Management Protocol,* Unapproved Draft IEEE 802.10c/D2, September 12, 1993.

[IEEE 93D] Institute of Electrical and Electronics Engineers, *Standard for Futurebus+ — Profile M (Military),* IEEE Standard 896.5-1993, 1993.

[IEEE 93E] Institute of Electrical and Electronics Engineers, *IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS) - Secure Data Exchange Security Labels (SDE-SL),* Unapproved Draft IEEE 802.10g/D0, November 5, 1993.

[ISO 84] International Standards Organization, *Information Processing Systems — Open Systems Interconnection Basic Reference Model,* ISO 7498, October 1984.

[ISO 89A] International Standards Organization, *Information Processing Systems—Open Systems Interconnection Basic Reference Model — Part 2: Security Architecture*, ISO 7498-2, February 1989 (also ITU-T Recommendation X.800).

[ISO 89B] International Standards Organization, Information Processing, *Systems — Fiber Distributed Data Interface (FDDI) — Part 1: Physical Layer Protocol* (PHY), ISO 9314-1, April 1989.

[ISO 89C] International Standards Organization, *Information Processing Systems — Fiber Distributed Data Interface (FDDI) — Part 2: Token Ring Media Access Control,* ISO 9314-2, June 1989.

[ISO 90A] International Standards Organization, Inf*ormation Processing Systems — Fiber Distributed Data Interface (FDDI) — Part 3: Physical Layer Medium Dependent (PMD),* ISO 9314-3, October 1990.

Appendix B – References (continued)

[ISO 90B] International Standards Organization, *Information Processing Systems — Local Area Networks — Part 2: Logical Link Control, ANSI/IEEE Std 802.2,* ISO 8802-2, January 12, 1990 (also ITU-T Recommendation X.810).

[ISO 90C] International Standards Organization, *Information Technology — Text Communication, Message-Oriented Text Interchange System — Part 1: System and Service Overview,* ISO 10021-1, Dec. 1990.

[ISO 90D] International Standards Organization, *Information Processing Systems — The Directory — Part 8: Directory Authentication,* ISO 9594-8, 1990.

[ISO 90E] International Standards Organization, *Information Technology – Portable Operating System Interface (POSIX) – Part 1: System Application Program Interface (API) [C Language],* ISO/IEC 9945-1, December 7, 1990. (Cross Reference: IEEE Std 1003.1)

[ISO 92A] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Guide to Open Systems Security,* Working Draft Technical Report, May 1992.

[ISO 92B] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 1: Security Frameworks Overview,* ISO / IEC CD 10181-1, July 21, 1992.

[ISO 92C] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 3: Access Control Framework, ISO/IEC CD 10181-3.2,* October 9, 1992.

[ISO 92D] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 6: Confidentiality Framework, ISO/IEC CD 10181-6, (changed to part 4 in 1993),* Dec. 11, 1992.

[ISO 92E] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 5: Integrity Framework, ISO/IEC CD 10181-5,* December 11, 1992.

Appendix B – References (continued)

[ISO 92F] International Standards Organization, *Information Processing Systems — Fiber Distributed Data Interface (FDDI) — Part 5: Hybrid Ring Control, ISO 9314-5, (FDDI-II)*, JTC1 Project Draft, 1992.

[ISO 93A] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 2: Authentication Framework*, ISO/IEC DIS 10181-2, June 1, 1993 (also ITU-T Recommendation X.811).

[ISO 93B] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 4: Non-repudiation Framework, ISO/IEC CD 10181-4*, (changed to part 6 in 1993), May 24, 1993 (also ITU-T Recommendation X.813).

[ISO 93C] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 7: Security Audit Framework*, ISO/IEC CD 10181-7, March 16, 1993 (also ITU-T Recommendation X.816).

[ISO 93D] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Generic Upper Layers Security (GULS) – Part 1: Overview, Models and Notation*, ISO/IEC DIS 11586-1, July 27, 1993.

[ISO 93E] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Generic Upper Layers Security (GULS) – Part 2: Security Exchange Service Element (SESE) Service Definition*, ISO/IEC DIS 11586-2, July 1993.

[ISO 93F] International Standards Organization, Information Technology — Information Retrieval, Transfer and Management for OSI, Generic Upper Layers Security (GULS) – Part 3: Security Exchange Service Element Protocol Specification, ISO/IEC DIS 11586-3, July 23, 1993.

[ISO 93G] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Generic Upper Layers Security (GULS) – Part 4: Protecting Transfer Syntax Specification*, ISO/IEC DIS 11586-4, July 27, 1993.

