



2

NAVAL POSTGRADUATE SCHOOL Monterey, California



S DTIC
ELECTE
APR 07 1992
D

THESIS

CONSIDERATIONS FOR A SHIPBOARD
MULTILEVEL SECURE LOCAL AREA NETWORK

by

John W. Riley III

March 1992

Principal Advisor:

N.F. Schneidewind

Approved for public release; distribution is unlimited

92-08892



92 4 06 153

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE				Form Approved OMB No 0704-0188	
1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED			1b RESTRICTIVE MARKINGS		
2a SECURITY CLASSIFICATION AUTHORITY			3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited		
2b DECLASSIFICATION/DOWNGRADING SCHEDULE			4 PERFORMING ORGANIZATION REPORT NUMBER(S)		
4 PERFORMING ORGANIZATION REPORT NUMBER(S)			5 MONITORING ORGANIZATION REPORT NUMBER(S)		
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School		6b OFFICE SYMBOL (if applicable) AS	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School		
6c ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000			7b ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000		
8a NAME OF FUNDING/SPONSORING ORGANIZATION		8b OFFICE SYMBOL (if applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER		
8c ADDRESS (City, State, and ZIP Code)			10 SOURCE OF FUNDING NUMBERS	PROGRAM ELEMENT NO	PROJECT NO
				TASK NO	WORK UNIT ACCESSION NO
11 TITLE (Include Security Classification) CONSIDERATIONS FOR A SHIPBOARD MULTILEVEL SECURE LOCAL AREA NETWORK					
12 PERSONAL AUTHOR(S) RILEY, John W. III					
13a TYPE OF REPORT Master's Thesis		13b TIME COVERED FROM _____ TO _____		14 DATE OF REPORT (Year, Month, Day) 1992 March	15 PAGE COUNT 79
16 SUPPLEMENTARY NOTATION The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the US Government					
17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)		
FIELD	GROUP	SUB-GROUP	shipboard local area network; shipboard LAN; LAN multi-level security; NAVMACS/GateGuard interface; VERDIX secure LAN; DMS multilevel; mailserver, MMS		
19 ABSTRACT (Continue on reverse if necessary and identify by block number) This thesis investigates the possibility of implementing a multilevel secure local area network on a medium-sized ship. In particular it focuses on medium-sized ship communications suite connectivity to a GateGuard computer system, and then on incorporating systems that have been developed under the Navy's transition plan for the Defense Message System; specifically the Multilevel Mailer Server being installed at Navy Telecommunications Centers. A review of data communications security considerations as well as DoD and Navy directives is provided for background on the accreditation requirements of multilevel secure systems. Additionally two commercially available products, the VERDIX Secure Local Area Network and Trusted Information System' XENIX trusted operating system are reviewed and then shown how they could potentially be integrated into a shipboard local area network. A potential configuration is provided with recommendation for further study of system application compatibility.					
20 DISTRIBUTION/AVAILABILITY OF ABSTRACT <input checked="" type="checkbox"/> UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS RPT <input type="checkbox"/> DTIC USERS			21 ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED		
22a NAME OF RESPONSIBLE INDIVIDUAL SCHNEIDEWIND, N.F.			22b TELEPHONE (Include Area Code) 408-646-2719		22c OFFICE SYMBOL AS/ss

DD Form 1473, JUN 86

Previous editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

S/N 0102-LF-014-6603

UNCLASSIFIED

Approved for public release; distribution is unlimited.

Considerations for a Shipboard Multilevel Secure Local Area Network

by

John W. Riley III
Lieutenant Commander, United States Navy
B.A., Tulane University, 1980

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN TELECOMMUNICATIONS SYSTEMS MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL

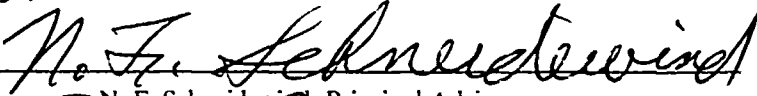
March 1992

Author:

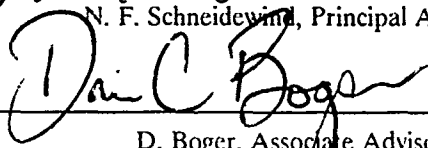


John W. Riley III

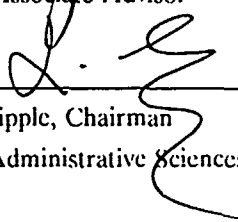
Approved by:



N. F. Schneidewind, Principal Advisor



D. Boger, Associate Advisor



D. R. Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

This thesis investigates the possibility of implementing a multilevel secure local area network on a medium-sized ship. In particular it focuses on medium-sized ship communications suite connectivity to a GateGuard computer system, and then on incorporating systems that have been developed under the Navy's transition plan for the Defense Message System; specifically the Multilevel Mail Server being installed at Navy Telecommunications Centers. A review of data communications security considerations as well as DoD and Navy directives is provided for background on the accreditation requirements of multilevel secure systems. Additionally two commercially available products, the VERDIX Secure Local Area Network and Trusted Information Systems' XENIX trusted operating system are reviewed and then shown how they could potentially be integrated into a shipboard local area network. A potential configuration is provided with recommendation for further study of system application compatibility.

Accession For	
NTIS CRA&I	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

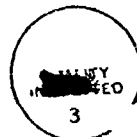


TABLE OF CONTENTS

I. INTRODUCTION	1
A. BACKGROUND	1
1. Current Systems	1
2. Prototype Systems	2
a. SWIFTNET	2
b. GWIS	3
c. Shipboard Non-tactical ADP Program	4
B. THE PROBLEMS	7
1. Message Handling	7
2. Electronic Library	8
C. PURPOSE	9
D. ORGANIZATION	9
II. SECURITY OVERVIEW	11
A. BACKGROUND	11
1. Access controls	11
a. Authentication	12
b. Partial Access Control	12
c. Full Access Control	13
d. Access Control Matrix	13
2. Encryption	15
a. Data Encryption Standard	15

b.	Public Key Encryption	16
3.	Multilevel Security	16
B.	LOCAL AREA NETWORK MULTILEVEL SECURITY	17
1.	Typical Network Configurations	18
a.	Case 1: Untrusted Computer Systems on an Untrusted Network	18
b.	Case 2: Trusted Computer Systems on an Untrusted Network	18
c.	Case 3: Untrusted Computer Systems on a Trusted Network	18
d.	Case 4: Trusted Computer Systems on a trusted Network	19
2.	Typical Network Security Approaches	19
a.	Trusted Interface Units	20
b.	Network Encryption	20
C.	DEPARTMENT OF DEFENSE COMPUTER SECURITY REQUIREMENTS	21
1.	Applicable Navy Instructions	22
a.	Safeguarding Personal Information in Automatic Data Processing Systems	22
b.	Automatic Data Processing Security Program	23
c.	Navy Implementation of National Policy on the Control of Compromising Emanations (TEMPEST)	23
2.	National Computer Security Center's Standards	24
III.	NAVAL TELECOMMUNICATIONS	25
A.	BACKGROUND	25
1.	Ashore Systems	25
2.	Afloat Systems	26
B.	SYNCROTECH SOFTWARE CORPORATION INVESTIGATION	28

1.	Syncrotech Corporation Assumptions	28
2.	Syncrotech Corporation Proposed Solutions	29
3.	Syncrotech Corporation Conclusions	31
C.	SHORE COMMAND INTERFACE	31
D.	NAVMACS II	31
E.	ASSESSMENT	33
IV. DEFENSE MESSAGE SYSTEM INITIATIVES		34
A.	BACKGROUND	34
B.	DEPARTMENT OF THE NAVY TRANSITION PLAN	35
1.	Navy Telecommunications Centers	36
2.	Security Services Provided	38
C.	MULTILEVEL MAIL SERVER	38
1.	MMS General Operating Overview	39
a.	The MMS Processor	39
b.	MMS Operating System	40
2.	Selected MMS Detailed Operating Characteristics	40
a.	Access Control and Authentication	42
b.	Support Software Environment	42
D.	MESSAGE DISSEMINATION SUBSYSTEM	43
1.	MDS Objectives	43
2.	Functional Description	44
a.	MDSFS Message Input and Queuing	45
b.	MDSUIP Message Selection and Delivery	45
V. TRUSTED XENIX AND VERDIX SECURE LOCAL AREA NETWORK		46

A.	TRUSTED XENIX	46
1.	Environmental Strengths	47
2.	Communications Support	47
B.	VERDIX SECURE LOCAL AREA NETWORK	48
1.	Product Overview	49
a.	The Verdix Network Security Center	49
b.	The Verdix Network Security Device	50
2.	Communication Protocols	51
C.	SUMMARY	52
VI. A MULTILEVEL SECURE SHIPBOARD LAN PROPOSAL		53
A.	SHIPBOARD LOCAL AREA NETWORK OVERVIEW	53
1.	Specific Required Attributes	54
2.	Functional System Description	54
a.	Communications Suite and Interfaces	54
b.	GateGuard, MMS, and LAN Interfaces	55
3.	Nodes	56
4.	Assumptions	57
5.	Application Scenarios	58
a.	Scenario One : Secret Message	58
b.	Scenario Two: Command Mandated Special Category Message	58
c.	Scenario Three: All Navy Message	59
d.	Scenario Four: Personnel Evaluations	60
B.	COST INFORMATION	61
VII. CONCLUSIONS AND RECOMMENDATIONS		63

A. CONCLUSIONS	63
B. RECOMMENDATIONS	64
APPENDIX A	65
LIST OF REFERENCES	68
INITIAL DISTRIBUTION LIST	70

I. INTRODUCTION

The information age is here. Organizations with the capability to rapidly collect, process, and disseminate information are the most successful in today's environment. This new era has not only affected the commercial business community but also the military. It has been observed that coalition military victory over Iraq was due, in a large part, to the allies' ability to disrupt the Iraqi command and control structure.

A. BACKGROUND

The United States Navy is dependent upon the efficient flow of information within its ships. Tactical information flow is vital to combat readiness and mission success; yet non-tactical information flow should be considered a primary contributor to mission readiness. The overall efficient flow of administrative information is to enhance combat readiness by improving the flow of non-tactical communications vertically, horizontally, and diagonally through out the ship. To achieve this goal the U.S. Navy requires a shipboard management information system based on a non-tactical personal computer (PC) local area network (LAN). Administrative workload for key managers should be lessened and the volume of paper documentation reduced. The latter feature will result in a dollar cost savings (reduced consumable supplies, less demand on copiers), less weight and storage space consumed, and reduction in non-productive man-hour expenditures necessary to support a paper-based information system. [Ref. 1]

1. Current Systems

Today the shipboard non-tactical information flow resides in several independent Automated Information Systems (AIS). These systems are normally centralized and parochial, relying on government-owned and developed software. They are considered support systems and are dedicated to functions such as logistics, personnel, finance, and maintenance. Large ships have been characterized

by a number of independent, but related systems. These have typically not been networks, but centralized data processing systems with small hosts, usually minicomputers, supporting any number of dumb terminals. The rapid proliferation of personal computers, in combination with the above systems, has made it common to have two or three different terminals or computing devices in the same work space, each attached to its own support system. [Ref. 2]

2. Prototype Systems

The proliferation of different and separate systems and the rapid advancement of data communications technology has forced the Navy to reevaluate the way they design and procure non-tactical systems. The initial goal for the Navy is to link as many systems as possible onto a common fiber backbone. These include a Shipboard Wide Integrated Fault Tolerant Network (SWIFTNET) on USS YELLOWSTONE (AD 41), the GEORGE WASHINGTON Information System (GWIS) on USS GEORGE WASHINGTON (CVN 73), and the early development work on the SNAP III program. [Ref. 2]

a. SWIFTNET

Shipboard Wide Integrated Fault Tolerant Network (SWIFTNET) is installed in the USS YELLOWSTONE (AD 41). There are currently a number of related, but separate, AISs on YELLOWSTONE. They include [Ref. 2]:

- MRMS - Maintenance Resource Management System - MRMS supports maintenance work at shore repair activities. It provides for automated work requests as well as automated job status.
- PCRS - Personal Computer Remote System - PCRS is an automated message handling system that allows messages to enter or leave the system via a floppy disk. It is not yet a distributed net. It is the first step in eliminating paper in the Message Center.
- SNAP - Shipboard Non-tactical ADP Program - SNAP is an AIS that provides logistic support services from a centralized host.

The goal of SWIFTNET is to provide a common link for all of these support systems, as well as an office automation system. The prototype system consists of a fiber optic backbone of 8-strand fiber cable employing an FDDI architecture. Design criteria for SWIFTNET included

expendability, maintainability, survivability, performance, throughput, industry standards compliance, and upgradability. [Ref. 2]

b. GWIS

The purpose of GWIS is to increase combat readiness by improving non-tactical communications. The long term objective is to electronically link all work centers and shipboard offices (approximately 250) via a PC LAN. The LAN will contain the bridges into other systems, such as SNAP, allowing a truly integrated non-tactical information flow throughout the ship. Like SWIFNET, GWIS will provide a common backbone, consisting of 8-strand fiber, that will link several independent systems [Ref. 1] In addition to SNAP, GWIS will attempt to link the following systems [Ref. 1]:

- NALCOMIS - Naval Aviation Command Management Information System - NALCOMIS supports aviation logistics afloat and ashore. Modules include material management, repair management, and automated parts ordering.
- NAVMACS - Naval Modular Automated Communication System - NAVMACS is a family of automated communications systems sized to the need of individual ship types. It uses a modular concept and includes hardware and software. It is a message processing system that can route or store incoming or outgoing messages.
- SAMS - Shipboard Automated Medical System - SAMS is a stand-alone PC that supports the shipboard medical department.

Installation of GWIS is being conducted in a three phase effort. Phase I will provide hardware and links to the executive level, which is all Department Heads and above. Phase II extends communications to the Division and Work Center level. This will result in the capability to electronically process documentation from origin to destination without interruption, and this will enhance both vertical and horizontal levels of communication. Phase III will eventually incorporate the other existing systems described above. [Ref. 1] The GWIS will be built around several functional modules listed in Figure 1.

GWIS is a dynamic attempt to provide a necessary service to the ship's crew. It takes advantage of commercially available technology. GWIS represents a valuable opportunity to prototype a modern information system for warships, and hence make a giant leap toward the Chief of Naval

GWIS Desired Functional Modules

Correspondence. Provides E-Mail, outgoing correspondence review, distribution of incoming correspondence and action tracing.

Readiness Reporting. Provides a database for readiness reporting, using/interfacing with existing software to generate Navy formatted readiness reports. Provides daily department material status report to the Commanding Officer and Executive Officer.

Planning & Scheduling. Assists in developing daily, weekly, monthly and long range plans. Provides format and logic for producing the daily air plan and weapons load plan.

Project Management. Provides software to produce action plans and manage milestones for complex or large projects.

Preventive Maintenance Management. Processes and stores preventive maintenance records and generates reports.

Inspection Management. Stores results of inspections and tracks corrective action measures. Provides tickler system for recurring inspections. Additionally, stores results of zone inspection results and provides reports to the chain of command on corrective action.

Communications. Ultimate goal is to interface with NAVMACS to provide electronic review and release of outgoing messages and electronic distribution of incoming messages at locations not served by NAVMACS.

Personnel Management. Provides mid-level managers with the capability to access master personnel database.

Electronic Library. Electronically store all instructions, publications, and other reference material for quick retrieval.

Figure 1 Desired GWIS functional modules

Operation's goal of a paperless ship." [Ref. 1]

c. Shipboard Non-tactical ADP Program

The Shipboard Non-tactical ADP program (SNAP) has provided support services to Navy ships since 1978. SNAP I was designed for larger ships, such as tenders and aircraft carriers, while SNAP II is used by smaller combatants. SNAP is a centralized system, consisting of a host computer, either the Honeywell DPS-6 or the Harris H-300, linked to many dumb terminals throughout the ship. SNAP integrates a number of functional modules such as parts support, maintenance record preparation, word processing, data base management, and financial records. Each of these modules consists of

specially designed software, similar to commercial versions, but written and maintained for exclusive use by the Navy. [Ref. 2]

The author's personal experience is the SNAP II system can be characterized as inflexible and unresponsive to user needs. In 1986, a post implementation review of user concerns concerning SNAP II was conducted by Wheeler, Mallon, and Shotwell [Ref. 3] in which they concluded the SNAP hardware and implementation support services were adequate for the time. However, lack of training for end users was considered a significant problem. The authors recommended more efficient use of the system could be corrected by:

- Better communication with the end user
- Revision of training policy
- Revision of documentation to a more user friendly format
- Identification of a central control point for program policy, guidance, and standards.

Although the author agrees with the intent of the conclusions, several observations are offered. The six ships on which they conducted their survey had relatively recent SNAP II installations. The reported interviews indicated all Supply Officers were extremely satisfied with the system. In this author's opinion this was to be expected as the Supply function was the one function that reaped the most benefit from the system. Tracking supply requisitions and inventory control transitioned from a paper-based to a computer based system. The SNAP II system did not greatly help any other shipboard departments perform their respective function in near the magnitude as Supply (although it does provide a current ship's maintenance project). The rapid procurement and proliferation of personal computers and commercial software during this same time frame gave other shipboard departments flexibility in their computer processing needs. Most notably word processing. ([Ref. 3] reported that one of the biggest complaints concerning SNAP II was the system response time was significantly reduced while word processing functions were being performed.)

SNAP III is expected to change this. In fact, in 1986 Schneidewind [Ref. 4] recommended that SNAP III be based on commercially available hardware and software to the

maximum extent possible. Schneidewind recognized that data processing functions required for SNAP III are not significantly different than that required by commercial industry. He argued that the Navy's data processing functions can not be truly unique as there are a finite number of functions that can be performed by any application. Major recommendations the report made include:

- Transition from minicomputer to microcomputer system
- Transition to proven commercial office system
- Use local area network technology
- Acquire mass storage capability
- Acquire improved graphics capability
- Consider automating ship -- shore communications
- Start to develop a procurement policy to support acquisition of the above technology.

These recommendations were basically adopted by the Naval Sea Systems Command and it is expected SNAP III will lead the Navy into a truly distributed, PC-based, local area network and will lead the Navy to it's ultimate goal for a paperless ship.

It is expected SNAP III will utilize SAFENET, the Survivable, Adaptable Fiber optic Embedded local area NETWORK. SAFENET is a network protocol that utilizes a dual redundant token ring architecture that is ideal for the type of fault tolerant requirements the Navy demands. SAFENET I was compliant with IEEE 802.5. SAFENET II, which will be used for SNAP III, will be ANSI FDDI compatible. [Ref. 2]

SNAP III is still in the development process. A prototype system, called Micro-SNAP, will be placed aboard several vessels in 1991. Additionally, several ships have had prototype paperless ship systems on board for the past three years. Lessons learned from these efforts should make the final development and transition to SNAP III efficient and cost effective. [Ref. 2]

B. THE PROBLEMS

The three projects discussed above represent an important problem within the Navy. Each of the projects are serious, well-thought-out solutions to real problems, and each is valid in its own right. However, they represent three similar, but distinct ways of solving the same problem. In fact, these are only three well-documented solutions. They do not account for numerous other projects that have been initiated by individual commands in installing shipboard LANs. What is needed in the long term is a coordinated response, a single solution that will provide necessary services at the lowest possible costs. Each project described is an excellent first step. The next step must combine the best efforts of these systems into a single integrated solution.

Applications are the objective of developing fiber optic LANs in the first place. The functional modules described for the GWIS are an excellent cross section of what the Navy should expect from any network system. However, two particular applications are critical; They are the cornerstone efforts of any successful shipboard system. These applications are message handling and an electronic publications library. Unfortunately, both require security considerations which have not been satisfactorily addressed or pursued for a solution.

1. Message Handling

Any shipboard LAN must be capable of linking with the ship's message center, and the LAN must be capable of routing incoming and outgoing messages. An Automated Message Handling System (AMHS) provides enough benefits to easily pay for any development and installation costs for the LAN. An AMHS must be able to route incoming messages to the appropriate personnel and offices, and it must accept outgoing messages generated at the lowest level desired. In order to fully exploit the advantages of a LAN and AMHS combination, the system must be capable of handling classified message traffic. With the Navy's use of classifications, security clearances, and access based on need to know, the ground work is laid for the requirement of a multi-level secure system. Although all the previous projects have outlined the desire to integrate the message center with the appropriate LAN,

this has not been fully obtained due to the lack of a multi-level secure system. To date, the best solution has been to establish a system high level LAN, meaning that all nodes, personnel, and data on the LAN must all be cleared to the same level. Captain Nutwell, Commanding Officer of GEORGE WASHINGTON, recently stated:

The hardware we're going to have in our non-tactical network is not multi-level security capable because the computers aren't. If we wanted to process Secret, every machine on the network would have to be Secret. I think we'll continue to process Secret the old way. [Ref. 5]

While in port, ships rely heavily on the station infrastructure for over the counter message traffic, supply support, and maintenance support. Naval stations are in the process of developing their own local area networks. The capability for a shipboard LAN to connect with these shore-based LANs will be greatly advantageous, as ship repair, supply, and financial data will easily communicated. The Defense Message System (DMS) has developed a Multi-level Mail Server (MMS) system that will electronically transfer a ships message traffic from the local Naval Telecommunications Center to the ship moored at a local pier. This system is designed to transfer Unclassified to Secret message traffic to the ship. Again, an AMHS and shipboard LAN capable of distributing all the received traffic would be greatly desired.

2. Electronic Library

This is the second critical step to the Navy's paperless ship goal. Studies have shown that electronic storage devices such as CD-ROM can reduce the weight of paper and paper storage from 14 to 33%. On an AEGIS-class guided missile cruiser, this equates to a savings of about 23,600 pounds. [Ref. 2]

The Surface Warfare Development Group (SWDG) is a small Navy organization with immense responsibility. SWDG develops and evaluates new tactics and improves current tactics in the surface Navy's three dimensions of warfare: Anti-Air, Anti-Surface, and Anti-Submarine, including electronic warfare as well as command and control. Experimental tactics are issued as TACMEMOS, and later updated as approved tactics in TACNOTES. Ultimately these tactics are incorporated into

Naval Warfare Publications or a ship class Combat Systems Doctrine. Additionally, tactical lessons learned by the fleet are collected and compiled by SWDG in the development process. The entire lessons learned and some NWP's will be coming out on CD-ROMs and will be available to the fleet in the near future. [Ref. 6]

It has been the author's experience that these tactical information packages are often Secret. The capability to share these documents on a multi-level secure LAN will greatly improve the dissemination of tactics to ship's personnel, increasing combat readiness and reducing the administrative burden of maintaining a large paper based Secret account.

C. PURPOSE

The purpose of this thesis is to address the feasibility of installing a multi-level secure LAN on a U.S. Navy ship. The author will focus on a medium-sized ship, as he has reached the conclusion that only large afloat commands such as aircraft carriers and tenders will be subjected to extensive research and development of shipboard LANs. Also the command entities of the NTS will consider their job complete once messages are delivered to their defined end user - the ship. The author considers the end user to be the various officers and sailors on the vessels that must still drudge through a Secret paper information system. If a multi-level secure LAN system is impractical, then one must consider two separate shipboard LANs, with one a system level high of at least Secret. As discussed above, there are several desired uses of a shipboard LAN that would require multi-level security. The author will attempt to review the various alternatives and provide a recommendation on the best solution.

D. ORGANIZATION

This thesis is organized into seven chapters, each presenting background information to comprehend the task of providing multi-level security within a LAN. Chapter II provides a background on computer and data communications security to provide an understanding of terminology and different approaches to providing LAN security.

Chapter III reviews the Naval Telecommunications System and discusses the required integration of a LAN with a shipboard communications suite. A review of current Navy pursuit for a shipboard LAN and communication suite is provided with an assessment of the Navy's current policy.

Chapter IV will provide background information on the Navy's implementation of DMS and its capabilities. Procedures and hardware already in use at shore facilities will be reviewed to determine a shipboard application.

Chapter V will presents certain vendor products for multi-level secure LANs. Specifically, VERDIX's Secure Local Area Network, and Trusted Information System's XENIX trusted operating system will be reviewed. The intent is not to provide a product endorsement but to review a method of providing multi-level security.

Chapter VI will present a proposal for a multi-level secure shipboard LAN utilizing information presented in previous chapters.

The final chapter, Chapter VII, will provide a summary and conclusions. Again, the author does not intend to provide any product endorsement. The conclusions will offer one option the Navy has in pursuing the acquisition of a shipboard multi-level secure LAN.