Appendix B – References (continued)

[ISO 93H] International Standards Organization, *Information Processing Systems — Remote Database Access (RDA),* ISO/IEC DIS 9579, 1993.

[ISO 93I] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Lower Layers Security Model,* Working Draft, Proposed Technical Report, August 1993.

[ISO 93J] International Standards Organization, *Information Processing Systems — Reference Model of Data Management,* ISO 10032, December 1993.

[ISO 93K] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 4: Confidentiality Framework,* ISO/IEC DIS 10181-4, June, 1993 (also ITU-T Recommendation X.814).

[ISO 93L] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 5: Integrity Framework,* ISO/IEC DIS 10181-5, June, 1993 (also ITU-T Recommendation X.815).

[ISO 93M] International Standards Organization, *Information Technology — Portable Operating System Interface (POSIX) – Part 2: Shell and Utilities,* ISO/IEC 9945-2, 1993.

[ISO 94A] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Upper Layers Security Model,* (ISO / IEC CD 10745). Final text accepted November 1993. International Standard to be published in 1994 (will also be ITU-T Recommendation X.803).

[ISO 94B] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Network Layer Security Protocol,* ISO 11577. Final text accepted November 1993. International Standard to be published in 1994.

[ISO 94C] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Transport Layer Security Protocol,* ISO/IEC 10736. Final text accepted November 1993. International Standard to be published in 1994.

Appendix B – References (continued)

[ISO 94D] International Standards Organization, *Information Technology — Telecommunications and Information Exchange Between Systems, Transport Layer Security Protocol (Amendment 1 - Security Association Protocol*). Final text accepted November 1993. International Standard to be published in 1994.

[ISO 94E] International Standards Organization, *Information Technology — Information Retrieval, Transfer and Management for OSI, Security Frameworks in Open Systems – Part 3: Access Control Framework,* ISO/IEC DIS 10181-3., January 1994 (also ITU-T Recommendation X.812).

[ISO 94F] International Standards Organization, *Information Technology — Futurebus+ – Logical Protocol Specification,* ISO/IEC 10857, 1994 (also IEEE 896.1-1993).

[KIRKPAT 89] L. E. Kirkpatrick, "Why is a LAN a LAN?," *Local Area Network Security, Lecture Notes in Computer Science 396,* Springer-Verlag, 1989, pp.3-4

[LAMBERT 89] P. A. Lambert, *"Architectural Considerations for LAN Security Protocols," Local Area Network Security, Lecture Notes in Computer Science 396,* Springer-Verlag, 1989, pp. 5-11.

[LAMBERT 90] P. A. Lambert, *"The Lowdown on Lower Layer Security Protocols," Proceedings of the Sixth Annual Computer Security Applications Conference,* December 1990.

[LAMBERT 93] P. A. Lambert, *"Layer Wars: Protect the Internet with Network Layer Security," Proceedings of the Privacy and Security Research Group Workshop on Network and Distributed System Security,* Feb. 1993.

[LYNCH 93] D. C. Lynch and M. T. Rose, editors, *Internet System Handbook, Addison-Wesley Publishing Company,* Greenwich, Connecticut, 1993.

[MALAMUD 92] C. Malamud, *Stacks – Interoperability in Today's Computer Networks, Prentice Hall,* Englewood Cliffs, New Jersey, 1992.

[MAUGHAN 92] W. D. Maughan, *Standards for Computer Systems Security: An Interoperability Analysis of SDNS SP3 and ISO NLSP,* April 15, 1992.

Appendix B – References (continued)

[MICHAEL 93] W. H. Michael, W. J. Cronin, and K. F. Pieper, FDDI: *An Introduction to Fiber Distributed Data Interface, Digital Press,* Burlington, Massachusetts, 1993.

[MOTO 92A] Motorola Codex, *The Basics Book of Information Networking, Motorola University Press, Addison-Wesley Publishing Company, Reading,* Massachusetts, 1992.

[MOTO 92B] Motorola Codex, *The Basics Book of ISDN,* Motorola University Press, Addison-Wesley Publishing Company, Reading, Massachusetts, 1992.

[MOTO 92C] Motorola Codex, *The Basics Book of X.25* Packet Switching, Motorola University Press, Addison-Wesley Publishing Company, Reading, Massachusetts, 1992.

[MOTO 93A] Motorola Codex, The Basics Book of OSI and Network Management, Motorola University Press, Addison-Wesley Publishing Company, Reading, Massachusetts, 1993.

[MOTO 93B] Motorola Codex, *The Basics Book of Frame Relay, Motorola* University Press, Addison-Wesley Publishing Company, Reading, Massachusetts, 1993.

[MUFTIC 93] S. Muftic, et al, Security *Architecture for Open Distributed Systems,* John Wiley & Sons Limited, West Sussex, England, 1993.

[MULLER 93] N. J. Muller, *"Bridging Strategies for LAN Internets," Handbook of Local Area Networks – 1993-94 Yearbook,* Auerbach Publications, 1993, pp. S-99 – S-107.

[NAVSEA 93] Naval Sea Systems Command, *Integrated Interior Communications and Control (IC)^2 Program Plan,* no date (approximate publication date: August 18, 1993).

[NCSC 87] National Computer Security Center, *Trusted Network Interpretation (TNI),* NCSC-TG-005, 1987.

[NCSC 88A] National Computer Security Center, *A Guide to Understanding Configuration Management in Trusted Systems,* NCSC-TG-006, 1988.

[NCSC 88B] National Computer Security Center, *A Guide to Understanding Design Documentation in Trusted Systems,* NCSC-TG-007, 1988.

Appendix B – References (continued)

[NCSC 88C] National Computer Security Center, *A Guide to Understanding Trusted Distribution in Trusted Systems,* NCSC-TG-008, 1988.

[NCSC 88D] National Computer Security Center, *A Guide to Understanding Configuration Management in Trusted Systems,* NCSC-TG-006, 1988.

[NCSC 89A] National Computer Security Center, *Guidelines for Formal Verification Systems,* NCSC-TG-014, 1989.

[NCSC 89B] National Computer Security Center, *A Guide to Understanding Trusted Facility Management,* NCSC-TG-015, 1989.

[NCSC 91A] National Computer Security Center, *Trusted Database Management System Interpretation of the TCSEC,* NCSC-TG-021, 1991.

[NCSC 91B] National Computer Security Center, *A Guide to Understanding Trusted Recovery in Trusted Systems,* NCSC-TG-022, 1991.

[NCSC 91C] National Computer Security Center, *A Guide to Writing the Security Features User's Guide for Trusted Systems,* NCSC-TG-026, 1991.

[NCSC 92] National Computer Security Center, *A Guide to Understanding Object Reuse in Trusted Systems,* NCSC-TG-018, 1992.

[NIST 88] National Institute of Standards and Technology, Computer Systems Laboratory, *Programmer's Hierarchical Interactive Graphics System (PHIGS),* FIPS PUB 153 (ISO/IEC 9593.1-1990), October 14, 1988.

[NIST 89A] National Institute of Standards and Technology, Computer Systems Laboratory, *Government Open Systems Interconnection Profiles Users' Guide,* NIST Special Publication 500-163, August 1989.

[NIST 89B] National Institute of Standards and Technology, Computer Systems Laboratory, *Information Resource Dictionary System (IRDS),* FIPS PUB 156, April 5, 1989.

[NIST 90A] National Institute of Standards and Technology, *Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols,* NISTIR 90-4250, February 1990.

Appendix B – References (continued)

[NIST 90B] National Institute of Standards and Technology, *Secure Data Network System (SDNS) Key Management Documents,* NISTIR 90-4262, February 1990.

[NIST 90C] National Institute of Standards and Technology, *Secure Data Network System (SDNS) Access Control Documents,* NISTIR 90-4259, February 1990.

[NIST 90D] National Institute of Standards and Technology, *The User Interface Component of the Applications Portability Profile (X-Windows),* FIPS PUB 158, May 1990.

[NIST 91A] National Institute of Standards and Technology, Computer Systems Laboratory, *Security in ISDN,* NIST Special Publication 500-189, September 1991.

[NIST 91B] National Institute of Standards and Technology, *Govemment Open Systems Interconnection Profile (GOSIP),* FIPS PUB 146-1, April 1991.

[NIST 91C] National Institute of Standards and Technology, *Graphical Kemel System (GKS),* FIPS PUB 120-1 (ISO 7942), January 8, 1991.

[NIST 92A] National Institute of Standards and Technology, *Govemment Open Systems Interconnection Profile (GOSIP) Chapter 6, Security Options,* Proposed Draft for Version 3, July 1992.

[NIST 92B] National Institute of Standards and Technology, *Standard Security Label for the Govemment Open Systems Interconnection Profile (GOSIP),* Draft FIPS PUB XXX, July 15, 1992.