II. SECURITY OVERVIEW

A. BACKGROUND

Network security can be defined as the protection of network resources against unauthorized disclosure, including accidental disclosure, modifications, restrictions, or destruction. Security has long been an object of concern and subject to extensive research and development for both data processing systems and communications facilities. With computer networks these concerns are combined, and for local networks the problem is most acute. [Ref. 7]

A full-capacity local network offers direct terminal access to the network and data files and applications distributed among a variety of computing devices and/or dumb terminals. The local network may also provide access to and from long haul communications. Providing security in this type of environment is most complex. [Ref. 7: p. 336]

Network security is a broad subject, and encompasses physical and administrative controls as well as automated ones. To ensure an understanding of terminology and concepts presented in follow-on chapters, the first portion of this chapter will provide a functional description of three areas of specific concern for local networks:

- Access control
- Encryption
- Multilevel security

1. Access controls

The purpose of access control is to ensure that only authorized users have access to the system and its individual resources and that access to and modification of particular portions of data is limited to authorized individuals and programs. Measures taken to control access in a data processing

system generally fall into two categories: first, those associated with users or groups of users and, second, those associated with data. [Ref. 7: p. 337]

a. Authentication

The control of user access is referred to as authentication. Authentication consists of validating a user's identification (ID) and password, either at the network level or within an individual host. The ID validation process ensures a user is enrolled in the validating system, while the password validation ensures that the person signing on is not an imposter. This id/password system has developed into a notoriously unreliable method of access control. [Ref. 7: p. 337]

In many local networks, two levels of authentication will probably be used. Individual nodes may be provided with a logon facility to protect host/node specific resources and applications. Additionally, the network as a whole may have protection to restrict network access to authorized users. This two-level facility is desirable for a local network that connects disparate hosts and simply provides a convenient means of terminal host access. [Ref. 7: p. 338]

The difficulty of authentication is compounded over a multi-access medium LAN. The logon dialogue must take place over the communications medium and eavesdropping is a potential threat. The eavesdropping threat can be classified as passive and active wiretapping. Passive wiretapping means observing the data stream but not modifying it. The passive wiretapper can read user data and also analyze LAN control data and traffic statistics. Active wiretapping means modifying the packet stream for various effects. [Ref. 8]

Additional access control issues can be considered to fall in two classes: partial, or distributed, access control and full, or centralized, access control.

b. Partial Access Control

Partial access control treats the network as a transparent communication link and requires that the LAN deliver data to a node only if the data is addressed to that node. This requires the LAN to perform five functions correctly [Ref. 8]:

- A source Network Interface Unit (NIU), a NIU that receives data for transport from its attached node, knows with certainty the destination address of the data and correctly places the address in the packet.
- The LAN keeps packets separated, not mixing and delivering as one packet data and/or an address from two different packets.
- The LAN protects the address against change while the packet is in transit.
- Every NIU can positively identify its attached node.
- No NIU delivers a packet received from the LAN transport medium to its attached node unless the packet is so addressed.

c. Full Access Control

Full access control means that in addition to partial access control the LAN transports data from one node to another only if they are authorized to communicate [Ref. 8]. In this centralized approach the network provides the logon service, which can be thought of as being associated with the Network Control Center (NCC). In the case of a LAN, this may be accomplished by setting up a connection between each inactive Network Interface Unit and the NCC. When the user activates a node and desires to access the network, the connection is automatically to the NCC. After a successful logon, the NCC then establishes a connection between the requesting node and the requested destination address. When this connection is terminated, the original user and NCC connection is reestablished. A similar technique would be used in a digital switch. A data port off-hook condition would result in a connection to a logon server; after authentication, the request connection would be made. [Ref. 7: p. 338]

d. Access Control Matrix

After successful authentication, the user is granted access to a host and/or processes. This is not sufficient for a system that includes sensitive data in its database. The authentication procedure identifies a specific user with a profile that specifies permissible operations and file accesses. The network operating system can enforce rules based on the user profile. However, the data base management system must control access to specific portion of records. For example, it may be

permissible for anyone in administration to obtain a list of company personnel, but only certain individuals may have access to salary information. The issue involves more than one level of detail. The network operating system may grant a user permission to access a file or use an application in which there are no further security checks, whereas the data base management system must make a decision on each individual access attempt. That decision depends on the user's identity and on the specific parts of the record being accessed. [Ref. 7: pp. 337 to 339]

A general model of access control as exercised by a data base management system is that of an access matrix. One axis on the table consists of identified subjects that may attempt data access. Typically, this list will consist of individual users or user groups, although access could be controlled for terminals, hosts, or processes instead of or in addition to users. The other axis lists the objects that may be accessed. In the greatest level of detail, objects may be individual data fields; however, larger groupings, such as records, record types, or even an entire data base may also be objects in the matrix. Each entry in the matrix indicates the access rights of a particular subject to a specific object. [Ref. 7: pp. 337 to 339]

In practice, an access control matrix is implemented by decomposition in one of two ways. The matrix may be decomposed by columns, yielding access control lists. For each object, an access control lists specified users and their permitted access opportunities. Thus a user's name can be checked against the access control list for that resource to see if and what type of permission has been granted. A user must have a valid network account and the necessary permission to access the object. Decomposition by rows yields capability tickets. A capability ticket specifies authorized objects and operations for a user. This is a type of share level security, which works by assigning a unique password, capability ticket, to each shared resource or database. Any user who knows the password may share that resource. This is appropriate for environments that do not require tight security measures. [Ref. 7: pp. 337 to 344]

Network concerns for access control are similar to those of authentication. Encryption may be required to ensure secure communications on a LAN. Typically, access control is decentralized,

that is, controlled by host-based data base management systems. However, if a network data base server exists on a LAN, access control becomes a network function. [Ref. 7: p. 340]

2. Encryption

In the previous section eavesdropping was discussed and broadly categorized into two areas, active and passive wiretapping. Additionally eavesdropping could be accomplished by programming an NIU to accept packets other than those addressed to it. An effective countermeasure is to encrypt the data in each packet.

Encryption conceals the meaning of data by changing the intelligible plaintext into intelligible cipher text. An encryption system consists of two parts; the algorithm which is the set of rules for transforming information, and the key which personalizes the algorithm by making the transformation of specific data unique. Different keys produce completely different ciphertexts, therefore communicating parties must share the same key. The key is relatively small, in number of bits, and can be easily transported from one node to another. [Ref. 9]

Encryption algorithms may be implemented in software and hardware/firmware. Software advantages are mostly realized when protecting stored data files and data in a host computer. Hardware advantages include: greater processing speeds, independence from communication protocols, ability to be implemented on dumb devices (terminals, telex, facsimile machines), and greater protection of the key because it is physically locked in the encryption box. Tampering with the box can cause erasure of the keys and related information. [Ref. 9: p. 496]

a. Data Encryption Standard

The Data Encryption Standard (DES), developed by the National Institute of Standards and Technology (formerly the National Bureau of Standards), is based on a conventional encryption scheme. Original data in plaintext is transformed to a cipher coded bit form by means of an algorithm. Upon reception, the ciphertext is transformed back to its original form if the algorithm and key are known at the destination address. [Ref. 9: p. 499]

DES is a member of a class of algorithms known as symmetric. This means that the key used to decrypt a particular bit stream must be the same as that used to encrypt it. Since the DES algorithm is publicly known, the disclosure of a key may compromise the entire message. [Ref. 9: p. 500]

Achieving key distribution can be accomplished in several ways. For two nodes A and B:

- A key could be selected by A or B and physically delivered, by courier, to the other party.
- A third party could select the key and physically deliver it to A and B.
- If A and B have previously and recently used a key, one party could transmit the new key to the other, encrypted using the old key.
- If A and B each have an encrypted connection to a third party C, C could deliver a key or the encrypted links to A and B.

The last course is attractive in a LAN context and could be handled by an NCC; however, the keys used to communicate with C would have to be distributed by some means. [Ref. 7: pp. 340 to 341]

b. Public Key Encryption

Public key encryption inherently differs from private key systems such as DES. Public keys are based on a one way function, data is transformed to ciphertext by use of a publicly known encryption key for the destination address. Once the data is encrypted it cannot be taken apart unless the corresponding private key of the destination node is known. One way functions, which are relatively easy to calculate in one direction, are computationally impossible to reverse without the private key. In other words, the encryption/decryption can be accomplished by a pair of keys which create transformations that are the inverse of each other. [Ref. 9: pp. 500 to 503]

3. Multilevel Security

Multilevel data processing can be described as having data of several different levels of classification being processed on a single computer or network at the same time, while users of different clearances are on the system. For this approach to work, the system must be trusted to maintain the separation of different classified data and prevent users from accessing data for which they lack proper

clearance [Ref. 10]. This requirement, based the Bell and LaPadula model, can be simply stated in two parts. A multiple level secure system must enforce [Ref. 7: pp. 342 to 343]:

- No read up: A user can only read an object of less or equal security level.
- No write down: A user can only write into an object of greater or equal security level.

To verify that a computer system meets a promulgated policy, computer security models have been developed. These models, in a mathematical manner, describe how to mediate the flow of information in an ADP environment to and from users and data repositories. The abstract mechanism that controls this flow is known as a reference monitor. [Ref. 10] The reference monitor enforces the security rules (no read up, no write down) and has the following properties [Ref. 7: pp. 342 to 343]:

- Complete mediation: The security rules are enforced on every access, not just, for example, when the file is open.
- Isolation: The reference monitor and data base are protected from unauthorized modification.
- Verifiability: The reference monitor's correctness must be provable; thus it must be small, simple, and easy to understand.

In order to accomplish the above, computer operating systems were redesigned in the form of a hierarchy of modules. The innermost level of the hierarchy has the most privilege regarding executing code. As one moves out from the inner layer less privileges are granted and fewer functions are able to be executed. The innermost level contains those portions of the operating system that are most critical to security needs, specifically access control, memory, and input/output management. Taken together, these portions of the operating system are known as the kernel of the OS. In addition to the kernel, the system also includes trusted processes; these can run outside the kernel and are trusted not to violate certain security rules of the model. Taken together, the kernel and trusted processes are referred to as the Trusted Computing Base (TCB). [Ref. 10]

B. LOCAL AREA NETWORK MULTILEVEL SECURITY

Several approaches to multilevel network security have been proposed over the years. Approaches have involved many schemes and configurations. Accordingly, a review is appropriate.

1. Typical Network Configurations

Consideration should be given to various network configurations involving both trusted and untrusted systems with examination of some typical connection scenarios. This discussion will be helpful in understanding specific network security requirements and the evaluation of network security models.

The four possible network configurations are as follows [Ref. 11]:

- Untrusted computer systems on an untrusted network
- Trusted computer systems on an untrusted network
- Untrusted computer systems on a trusted network
- Trusted systems on a trusted network

a. Case 1: Untrusted Computer Systems on an Untrusted Network

In this case the untrusted systems and untrusted network operate in a Dedicated or in a System High mode. There is no access control policy for the computer systems or the network, and no labels are associated with information processed or transferred in the network. A network or computer TCB is not required. Users are cleared to the maximum level, but information can range from some low level to the maximum established network level. It is necessary to ensure information classified above the maximum level not combine with any parts of the entire system. [Ref. 11]

b. Case 2: Trusted Computer Systems on an Untrusted Network

The computer systems are trusted to operate in a multi-level mode including the network security level. Access control is required within the computer system. The computers TCB is required to ensure that the information is properly labeled with the network high security level and that information of a higher level than the network is not allowed to be placed in the network. The computer TCB must also know the level of other computer systems within the network. [Ref. 11]

c. Case 3: Untrusted Computer Systems on a Trusted Network

The computer systems connected to the network operate in the System High mode. Because the network can carry information of different classifications, it is necessary to attach labels

either to information units or to virtual circuits when sessions are established. Untrusted computer system levels must be within the range of levels for which the network is trusted and a network mandatory security policy must be enforced. [Ref. 11]

d. Case 4: Trusted Computer Systems on a trusted Network

Both the computer systems and the network operate in a multi-level mode. Both the computer systems and the network must have TCBs. Not all users are cleared for all information on the network; therefore, the range of security levels of the computer systems must overlap with the corresponding levels of the network. Both systems must ensure that they only pass information within the corresponding security level range. This configuration also requires no illicit information flow and that all information is correctly labeled. [Ref. 11]

2. Typical Network Security Approaches

Approaches closely parallel configurations, but there are slight differences. Approaches that have surfaced over the years include [Ref. 7 p. 344]:

1. Physical separation: The security problem disappears if the various LANs are in separated areas and protected at their designated security levels. This approach negates most of the benefit of the LAN. Connectivity is limited. Security requirements permit data to be passed upward (from a lower to higher classification area), but this approach does not facilitate such data transfer.
2. Bandwidth separation: With a broadband cable, each classification level could be assigned a separate channel. Cross channel traffic could be supported by a multilevel secure host. A trusted multilevel host is required.
3. Encryption: Each NIU would require encryption capability, requiring a trusted facility for distributing keys to end points requesting a connection
4. Trusted hosts: Liberal use of trusted host machines (Guards) may be capable of satisfying security requirements. If the trusted host were a minicomputer, mainframes could be connected by a trusted front end. Terminal would have to interface to the network via a trusted host.
5. Trusted NIU: This is an NIU that provides a reference monitor capability. This NIU may also be referred to as a Trusted Interface Unit (TIU). It is a remarkably simple device.