[NIST 92C] National Institute of Standards and Technology, *Govemment Network Management Profile (GNMP),* FIPS PUB 179, December 14, 1992.

[NIST 92D] National Institute of Standards and Technology, *Key Management Using ANSI* X9.17, FIPS PUB 171, April 27, 1992.

[NIST 92E] National Institute of Standards and Technology, "TCP/IP or OSI? Choosing a Strategy For Open Systems," *NIST Computer Systems Laboratory Bulletin,* June 1992.

Appendix B – References (continued)

[NIST 92F] National Institute of Standards and Technology, *SDNS Security Protocol 2 for LANs (SP2L),* (uses IEEE 802.10 SDE), First Draft, OSE Implementors' Workshop Security Special Interest Group, SDN.201, December 22, 1992.

[NIST 92G] National Institute of Standards and Technology, Computer Systems Laboratory, *A Study of OSI Key Management,* NISTIR 4983, Nov 1992.

[NIST 92H] National Institute of Standards and Technology, *A Formula Description of the SDNS Security Protocol at Layer 4 (SP4),* NISTIR 4792, March 1992.

[NIST 92I] National Institute of Standards and Technology, *Federal Criteria for Information Technology Security, Volume I, Protection Profile Development,* Version 1.0, December 1992.

[NIST 92J] National Institute of Standards and Technology, *Federal Criteria for Information Technology Security, Volume II, Registry of Protection Profiles, Version 1.0,* December 1992.

[NIST 92K] National Institute of Standards and Technology, *Initial Graphics Exchange Specification (IGES),* FIPS PUB 177, November 30, 1992.

[NIST 93A] National Institute of Standards and Technology, Computer Systems Technology, *Stable Implementation Agreements for Open Systems Interconnection Protocols Version 6, Edition 1, NIST Special Publication 500-206,* December 1992 (with March 1993 updates).

[NIST 93B] National Institute of Standards and Technology, *Stable Implementation Agreements for Open Systems Interconnection Protocols Part 12 – OS Security, NIST Special Publication 500-206,* June 1993.

[NIST 93C] National Institute of Standards and Technology, *Working Implementation Agreements for Open Systems Interconnection Protocols Part 12 – OS Security,* NIST Special Publication 500-206, June 1993.

[NIST 93D] National Institute of Standards and Technology, *Workshop Policies and Procedures,* Output from the June 1993 Open Systems Environment Implementors' Workshop (OIW), no date.

Appendix B – References (continued)

[NIST 93E] National Institute of Standards and Technology, Computer Systems Technology, *Application Portability Profile (APP) The U.S. Government's Open System Environment Profile OSE/1, Version 2.0,* Special Publication 500-210, June 1993.

[NIST 93F] National Institute of Standards and Technology, *Computer Systems Publications and Products, NIST Publication List 88,* August 1993.

[NIST 93G] National Institute of Standards and Technology, *Federal Information Processing Standards Publications (FIPS PUBS) Index, NIST Publications List 58,* June 1993.

[NIST 93H] National Institute of Standards and Technology, *Secure Hash Standard,* FIPS PUB 180, May 11, 1993.

[NIST 93I] National Institute of Standards and Technology, "Digital Signature Standard," *NIST Computer Systems Laboratory Bulletin,* January 1993.

[NIST 93J] National Institute of Standards and Technology, "The NIST Graphics Testing Program," *NIST Computer Systems Laboratory Bulletin,* April 1993.

[NIST 93K] National Institute of Standards and Technology, "Connecting to the Internet: Security Considerations," *NIST Computer Systems Laboratory Bulletin,* July 1993.

[NIST 93L] National Institute of Standards and Technology, "Federal Information Processing Standards (FIPS) Activities," *A Letter from the Computer Systems Laboratory,* Number 42, May 1993.

[NIST 93M] National Institute of Standards and Technology, "Federal Information Processing Standards (FIPS) Activities," *A Letter from the Computer Systems Laboratory,* Number 43, August 1993.

[NIST 93N] National Institute of Standards and Technology, *Database Language SQL,* FIPS PUB 127-2, December 3, 1993.

[NIST 93P] National Institute of Standards and Technology, *Computer Graphics Metafile (CGM),* FIPS PUB 128-1 (ISO 8632.1-4 1992), May 11, 1993.

[NIST 93Q] National Institute of Standards and Technology, *POSIX: Portable Operating System Interface for Computer Environments,* FIPS PUB 151-2, May 12, 1993.

Appendix B – References (continued)

[NIST 93R] National Institute of Standards and Technology, *Standard Security Label for the Government Open Systems Interconnection Profile,* Proposed FIPS PUB, Draft, September 30, 1993.

[NRL 93A] Naval Research Laboratory, Information Technology Division, Center for High Assurance Computing Systems, *An Internetwork Authentication Architecture,* NRL/FR/5544--93-9561, August 5, 1993.

[NRL 93B] Naval Research Laboratory, Information Technology Division, *User Level Security in the Copernicus TADIXS*, Technical Memorandum 5520-36A, 55-2372-A3, March 26, 1993.

[OSF 91] Open Software Foundation, *Security in a Distributed Computing Environment, A White Paper,* January, 1991.

[RFC 92A] Internet Network Working Group, *The MD2 Message-Digest Algorithm,* B. Kaliski, RSA Data Security Inc., Request for Comments: 1319, April 1992.

[RFC 92B] Internet Network Working Group, *The MD4 Message-Digest Algorithm,* R. Rivest and S. Dusse, RSA Data Security Inc., Request for Comments: 1320, April 1992.

[RFC 93A] Internet Network Working Group, *Security Label Framework for the Internet,* Russ Housley, Spyrus Inc. (previously with Xerox Special Information Systems), Request for Comments: 1457, May 1993.

[RFC 93B] Internet Network Working Group, *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures,* J. Linn, Request for Comments: 1421, February 1993.

[RFC 93C] Internet Network Working Group, *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management,* S. Kent, Request for Comments: 1422, February 1993.

[RFC 93D] Internet Network Working Group, *Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers,* D. Balenson, Request for Comments: 1423, February 1993.

[RFC 93E] Internet Network Working Group, *Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services,* Request for Comments: 1424, February 1993.

Appendix B – References (continued)

[RILEY 92] John W. Riley III, *"Considerations for a Shipboard Multilevel Secure Local Area Network"*, Thesis, Naval Postgraduate School, March 1992.

[ROSE 90] M. T. Rose, *The Open Book — A Practical Perspective on OSI,* Prentice Hall, Englewood Cliffs, New Jersey, 1990.

[ROSE 92] M. T. Rose, *The Little Black Book: Mail Bonding with OSI Directory Services, Prentice Hall, Englewood Cliffs,* New Jersey, 1992.

[ROSEN 93] R. Rosenbaum, *"Wireless Networking," Handbook of Local Area Networks – 1993-94 Yearbook,* Auerbach Publications, 1993, pp. S-169 – S-175.

[ROSS 91] F. E. Ross, *"The Fiber Distributed Data Interface," Handbook of Local Area Networks,* Auerbach Publications, 1991, pp. 265 - 293.

[SAYDJ 87] O. S. Saydjari, J. M. Beckman, J. R. Leaman, "LOCKing Computers Securely," *10th Proceedings of the National Computer Security Conference,* October 1987, pp. 129-141.

[SAYDJ 89] O. S. Saydjari, J. M. Beckman, J. R. Leaman, "LOCK Trek: Navigating Uncharted Space," *Proceedings of the IEEE Symposium on Security and Privacy,* May 1989, pp. 167-175.

[SCHLAR 90] S. K. Schlar, *Inside X.25: A Manager's Guide, McGraw-Hill,* New York, New York, 1990.

[SECCOMP 91A] R. C. O'Brien, Computing Technology Corporation, *The LOCKGuard,* December 1991.

[SECCOMP 91B] S. Miller, Computing Technology Corporation, *An Overview of the LOCK System,* 1991.

[SECNAV 93] Secretary of the Navy, Assistant for Tactical Computers, *Acquisition of Computer Resources Used in Mission Critical Systems,* SECNAV Instruction 5200.32A, February 9, 1993.

[SECWARE 93] SecureWare, *Reserve Component Automation System MAXSIX Design Specification, Revision B,* 010-000-67-00, April, 1993.

[SLONE 91] J. P. Slone and A. D. Drinan, Editors, *Handbook of Local Area Networks,* Auerbach Publications, Boston, Massachusetts, 1991.

Appendix B – References (continued)

[SLONE 92] J. P. Slone and A. D. Drinan, Editors, *Handbook of Local Area Networks – 1992-93 Yearbook,* Auerbach Publications, Boston, Massachusetts, 1992.

[SLONE 93] J. P. Slone and A. D. Drinan, Editors, *Handbook of Local Area Networks – 1993-94 Yearbook,* Auerbach Publications, Boston, Massachusetts, 1993.