Each approach is unique, however some are more advantageous than others. Of the five approaches listed above, encryption and the TIUs are considered, by the author, to be most appropriate to a shipboard environment and subsequent attention will be focused in these areas. Additionally, the

first alternative of physical separation, may be a viable alternative for shipboard application requirements.

a. Trusted Interface Units

The Trusted Interface Unit (TIU) is a piece of firmware that performs all the functions of a an ordinary NIU; however, it is designed to operate at an assigned security level. Two other functions are required:

- The TIU will label each frame that it transmits with its security level.
- The TIU will accept only frames that are labeled with its own or lesser security level.

TIU's were originally conceived to be designed and produced in three versions, in increasing order of complexity. A single level TIU is set to monitor a single security level. The TIU must be physically protected to the network-high level, and is designed to reliably isolate the traffic at one particular security level from traffic at all other levels. A variable level TIU is similar to a single level TIU, except the operator can change the level of the TIU by adjusting electronically linked terminal switches or keyboard keys. The range of adjustments correspond to the approved security levels for that particular TIU and terminal. A multilevel TIU requires fully trusted software; however, a network can operate in a multilevel mode using only single and/or variable level TIUs. See Figure 2. [Ref. 12]

b. Network Encryption

With either of the encryption approaches previously described, network encryption can be end-to-end or link orientated. End-to-end encryption is handled by the processes at each end of the session. In this capacity encryption becomes a presentation layer function. This approach allows certain flexibility within the LAN, allowing encryption devices to be installed on selected nodes. The other approach is to encrypt at the link level. Data plus all headers, except the layer 2 header are encrypted. This encryption capability can be incorporated into a NIU. [Ref 7: p. 342]

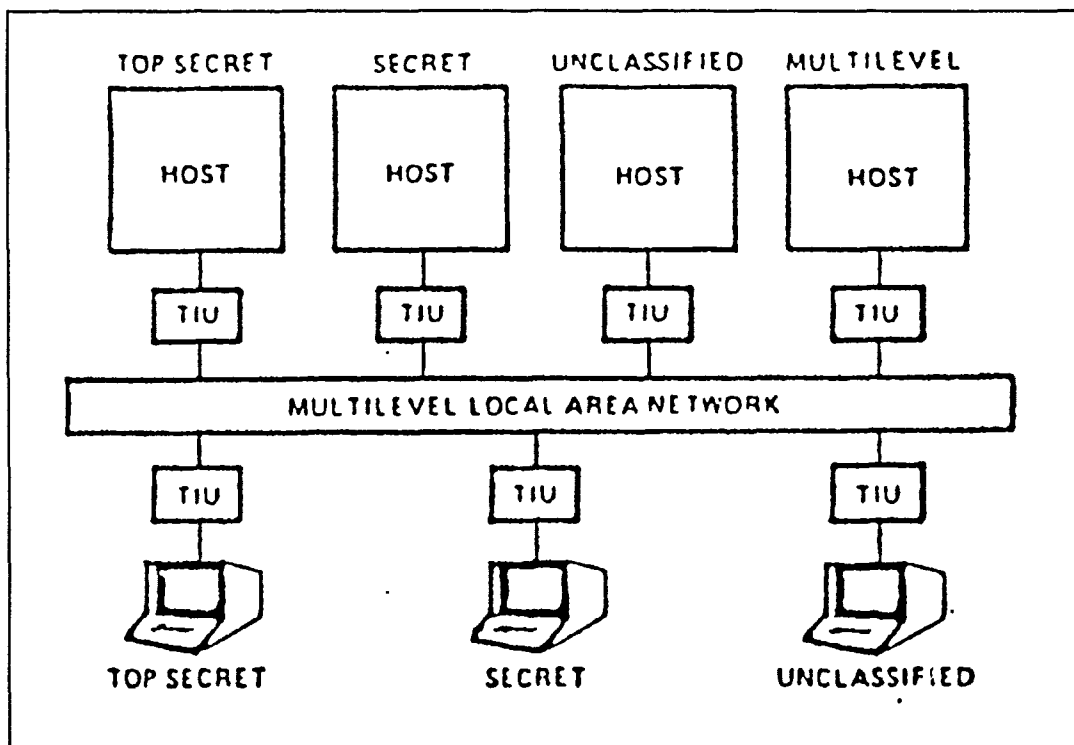


Figure 2 Example of local area network utilizing TIUs

C. DEPARTMENT OF DEFENSE COMPUTER SECURITY REQUIREMENTS

In December of 1985, the U.S. Department of Defense published the Trusted Computer System Evaluation Criteria (TCSEC), commonly known as the Orange Book. The TCSEC is used to evaluate the effectiveness of security controls built into automatic data processing system products [Ref. 11]. "The basic philosophy of the protection described in the TCSEC requires that the access of subjects (i.e., human users or processes acting on their behalf) to objects (i.e., containers of information) be mediated in accordance with an explicit and well defined security policy." [Ref. 11] The Trusted Network Interpretation (TNI), commonly referred to as the Red Book, provides an interpretation of the TCSEC for networks. The Orange and Red Books establish ratings that span four hierarchical divisions: D, C, B, and A, in ascending order of increasing provisions of security. Each division includes one or more numerical ratings, numbered from 1 to 3, which provide a finer-granularity rating. Stronger ratings correlate with higher numbers. Thus evaluated systems are assigned a digraph, such as C2 or A1, that

places the system in a class in a division. Currently, the following classes exist, in ascending order: C1, C2, B1, B2, B3, and A1. [Ref. 13] Summary criteria for the various classes, reproduced from the Orange Book, can be found in Appendix A.

1. Applicable Navy Instructions

When considering shipboard non-tactical local area networks, there are two distinct issues that prevail [Ref. 14]:

- LANs which handle personal information must provide in accordance with the Privacy Act of 1974 (5 U.S.C. 552a) and the Computer Security Act of 1987 (Public Law 100-235). Any shipboard LAN that will incorporate office automation will fall into this category.
- LANs which handle classified material must provide security protection in accordance with Executive Order 12356 (National Security Information). Any shipboard LAN which integrates the ship's message center to distribute CONFIDENTIAL, SECRET, or TOP SECRET message traffic with a office automation system will fall into this category.

The purpose of this thesis is to focus on the latter of the two issues; however, a brief discussion of the personal information issue is considered appropriate because methods of risk assessment may overlap or provide mutual support.

a. Safeguarding Personal Information in Automatic Data Processing Systems

SECNAVINST 5239.1 (Safeguarding Personal Information in Automatic Data Processing Systems) is the Navy's implementation instruction for the Privacy Act of 1974. This instruction addresses personal information privacy and does not pertain to classified data. Two enclosures to the instruction are utilized to establish a risk assessment approach which weighs the likelihood of a security breach, the damage that would occur, and the cost of prevention. Because of the assessment approach taken, the instruction should not be considered a set of firm requirements that are mandatory under all circumstances. The document suggests that a mixture of technical and physical safeguards with strict administrative controls may be more cost effective than high-cost technical solutions. [Ref. 14: p. 11]

b. Automatic Data Processing Security Program

OPNAVINST 5239.1A (Department of the Navy Automatic Data Processing Security Program), implements DoD Directive 5215.1 (Computer Security Evaluation Center) within the Department of the Navy and integrates the directive into the Navy's ADP security program. OPNAVINST 5239.1A covers both personal security and classified data security issues. It divides data into three protection levels:

- Level I: Classified data
- Level II: Unclassified data requiring special protection, such as Privacy Act information
- Level III: Other unclassified data

Similar to SECNAVINST 5239.1, OPNAVINST 5239.1A is based upon risk assessment procedures intended to balance the threat, the possible damage, and the cost of countermeasures in a cost effective manner. Certain minimal mandatory requirements are cited; however, these are primarily regarding environmental/physical security and contingency planning as opposed to technological issues. Additionally the instruction establishes the definition of the Designated Approving Authority (DAA) for ADP accreditation. For most shipboard LANs this will be the Commanding Officer, however if the LAN is operated in the Multilevel Security mode, the authority to accredit the system rests with Commander, Naval Data Automation Command (COMNAVDAC). Computer systems may operate for a limited time under an Interim Authority to Operate, which is issued by the DAA. [Ref. 14: p. 13]

c. Navy Implementation of National Policy on the Control of Compromising Emanations (TEMPEST)

OPNAVINST C5510.93D is a CONFIDENTIAL instruction that provides policy for compliance with TEMPEST requirements. OPNAV NOTICE C5510 revises the OPNAV instruction implementing a revised national policy on compromising emanations. This notice clarifies, revises, and in some cases liberalizes previous requirements for full TEMPEST certification. [Ref. 14: pp. 12 to 13]

This technical guidance and requirements are not the focus of this thesis and will not be pursued further. The author believes the advent of fiber and use of fiber optics with LANs essentially makes TEMPEST requirements relatively simple to fulfill.

2. National Computer Security Center's Standards

In addition to the DoD standards previously described (Red and Orange Books), the National Computer Security Center (NCSC) has published a set of technical guidelines to help industry develop certifiable systems and enhance the NCSC-contractor relationship in the product evaluation phase. The guidelines promulgate testing standards to terminology that will be used. A complete description of these various standards may be found in [Ref. 14]. A list of standards is provided below:

- CSC-STD-003-85: Computer Security Requirements
- CSC-STD-004-85: Technical Rationale Behind CSC-STD-003-85
- CSC-STD-002-85: DoD Password Management Guide
- NCSC-TG-001: Audit in Trusted Systems
- NCSC-TG-002: Trusted Product Evaluation
- NCSC-TG-003: Discretionary Access Control
- NCSC-TG-004: Glossary of Computer Security Terms
- NCSC-TG-008: Trusted Distribution
- NCSC-TG-009: Computer Security Subsystem Interpretation
- NCSC-TG-011: Trusted Network Interpretation Environments Guideline
- NCSC-TG-013: Rating Maintenance Phase
- NCSC-TG-019: Trusted Product Evaluation Questionnaire

The above guidelines are more pertinent to the computer, software, and network development communities than to the user community. However, the documents are of interest to the user community from the standpoint of supporting a well informed decision regarding the acceptance of a network for a particular set of shipboard applications. [Ref. 14: p. 13]

III. NAVAL TELECOMMUNICATIONS

The Naval Telecommunications System (NTS) embraces all naval telecommunications operations that provide for the exchange information among naval forces at sea, in the air, and ashore [Ref. 15].

A. BACKGROUND

The NTS system is designed to get necessary communications to the fleet. Using the Defense Communications System as a backbone, the Navy has designed ashore and afloat automated systems to process narrative and data pattern messages. [Ref. 16]

1. Ashore Systems

Shore communications stations are the backbone of the NTS. The Naval Communications Master Stations (NAVCAMS) and the Naval Communications Station (NAVCOMMSTA) provide the conduit for communications between shore commands and the fleet. A summary from NTP-4C [Ref. 16: pp. 2-1 to 2-5] of major elements of the shore site of NTS, pertinent to this thesis, are provided below:

- Automatic Digital Network (AUTODIN)- AUTODIN is a world-wide Department of Defense computerized system which provides automatic switching of message traffic providing significantly fast service to ashore locations. The system transmits both narrative and data pattern (either card or magnetic tape) messages. Autodin provides five modes of operation that provide for the variation in speed from 100.
- words-per-minute duplex teletypewriter to 2400 baud terminals.
- Naval Communications Processing and Routing System (NAVCOMPARS)- NAVCOMPARS is the automated communications system which serves as the interface with AUTODIN or other networks ashore and operational fleet units. The system provides fleet support through broadcast management, CUDIXS or full period terminations and primary ship/shore circuits. There are five NAVCOMPAR sites, one at each of the four NAVCAMS plus one at NAVCOMSTA Stockton, California.
- Local Digital Message Exchange (LDMX)- The LDMX provides automatic message routing and reformatting for ashore Navy commands. It satisfies the Defense Communication Agency (DCA) criteria for AUTODIN access and permits entry of traffic through optical character recognition

equipment (OCRE). The system directly distributes incoming messages to and serves as the file and retrieval location for remote subscribers.

- Standard Remote Terminal (SRT)/Remote Information Exchange Terminal (RIXT)- SRT/RIXT is an input/output terminal which allows remote users to access AUFODIN.
- Common User Digital Information Exchange System (CUDIXS)- The CUDIXS system could be classified in ashore and afloat systems, but its primary components are located at the five NAVCOMPARS sites. This system provides a 2400 baud satellite link and full duplex interface for the receipt and transmission of narrative message traffic between NAVCOMPARS and the ships equipped with afloat automated systems.

2. Afloat Systems

The heart of the Navy afloat communication system is the Naval Modular Automated Communication System (NAVMACS). The system is designed to increase the speed, efficiency and capacity of the naval afloat and ashore communications operations. The NAVMACS modular concept allows the system to be configured to the particular ship class. Each NAVMACS system includes a unique device for the composition or entry of outgoing messages. For example, a message entry in NAVMACS V2 requires a paper tape copy of the message. Each ship has a specific type of output device for delivery of incoming addressed messages. On NAVMACS V2/V3 ships, a reproduced copy of a message is hand delivered to the reader. However, NAVMACS V5 provides on-line remote distribution for addressed messages which can be viewed on a Keyboard Video Display Terminal (KVDT) screen and/or printed on a remote printer. [Ref. 17] With emphasis on the types of message entry or delivery devices provided by each system, the various hardware/software configurations for NAVMACS equipped ships are described below:

- NAVMACS (V)1. This single AN/UYK-20 minicomputer-based system is used on small ships with minimal communication requirements. The NAVMACS (V)1 system can simultaneously input and screen message traffic from four fleet broadcast channels and interface with the CUDIXS Link. NAVMACS (V)1 CUDIXS Link communication is limited to send-only for message traffic. Message entry for outgoing traffic is via paper tape, and distribution of incoming addressed messages is manual, using reproduced copies. Delivery devices are four 75-baud teletype page printers. Message composition is accomplished using teletype equipment which produces 5-level paper tapes of outgoing messages. [Ref. 17]
- NAVMACS V2. A single AN/UYK-20 or AN/UYK-44 minicomputer-based system, NAVMACS V2 is installed on small ships with more peripheral equipment than NAVMACS V1. The NAVMACS V2 system can simultaneously input and screen message traffic from four fleet

broadcast channels and the CUDIXS Link - CUDIXS Link communications are half duplex, providing the input and output of message traffic. Message entry for outgoing traffic is via paper tape, and distribution of addressed incoming messages is manual, using reproduced copies. Delivery devices are two 2400-baud medium-speed line printers. Outgoing message composition can be provided by a Message Preparation Device (MPD), if installed. The output of the MPD via the NAVMACS program is a 5-level paper tape of the message and a printed copy of the message. If no MPDs are installed, message composition is accomplished by using teletype equipment which produces a 5-level paper tape of the message. Other means of 5-level tape production already being used on some ships are discussed later. [Ref. 17]

- NAVMACS V3. NAVMACS V3 is a dual AN/UYK-20 minicomputer-based system for large ships. The NAVMACS V3 system can simultaneously input and screen message traffic from four fleet broadcast channels, four Full-Period Termination (FPT) channels, and the CUDIXS Link. CUDIXS Link communications are half duplex, providing the input and output of message traffic. The FPT circuits are full duplex, providing simultaneous input and output of message traffic. The primary means of message entry for outgoing traffic is by message composition at one of the on-line KVDTs. Once the message is composed, it can be transmitted without being re-entered by paper tape. Another method of outgoing message entry is via paper tape. The message is loaded into the system, and if no format errors are detected, the message is output on the desired circuit. Distribution of incoming addressed messages is manual, using reproduced copies. Delivery devices are two 2400-baud medium-speed line printers. [Ref. 17]
- NAVMACS V5/V5A. Up to three AN/UYK-20A or AN/UYK-44 minicomputers are used in this system for very large ships with the greatest communication requirements. The NAVMACS V5/V5A system can simultaneously input and screen message traffic from multiple channels of fleet broadcast, FPT, remote devices, and remote systems. CUDIXS Link communications are half duplex, providing the input and output of message traffic. The FPT circuits are full duplex, providing the simultaneous input and output of message traffic. The primary means of message entry for outgoing traffic is message composition at one of the on-line KVDTs. Once the message is composed, it can be transmitted without being re-entered by paper tape. A second method of outgoing message entry is via paper tape. A third method of outgoing message entry is from a remote system such as the Personal Computer Remote System (PCRS) or the Naval Intelligence Processing System (NIPS). If no format errors are detected, the message is output on the desired circuit. Distribution of incoming addressed messages is automatic and controlled by a data base maintained by NAVMACS operators. On ship delivery devices include medium-speed line printers, KVDTs, paper tape punches, and remote systems. [Ref. 17]

The NAVMACS systems have not kept pace with the technology and proliferation of PCs and word processing software during the 1980's. Navy personnel, now more computer literate, find the message preparation capabilities in NAVMACS limiting and less flexible than commercial text editors; consequently, many ships have purchased PCs and software for message composition and editing. To provide the media for outgoing message entry for the NAVMACS systems, ships have also purchased paper tape reader/punches to provide paper tapes. Expensive message preparation terminals, with very limited text editing capability, using the MPDs and KVDTs are therefore ignored. [Ref. 17]

B. SYNCROTECH SOFTWARE CORPORATION INVESTIGATION

On April 26, 1991 Syncrotech Software Corporation provided results to NCTS concerning a study of options for connecting the Naval Modular Automated Communications Systems (NAVMACS) and personal computer (PC)-based Local Area Networks (LAN) aboard Navy ships. The report demonstrated the feasibility of interfacing all systems with GateGuard. GateGuard is a PC-based, software-controlled system which is already used as a shore-based communications link between Automatic Digital Network (AUTODIN) Subscriber Terminals (AST) and Office Automation Systems (OAS) via a LAN. GateGuard functions as a gateway to AUTODIN and provides the protection of a security guard device separating AUTODIN and the OAS. The system's name is derived from these basic functions. [Ref. 17]

1. Syncrotech Corporation Assumptions

Syncrotech based their investigation on several assumptions which are provided below from [Ref. 17]:

1. If required the NAVMACS family of software could be modified. However, the amount of coding needed to implement a new Input/Output (I/O) driver to handle a PC/GateGuard interface required investigation. Any additional code would reduce the already low amount of dynamic memory used to temporarily store incoming messages. This is most critical in NAVMACS V2, which has no long-term storage. NAVMACS V1 was not a candidate for the PC/GateGuard interface.
2. For security reasons, the GateGuard terminal would be co-located with the NAVMACS V2/V3 systems, since NAVMACS V2 provides no security control for delivery devices, and NAVMACS V3 only provides security control for transmit circuits. GateGuard would provide the security protection required for NAVMACS V2/V3 remote distribution. NAVMACS V5 can control the level of security for any remote system or device.
3. The current screening/control functions (e. g -, Command Guard List (CGL), Local Routing List (LRL), or all NAVMACS V5 screening) would remain in the respective NAVMACS programs, and GateGuard would only be used to augment these functions at an office level. The final control of when and how a message is transmitted on a specific circuit would also still remain in the NAVMACS program.

2. Syncrotech Corporation Proposed Solutions

In Syncrotech's report the final proposed solutions fell into three categories; a solution for NAVMACS V5, a solution for NAVMACS V2 and V3, and a long term solution for the entire NAVMACS modular family. The proposed solutions, from [Ref. 17] are summarized below.

1. NAVMACS V5/V5A - NAVMACS V5/V5A currently supports a remote system interface which provides a path for outgoing message entry and remote distribution. The Generic Interface Design Specification (IDS) for NAVMACS V5/V5A provides the information necessary to pass messages to and from NAVMACS V5/V5A. Using this interface, NAVMACS V5/V5A could be connected to GateGuard. NAVMACS V5/V5A would interface with GateGuard via a Bus Interface Unit (BIU) while the ship is underway. While in port, the GateGuard could connect with the local NTCC, via secure telephone communications, for over the counter message traffic delivery. The various interface connections are made possible by the BIU, which provides the required interface level conversions and handles the interface protocol necessary to pass message data. The software-controlled interface protocol in the BIU would have to be changed to communicate using NAVMACS V5/V5A generic interface protocol while the ship is underway. While the ship is in port, the BIU could use the existing AST protocol to interface with the shore. The software in the BIU which communicates with GateGuard would remain unchanged in either case. Changes to the NAVMACS V5/V5A remote system interface were analyzed but were not proposed because these flex channels are now used by several other systems. Any software to handle the current BIU protocol would require additional changes to the NAVMACS V5 operating system, as well as the addition of a new remote system software control module.

2. NAVMACS V2/V3. As designed, NAVMACS V2/V3 software does not provide a remote interface for message entry and delivery. However, NAVMACS V2/V3 does provide an International Telegraph Alphabet #2 (ITA-2) Baudot interface which inputs data from and outputs data to a 75-baud ITA-2 Baudot device, normally a paper tape reader/punch. Access to this I/O channel is provided via a secure patch panel. The program controlled baud rate for this channel is currently set at the lowest rate on the AN/UYK-20 I/O card. The rate may be changed by restrapping the I/O card; the software need not be modified. While the ship is underway, a BIU could be connected to this channel, and the required interface protocol software could be downloaded. NAVMACS V2/V3 would then be interfaced with GateGuard as shown in Figure 3. Message entry for NAVMACS V2 transmission on the CUDIXS Link would be handled like the current method. The NAVMACS operator would enter TRA TR2, and the GateGuard operator would then initiate the message transfer to NAVMACS via the BIU. Message entry from NAVMACS V3 would be accomplished by using the LOD MSG TR2 RELAY command from any KVDT. Message distribution to GateGuard could be accomplished by modifying the NAVMACS V2/V3 software to send all addressed messages to both PR1 and TP2. Message distribution may also be accomplished by having the shore station add a Plain Language Address (PLA) to the NAVMACS Originator Screening List (OSL) for all fleet broadcast and CUDIXS messages. The NAVMACS V2/V3 operator can then take TP1 down, which altroutes the messages to TP2 (GateGuard) for distribution to a LAN. The GateGuard terminal should be located inside the Main Communication Center (MAIN COMM), as, NAVMACS cannot control the security level for messages sent to TP2. Responsibility for primary delivery of addressed messages would still remain with the line printer connected to the NAVMACS V2/V3 system. While the ship is in port, NAVMACS V2/V3 could receive over-the-counter service via a shore AST connection. The BIU would then be downloaded with the AST interface protocol software.

3. NAVMACS V2/V3/V5/V5A Universal Serial Interface. A PC with the required serial interface boards can be connected to any NAVMACS system. Software capable of handling all the required functions could then be downloaded and run under Windows. Because GateGuard does not currently provide these features, the PC program would have to be developed using commercial off-the-shelf software when possible. The NAVMACS Universal Serial Interface (NUSI) concept would at a minimum provide windows for the Control Teletype (CTTY), KVDT, paper tape reader/punch, diskette message entry/storage interface, LAN, shore AUTODIN connection, and remote system interface. Each serial interface connection would be assigned a window for monitoring and control. Access to each window would be provided by the host PC. The functions provided by each window would be limited to the existing services that each interface currently provides (e. g the CTTY window would be used for NAVMACS V2 command entry/system response). One major advantage to this proposed solution is that it overcomes the message entry problem which occurs when an operator enters TRA TR2 on the CTTY or LOD MSG TR2 RELAY from a NAVMACS V3 KVDT. When the operator enters TRA TR2 in the CTTY window, the program could initiate the input message transfer immediately because it also controls the message entry to/from NAVMACS via the TP/TR2 I/O port. The same applies to the NAVMACS V3 system through the use of a KVDT window.