[SMITH 93] P. Smith, "Wireless Technology in a Wired World," *Handbook of Local Area Networks – 1993-94 Yearbook,* Auerbach Publications, 1993, pp. S-177 – S-189.

[SPAWAR 91A] Space and Naval Warfare Systems Command, Copernicus Project Office, Director, Space and Electronic Warfare, *The Copernicus Architecture, Phase I: Requirements Definition,* August 1991.

[SPAWAR 91B] Space and Naval Warfare Systems Command, Copernicus Project Office, Director, Space and Electronic Warfare, *The Copernicus Architecture, Initial Implementation Plan for Phase II,* Dec. 1991.

[SPAWAR 92A] Space and Naval Warfare Systems Command, Next Generation Computer Resources (NGCR) Security Task Group (NSTG), *Information Security Report for Mission-Critical Computer Resource System Developers,* May 21, 1992.

[SPAWAR 92B] Space and Naval Warfare Systems Command, *Embeddable INFOSEC Product Security Placement Options,* August 21, 1992.

[SPAWAR 92C] Space and Naval Warfare Systems Command, Military Standard, *Survivable Adaptable Fiber Optic Embedded Network (SAFENET),* MIL-STD-2204, October 31, 1992.

[SPAWAR 92D] Space and Naval Warfare Systems Command, Military Standard, *Survivable Adaptable Fiber Optic Embedded Network (SAFENET) Network Development Guidance,* MIL-HDBK-818-1, October 31, 1992.

[SPAWAR 92E] Space and Naval Warfare Systems Command, *Security Policy for* the Copernicus *TADIXS,* December 21, 1992.

Appendix B – References (continued)

[SPAWAR 93A] Space and Naval Warfare Systems Command, Military Standard, Survivable Adaptable Fiber Optic Embedded Network (SAFENET) Network Development Guidance, MIL-HDBK-818-1, *Revised Section 14: Network Application Programming Interface,* July 28, 1993.

[SPAWAR 93B] Space and Naval Warfare Systems Command, *Next Generation Computer Resources (NGCR), Military Standard Operating System Interface Standard (OSIF),* MIL-STD-OSIF, Draft 8, July 1, 1993.

[SPAWAR 93C] Space and Naval Warfare Systems Command, Next Generation Computer Resources, *MIL-HDBK-OSIF Handbook,* Draft, July 9, 1993.

[SPAWAR 93D] Space and Naval Warfare Systems Command, Next Generation Computer Resources (NGCR) Security Task Group (NSTG), *Battle Management System Case Study, Report on the Security Considerations of a Battle Management Command and Control System for the Next Generation Computer Resources Security Task Group's Recommendations on Standards Development,* Draft WP-2, February 26, 1993.

[SPAWAR 93E] Space and Naval Warfare Systems Command, Next Generation Computer Resources (NGCR) Security Task Group (NSTG), *NGCR Security Task Group Submarine Combat System Study,* Draft WP-3, Version .07, February 9, 1993.

[SPRAGINS 91] J. D. Spragins, J. L. Hammond, and K. Pawlikowski, *Telecommunications Protocols and Design,* Addison-Wesley Publishing Company, Reading, Massachusetts, 1991.

[SSI 92] Secure Solutions, Inc., *Placement of Network Security Services for Secure Data Exchange,* SBIR Topic N91-061, November 2, 1992.

[TANEN 89] A. S. Tanenbaum, *Computer Networks,* Second Edition, Prentice Hall, Englewood Cliffs, New Jersey, 1989.

[TARDO 91A] J. J. Tardo, "General Communications Security Services and Protocols," *Handbook of Local Area Networks,* Auerbach Publications, 1991, pp. 713 - 730.

[TARDO 91B] J. J. Tardo, "Application-Specific Communications Security Services and Protocols," *Handbook of Local Area Networks,* Auerbach Publications, 1991, pp. 731 - 753.

Appendix B – References (continued)

[TIS 93] Trusted Information Systems Inc., "Preliminary Discussion: Security Issues of a Unix PEM Implementation," *Proceedings of the Privacy and Security Research Group Workshop on Network and Distributed System Security,* February 1993.

[YAMAMO 93] M. Yamamoto, et al, "Traffic Control Scheme for Interconnection of FDDI Networks Through ATM Network," *Proceedings of the Twelfth Annual Joint Conference of the IEEE Computer and Communications Societies,* Networking: Foundation for the Future, March 1993.