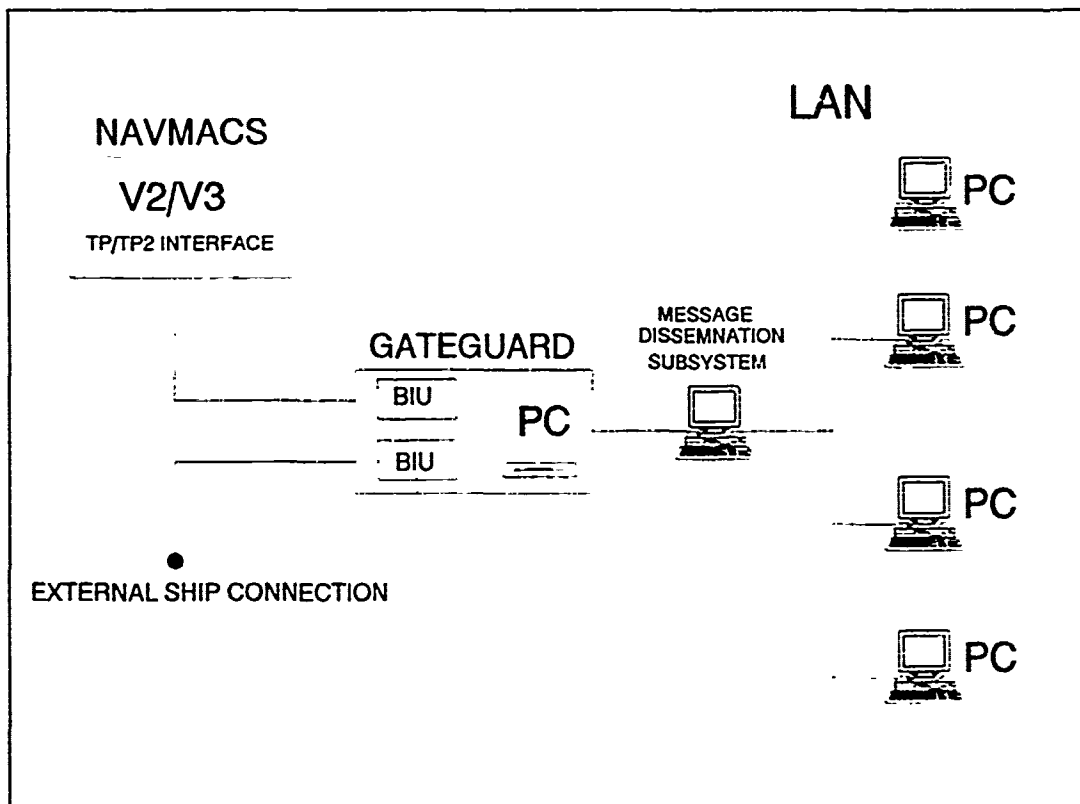


Figure 3 NAVMACS V2/V3 and Gateguard interface

3. Syncrotech Corporation Conclusions

The Syncrotech report final conclusions stated that GateGuard can be connected to any NAVMACS system provided that the BIU interface protocol can be changed to accommodate each system. Additionally, changes to the NAVMACS interface handlers to emulate the required transfer protocol for the BIU interface are restricted by memory limitations. NAVMACS V2/V3 software must be changed to provide distribution to a device (I/O channel) other than PR1 and PR2 unless the concepts outlined by Syncrotech are utilized. [Ref. 17]

C. SHORE COMMAND INTERFACE

Naval Communications Detachment, Cheltenham, Maryland, the Naval command responsible for maintaining the NAVMACS family software, currently has a GateGuard computer linked to their servicing LDMX using a Bit Interface Card (BIC) to replace a BIU. In other words they are using an inboard circuit board to replace an outboard box. The protocol used between LDMX and GateGuard is not supported by NAVMACS. Software in the BIC will have to be modified to support NAVMACS V5 remote terminal protocol. To date, no further progress has been made in connecting GateGuard to NAVMACS. [Ref. 18]

D. NAVMACS II

Director, Space and Electronic Warfare (OP-094), is the principal advisor to the Chief of Naval Operations (CNO) concerning command and control matters, and is responsible for ensuring optimum use of Navy Information systems [Ref. 19]. OP-094 is currently strongly pursuing a program to replace the NAVMACS variants with NAVMACS II. Hardware for this system would be acquired from a Command and Control Workstation. Initially this uses the Desk Top Computer Contract 2 (DTC-2). Initial design uses a SUN workstation with VME bus SPARC technology. The hardware would be designed and implemented to accommodate upgrades every eighteen to twenty-four months. Software utilizes the UNIX operating system, and application programs will be written in C and Ada. This system

has an ETHERNET interface, so connectivity to remote terminals on a LAN is planned. However, the driving force to replace NAVMACS variants is to replace the maintenance-expensive UYK-20's and 44s and to obtain a system that can support higher speed ship-shore links. An overview of NAVMACS II can be seen in Figure 4. The schedule for deployment of this prototype system is ambitious and scheduled for April of 1992. Plans are to deploy the system battlegroup by battlegroup, which means literally dismantling the system on an individual ship within one battlegroup and installing it on another ship in a different battlegroup. Although the NAVMACS II specifically intends to interface with a LAN, little attention has been given to security issues. [Ref. 20]

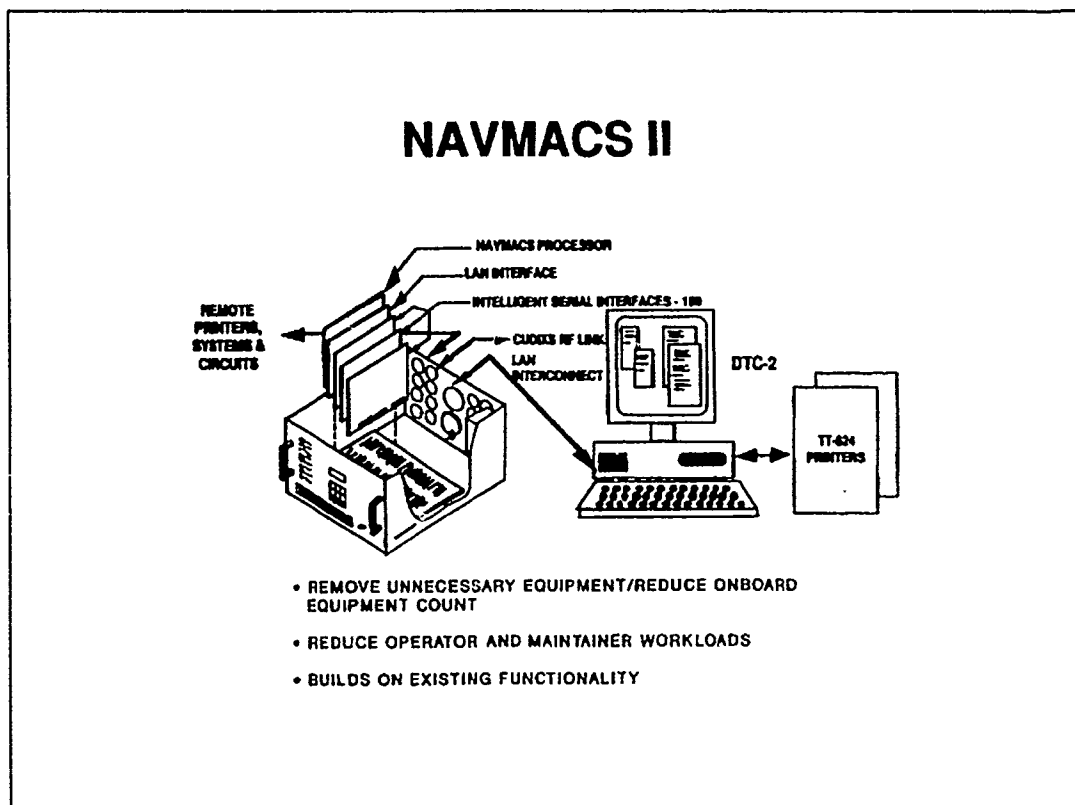


Figure 4 NAVMACS II overview

E. ASSESSMENT

As discussed in Chapter I, any viable shipboard LAN must be capable of integrating the ship's message center. The first step to accomplish this was taken by having Syncrotech research the feasibility of connecting NAVMACS with a GateGuard computer. Unfortunately no further progress has been made due to the desire to acquire the NAVMACS II variant and, in the author's opinion, the lack of a Navy Command entity pushing to get the task accomplished. Regardless of the NAVMACS variant, the issue of routing various classifications of messages on a shipboard LAN has not been addressed. The state of world affairs and the subsequent declining US Defense budget may delay the acquisition of NAVMACS II. The recommendation of Syncrotech to modify the NAVMACS V2 and V3 operating system should be pursued to further the progress towards a multilevel secure shipboard LAN. The Syncrotech focus on the NAVMACS V5 system also confirms the author's opinion that only large ships, such as aircraft carriers and heavy amphibious assault ships will benefit from any further progress. NCTS provided Syncrotech with a listing of Afloat Automated Telecommunications systems for which they were responsible for maintaining the appropriate software operating programs. The commands included Coast Guard units as well as several Marine Corps commands. The list was qualified as being subject to change due to various fleet upgrades and ship decommissioning. Regardless, the figures are apparent that the primary NAVMACS variant in use is the NAVMACS V2. Of the 402 commands listed, the breakdown of NAVMACS variants is as follows: NAVMACS V5/V5A: 28, NAVMACS V3: 69, NAVMACS V2: 266, NAVMACS V1: 50. Admittedly, larger commands with NAVMACS V5 process more message traffic; however, it may be prudent to pursue a multilevel secure LAN on a NAVMACS V2 or V3 ship where quality control could be more easily accomplished and lessons learned provided to benefit implementation on larger ships. Simply stated, it would be easier to evaluate a multilevel secure LAN on a Guided Missile Cruiser with fewer nodes (easier initial physical security to monitor) and less classified message traffic.

IV. DEFENSE MESSAGE SYSTEM INITIATIVES

The target architecture of the Defense Message System (DMS) is to provide electronic delivery of messages between organizations and individuals in the DoD. AUTODIN currently provides message service between organizational elements while the DDN E-Mail provides message service between individuals. Although both systems provide messaging services to DoD users, they are currently not interoperable. DMS consists of hardware, software, procedures, facilities, and personnel involved in transferring messages from writer to reader, except for the transmission systems providing connectivity, such as the Defense Data Network (DDN) and base level transmission facilities. The DMS target architecture will attempt to make AUTODIN and DDN E-Mail interoperable, therefore a baseline was established consisting of AUTODIN, its baselevel support Telecommunications Centers (TCCs), and E-Mail on the DDN, as they existed in September of 1989. This baseline, frozen in time for comparison purposes, serves as the reference against which the future performance, costs, and manpower incurred during the evolution of the target architecture will be measured and compared. [Ref. 21]

DMS is not and will not be a network or a single supplier service. It is intended and foreseen that DMS will be a multi-vendored combination of user-owned and managed equipment in combination with user-leased services connected to DCS-owned and managed equipment. Interoperability and standardization of these various equipments and services will be achieved by linking them together with a common set of messaging (X.400) and directory (X.500) protocols. [Ref. 21: p. 1-2]

A. BACKGROUND

Previous efforts to modernize the DoD's messaging capabilities were terminated in January of 1988 by the Assistant Secretary of Defense Command, Control, Communications and Intelligence (ASD C3I) due to blunders. A multi-service and Agency Defense Message System Working Group (DMSWG) was then established to assess the DoD's messaging systems future. The goal was to improve the current

system's functionality, survivability, and security while concurrently reducing costs, staffing, and maintenance services. [Ref. 21: p. 1-1]

Through 1988, a recommended architecture and the phases for transitioning from the baseline to the target system were developed and approved. In August of 1988 the Under Secretary for Acquisition issued DMS program guidance assigning the Defense Communications Agency (DCA) the overall coordination responsibilities for the DMS program. This guidance provided a phased implementation strategy, a test and evaluation strategy along with conceptual approval of the target architecture. On November 2, 1989, ASD C3I issued a policy for transition to the DMS target architecture, mandating all services/agencies to develop and maintain their own DMS transition plans which detail the evolution of the base level and regional messaging facilities to the DMS target architecture. [Ref. 21: p. 1-1]

B. DEPARTMENT OF THE NAVY TRANSITION PLAN

The Department of the Navy (DON) implementation of the DMS will be evolutionary and is being conducted in three phases. Phase I, 1989-1994, centers on the automation of existing TCC functions, the extension of message services to the user, and migrating AUTODIN data pattern traffic to the DDN. AUTODIN and DDN E-Mail will continue to exist as separate but interoperable systems at the end of Phase I. In Phase II, 1995-2000, the TCCs will begin to be phased out and the X.400 and X.500 protocols will become available. Base user desk-top workstations, connected via BITS, will provide base-wide connectivity. Planned Message Security Protocol (MSP) components will be embedded in the user workstation to permit secure messaging throughout DoD. Phase III, estimated for completion by the year 2008, will implement the final DMS target architecture. The ultimate goal of this final phase is to provide end-to-end Integrated Services Digital Network (ISDN) connectivity. [Ref. 22]

Phase I implementation is currently ongoing in a strong and steady manner. This phase primarily involves shore commands and their servicing Navy Telecommunications Centers (NTCCs).

1. Navy Telecommunications Centers

Presently, NTCCs provide DON users with access to AUTODIN and offer over-the-counter (OTC) message services. Organizations which include ships in port and Naval shore commands (defined as subscribers), exchange messages with their servicing NTCC via the manual, manpower intensive, laborious OTC procedure. These procedures include manual distribution decisions on incoming messages as well as paper reproduction and manual collation of multiple page messages. The NTCC is said to either guard or protect for these subscribers. The term "guard" means that the NTCC provides internal office distribution to specified subscribers. The term "protect" specifies the NTCC to provide only a set number of copies to the subscriber, which arranges for its own internal distribution. Currently NTCC systems include LDMX, SRT, and RIXTs, which were defined and described in Chapter III. NAVCOMPARS, also described in Chapter II, provides communication links between underway ships and AUTODIN. Although outside the scope of DMS, the NAVCOMPARS must evolve to interface to the new DMS messaging service. [Ref. 22: p. E4]

It is the DMS Phase I implementation that is most applicable to the shipboard environment, and this phase where technology and lessons learned can be utilized in developing a shipboard LAN capable of fully integrating the ship's communication center. Chapter III discussed Syncrotech Corporation's investigation into connecting NAVMACS to GateGuard. The author has deduced that the tasking for the investigation was prompted by the DMS Phase I implementation at certain NTCCs and shore commands.

With the goal of providing writer-to-reader messaging, the implementation of the DMS in the DON will eliminate messages using paper media between the user organization and the NTCC. DMS Phase I will utilize the Navy Standard Teleprinter Ashore (NSTA) to satisfy requirements for low-cost message terminals, replacing teletype, Optical Character Readers (OCRs), and punched card/tape equipment. The NSTA allows a Personal Computer Message Terminal (PCMT) to exchange traffic with the NTCC using diskettes. Although the exchange of diskettes requires couriers (over-the-counter service), the implementation eliminates the use of paper, OCRs, and card punches, facilitating easier

message handling at the NTCC. The use of GateGuard provides electrical connectivity to the NTCC (with the LDMX) using the KERMIT protocol. As described in Chapter III, GateGuard is linked to the user's organization Office Automation System (OAS). GateGuard ensures that traffic electronically received from the NTCC does not exceed the classification level of the OAS. The implementation of common procedures and central accountability for organizational message receipt establishes a certification boundary between the DON and the DCA. Initially, GateGuard has only supported electrical message transfer from the NTCC to the OAS. When approved release authentication technologies or procedures are implemented on the OAS, a two way GateGuard exchange will be allowed. [Ref. 22: pp. 3-2 to 3-3]

Currently, most organizational OASs run at the unclassified level. Higher classified LANs exist, but normally run on a system high level concept, which was discussed in Chapter II. Separate GateGuard are required for unclassified messages passed to the OAS and for classified messages printed or written to diskette for manual dissemination. If a certified multilevel secure LAN exists, only one GateGuard will be required. The Navy DMS transition plan calls for pursuit of accreditation for a single GateGuard capable of segregating messages by classification. [Ref. 22: pp. 3-3 to 3-4]

The Phase I plan also includes the implementation of a Multilevel Mail Server (MMS) that will provide dedicated and dial-up GateGuard interfaces to user electronic mail boxes at the NTCC. The MMS will allow the exchange of message traffic classified up to SECRET. Additionally, a network of MMSs is being planned to phase out the use of AUTODIN. The MMS network, interconnecting MMSs via the Defense Integrated Secure Network (DISNET), will handle AUTODIN message traffic between Naval commands served by the MMS. [Ref. 22: p. E6]

MMS will be discussed in greater detail below; however a brief overview of security services from [Ref. 22] is considered appropriate because it may provide some points for comparison when reviewing shipboard options.

2. Security Services Provided

Present DON NTCCs systems have not been formally evaluated in accordance with the DoD directives discussed in Chapter II. The systems are certified by the Naval Telecommunications Integration Center (NAVTELSYSIC) and accredited by Commander, Naval Computer and Telecommunications Command. Additionally, all NTCC systems undergo DCA certification before connecting to AUTODIN. All communication links to the AUTODIN are encrypted using the KG family of encryption devices. The DDN is currently segregated into the MILNET for unclassified service and the three other networks are for classified material. Each classified network carries only one security level, SECRET on DISNET 1, TOP SECRET on DISNET 2, and TOP SECRET/ SPECIAL COMPARTMENTED INFORMATION (SCI) on DISNET 3. Intentions are to merge the three separate networks into one network, the DISNET. Physically unprotected trunks and host access lines on the MILNET are being link encrypted using KG-84As. A Low-cost Encryption and Authentication Device (LEAD) is planned to provide link encryption on MILNET terminals. On the classified systems, KG-84A devices are used for link encryption of physically unprotected trunks, host access lines, and terminal access lines. BLACKER, providing end-to-end link encryption is beginning to be implemented on the three DISNETS. [Ref. 22: pp. 3-36 to 3-37]

C. MULTILEVEL MAIL SERVER

The objective of the Multilevel Mail Server (MMS) project is to provide the capability of electronically exchanging various classified organizational messages between NTCC's LDMX and its over-the-counter subscribers. This will be accomplished with dial-up interfaces between a subscribers GateGuard to subscribers mailboxes within the MMS. The initial MMS will be installed at NTCC Cheltenham, Maryland to aid in defining configuration requirements and operational procedures needed for fielding at other sites. Specific goals for the MMS project include [Ref. 23]:

- Provide Gateguard with connectivity to the TCC
- Provide extended storage for organizations not operating on a 24 hour basis

- Provide message separation by classification
- Provide low cost secure dial-up connectivity
- Eliminate LDMX port availability contention
- Eliminate over-the-counter processing of Unclassified to Secret AUTODIN messages
- Provide the connectivity for receipt and transmission of AUTODIN messages via diskette or the subscriber OAS.

1. **MMS General Operating Overview**

The LDMX will segregate subscriber's message traffic by classification to separate circuits for the MMS. Three circuits will be provided, one each for Unclassified, Confidential, and Secret messages. After processing the messages from the LDMX, the MMS will post the messages to separately segregated subscriber accounts that have been programmed into the MMS Alias file. The MMS will determine the correct mailbox account for each message received by reading a predefined and pre-formatted Routing Indicator (RI) from the established format line and field of the message.

[Ref. 23: p. 2-3]

Subscribers will access the MMS from their installed GateGuard systems and Secure Telephone Unit III (STU-III) using the public telephone network. When subscribers access the MMS, they will be able to download messages waiting for them. MMS will download messages that are classified at the classification level that was accessed. The MMS will allow subscribers to download messages that are classified at lower classification levels than that level used to access the MMS, provided the subscriber had previously notified the NTCC of the requirement to download messages of multiple classifications during one login session. Higher classification levels than the one that is used to access the MMS will not be able to be downloaded. [Ref. 23: p. 2-3]

a. The MMS Processor

The AT&T 3B2/600G minicomputer available from the Standard Multi-user Small Computer Requirements Contract (SMSCRC) will be used as the MMS processor. The computer will operate at 24 MHz and contain a minimum of 32 MBytes of Random Access Memory (RAM). It will

be equipped with a multi-processor board which will support off-loading many of the less important system functions to itself thereby providing more time for the main processor to perform the primary system functions. The system was also designed to accommodate future expansion of the MMS requirements through system upgrades. [Ref. 23: pp. 3-7 to 3-8]

b. MMS Operating System

The MMS processor will initially run release 3.2.3.30 of the UNIX System V/MLS operating system which was specifically designed for the 3B2/600G. The operating system is designed to meet the TCB level of B1, however it is not yet certified by NCSC. The operating system's predecessor is currently certified at the B1 level, and because the new version is simply an extension of the certified release it is expected the new release will be certified prior to installation at Cheltenham. The system V/MLS TCB is protected from modification by non-administrative users through mandatory and discretionary access control. The system will be used in a multi-user mode. [Ref. 23: p. 3-11]

2. Selected MMS Detailed Operating Characteristics

The MMS will provide on-line access for the electronic exchange of AUTODIN messages between the NTCC's LDMX and a subscriber's GateGuard. Two way transfer of messages, from the LDMX to the GateGuard, and from the GateGuard to the LDMX is the ultimate goal. The MMS is the interface between the two systems and requires the capability to communicate with both, while concurrently separating messages by classification. [Ref. 23: p. 3-16]

The MMS will utilize V/MLS Secure Mail Package to enable the system to work; in the author's opinion, a similar package will be an integral part of a future shipboard MLS LAN. The E-mail package of the MMS V/MLS Operating System is mandatory and must be included in the final B1 certification. The secure mail package provides a repository for messages received from both the LDMX and from the subscriber's GateGuard. [Ref. 23: p. 3-11]

Each subscriber organization will have mailbox accounts established within the MMS and individual messages will be posted to separate class-marked mailboxes. After determining appropriate

distribution upon receiving the message from the LDMX the MMS E-mail system will append an E-mail header to the message and post it to the appropriate mailbox account which is determined by the specific subscriber to which the message is addressed and the classification of the message. The E-mail header is removed when the message is transferred to and from the LDMX or GateGuard, depending on which way the transmission is initiated. The E-mail header is only used for the internal processing within the MMS. Figure 5 demonstrates message flow procedures from the LDMX to the GateGuard. The process for message flow from a GateGuard to the LDMX is opposite of that shown in Figure 5, excluding access control processes such as subscriber logon and authentication. [Ref. 23: p. 3-21]

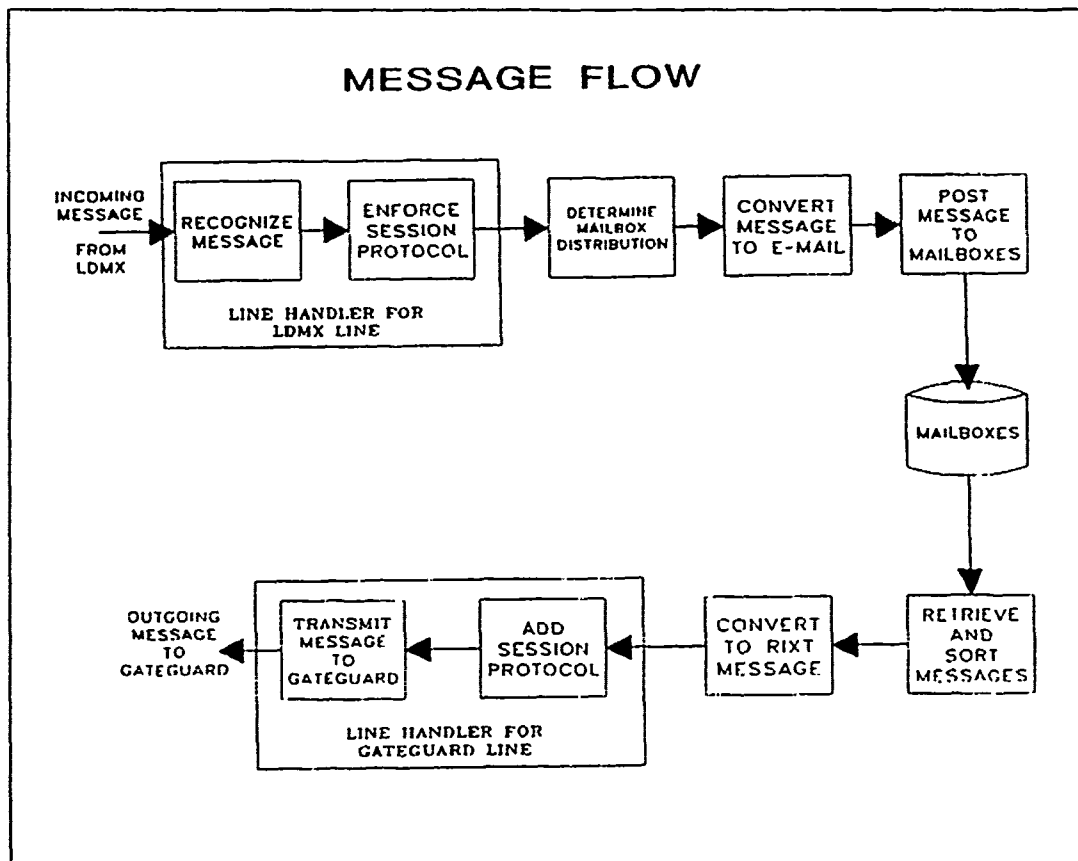


Figure 5 Message flow procedures from LDMX to GateGuard

MMS utilizes an RIXT protocol conversion to make the MMS appear to be an RIXT to the LDMX. Besides converting the protocol, the process will ensure that the classification link between the LDMX and the MMS is not exceeded. Messages will be delivered to both the LDMX and the Gateguard by First in First Out (FIFO) precedence. [Ref. 23: p. 3-21]

a. Access Control and Authentication

Access to the MMS will be controlled by a MLS Operating System. Subscribers must be capable of presenting identification and authentication (password) information that is recognized by the MMS TCB. The ID and password will map to mailbox accounts and, in conjunction with the security of the data port used to access the MMS, to a security level the subscriber is authorized to access. [Ref. 23: p. 3-24]

STU-III's with a STU-III Access Control System (SACS) will be used to provide synchronous dial-up communications between the GateGuard and MMS over the public telephone switched network. SACS will authenticate subscribers prior to gaining access to the MMS through a feature which provides affirmative authentication of a specific user by Key ID and/or Department Agency or Organization (DAO) code. SACS will be maintained and updated by system operators at the NTCC. SACS will prevent the calling party from establishing a link if the calling party is not listed on the access control list within SACS. Separate telephone numbers will be provided for each of the three message classifications. [Ref. 23: p. 3-24] Figure 6 provides an overview of MMS interfaces.

b. Support Software Environment

The Secure Mail Package must be compatible with the System V/MLS operating system. The intended database management system to be utilized is the UNIFY 2000, along with the PRELUDE office automation system. These and any other compiled software application programs must be compatible with the operating system. It is not anticipated that this will be a problem because the mentioned systems are available through the SMSCRC commodities contract which is the contract vehicle for the procurement of the software and hardware for the MMS. [Ref. 23: p. 4-4]

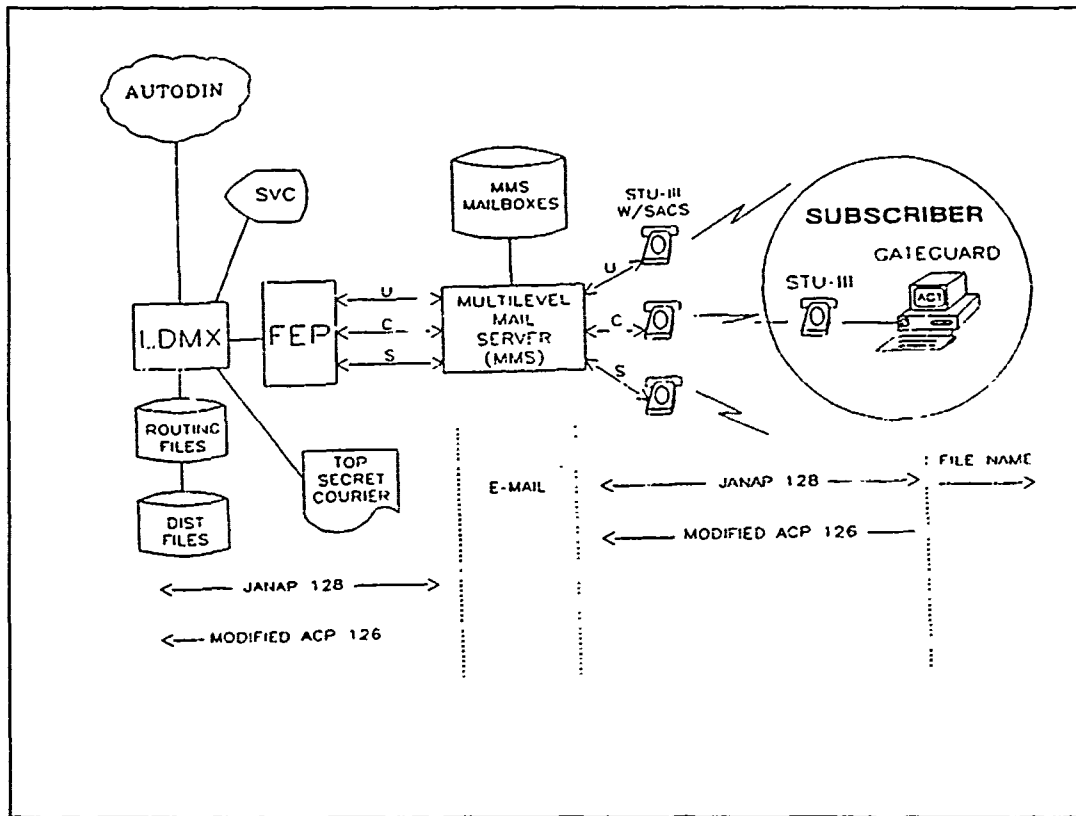


Figure 6 MMS interfaces

D. MESSAGE DISSEMINATION SUBSYSTEM

As stated previously DMS is a system in the sense that its components work together to perform a function, it is the result of many separate development and acquisition activities. The Message Dissemination Subsystem (MDS) is one of these components and is being implemented in a non-DCS/NTS Automated Information (AIS) supporting DoD messaging. [Ref. 24]

1. MDS Objectives

The MDS system is designed to provide a system to automate organizational messaging handling procedures. The system was designed based on the following objectives [Ref. 24: p. 3]:

- To eliminate manual message dissemination procedures requiring message reproduction and courier services.
- To operate at the system high security level of an organization's LAN and ADP systems.

- To require that all user terminals be IBM PC compatible with a connecting LAN and file server.
- To implement file server and user terminal software that is POSIX and MS-DOS compatible.
- To provide file transfer of messages in accordance with Navy formats, transparent to the operating environment.
- To use X.400/X.500 compatible design considerations permitting upgrade through commercial operating/network system enhancements.
- To use COTS equipment and systems software to take advantage of technology advancements in the area of office automation.
- To migrate using COTS and Non-Developmental items evolutionary implementation to the Government Open Systems Interconnection Profile (GOSIP).

2. Functional Description

The MDS will electronically send, receive and disseminate messages by utilizing a PC LAN. MDS is designed to accept input from standard diskette or Autodin messages from GateGuard. Additionally, MDS is capable of disseminating inter-office memos, individual DDN E-mail, and an organizational message summary. The distribution of organizational messages is the focus of this thesis, consequently attention will only be focused on the organizational message dissemination capabilities of MDS.

Basic components of the MDS include [Ref. 24: p. 17]:

- PC LAN - A PC LAN and file server will provide the medium for the electronic distribution of organizational message traffic.
- The Message Dissemination Subsystem File Server (MDSFS) - is the component of MDS that will be resident on the file server. This file server will allow the distribution of incoming or back-routed outgoing organizational messages to the AIS users.
- The MDS User Interface Program (MDSUIP) - is the component which allows access to the organizational message files created by the MDSFS. The MDSUIP will allow a user to select and view an organizational message.
- Marine Corps Text Format Editor (MTF Editor) - The MTF Editor is user PC software that allows a user to create, format, edit, and output an organizational message in accordance with required DoD message formats.

a. MDSFS Message Input and Queuing

The MDSFS will receive formatted message via GateGuard (utilizing the KERMIT protocol) or from floppy diskette and copy them to a directory in the MDSFS file server. As specified by the user, the MDSFS will poll the directory and when messages are present the MDSFS distribution process will begin. Distribution entails automatically searching the message for key information. Messages addressed to Navy shore commands require the originator to include office code routing indicators in the format of the message, thus the key information could be very easy to obtain. Once receiving user offices have been identified, a temporary log will be updated to facilitate distribution processing. Each user work station will have a message summary file in their PC LAN file server. The summary will contain records of organizational messages that have been distributed by the MDSFS. As new messages are received they will be appended to the user's message summary. [Ref. 24: p. 30]

b. MDSUIP Message Selection and Delivery

The MDSUIP component of the MDS is the user workstation software. It provides the user with a method of scanning and sorting messages waiting for inspection or action. Users will access their respective message summary file to review messages awaiting their inspection. The database records will include critical information about the message, such as the Originator, Date-Time-Group, subject, classification, and precedence. The database will be reviewed in a summary line format allowing the user to view characteristics of more than twenty message simultaneously. When the user selects the message for viewing, the MDSUIP will retrieve the message from the common message directory for viewing. The file will not be copied but only read into the user workstation's memory. Users will not have a write capability to the original message. This intended to preserve message integrity; however, a user may request the path and file name of the message. [Ref. 24: p. 33]

V. TRUSTED XENIX AND VERDIX SECURE LOCAL AREA NETWORK

The purpose of this chapter is to describe two products that are commercially available today. The author chose the Trusted XENIX and Verdix Secure LAN because they are two products that have been formally evaluated by the NCSC to meet B2 criteria. The primary references that support this chapter consists of company literature that does not disclose proprietary information. One must remember that the literature is primarily used to sell the individual products; however the author is only referencing literature that provides a functional description of the two products. The formal NCSC evaluation justifies the presentation of these two products. The author is not endorsing any of the products, but only desires to review the capabilities to demonstrate how they may be applied to a shipboard multilevel secure LAN.

Trusted Information Systems produces Trusted XENIX, a trusted operating system that controls information access to specific individuals and the network from the workstation. Verdix Secure LAN (VSLAN) components control the flow of information to each network component (e.g., server, workstation, gateway, printer). Coupled with software, integration of the two products allows for the exchange of compatible security labels, providing a MLS solution to many requirements. [Ref. 25]

A. TRUSTED XENIX

Trusted XENIX is a multilevel secure operating system for IBM Personal Computers and fully compatible clones. The Trusted XENIX System consists of three components. The Trusted Xenix Operating System is the base component and a prerequisite for the other components. The operating system performs several functions which include enforcing mandatory and discretionary security policies, performing user identification and authentication, generating audit trail and accounting records, and

providing a base to build secure application programs. The second component, the Trusted Xenix Development System, provides a set of application development software tools, including the C programming language. The Trusted Xenix Text Formatting System is the third component and provides high-level formatting macros for document preparation. [Ref. 26]

1. Environmental Strengths

Trusted Xenix enforces a least privileged user principle, allowing each user to perform only those functions required to perform their respective tasks. Normal user functions include tasks such as running application software, creating and deleting their files, and using editors. There are five different privileged user roles in addition to the normal users. They include a System Security Administrator, Secure Operator Account Administrator, and a Trusted System Programmer and Auditor. One person may fulfill the role of more than one function; however, they can only act in one capacity per login session. A wide range of auditing capabilities are available, including all actions taken by privileged users. [Ref. 26]

2. Communications Support

Separate from the operating system software, Trusted Information Systems also offers a communication software package. This software includes three network TCP/IP applications, single network TCP/IP, dual network TCP/IP, and Multilevel TCP/IP, each targeted towards different consumers with specific security needs to meet their LAN configurations. Additionally, a Multilevel STU-III software package is included in the software package. By utilizing this communications package, the Trusted XENIX user can communicate with an unlimited number of users. The TCP/IP programs provide a fully capable set of standard protocols including [Ref. 26]:

- Transmission Control Protocol (TCP) - provides reliable data transfer between computers.
- Internet Protocol (IP) - enables data to be transferred across networks using different technologies, e.g. X.25 and IEEE 802.3.
- File Transfer Protocol (FTP) - transfers files between computers.
- Simple Mail Transfer Protocol (SMTP) - sends and receives mail between computers.

- Telnet Protocol - provides for login on remote computer systems.

The Multilevel STU-III Software automates the setting of the Trusted XENIX security level for the STU-III serial-port connection by using special security labels provided by the STU-III hardware device. This eliminates the possibility of operator error and allows for remote multilevel security operations with STU-III communications security protection. [Ref. 26]

B. VERDIX SECURE LOCAL AREA NETWORK

The VERDIX Secure LAN (VSLAN) is a network component that is capable of interconnecting hosts systems operating at different security levels. The system mediates access between hosts, it does not mediate access attempts to host processes to information on host systems. It is intended to be used as a trusted building block upon which complete trusted network systems can be built. [Ref. 27]

The VSLAN was developed to provide the following services to its hosts [Ref. 27]:

- A system bus interface.
- A datagram-orientated communications service.
- Mediation of all data transfers between attached hosts in accordance with the VSLAN mandatory and discretionary access control policies.
- Identification and authentication of the individual responsible for operating a node of the network.
- Centralized management functions for security officers to exercise control over the operation of VSLAN.
- A capability to protect host datagrams and VSLAN control information against modification by random transmission errors.

The VSLAN supports the Ethernet/IEEE 802.3 protocol and provides backplane compatibility with most microcomputers, minicomputers, and workstations including PC-Bus (286/386 PCs), VMEbus (i.e., SUN workstations), 3B2 Bus (AT&T 3B2), and NuBus (Apple MAC II). The system also includes an eight port terminal server that supports TCP/IP and Telnet protocols. VSLAN is transparent to host operating systems and higher level protocols, supporting various versions of UNIX, VMS, and DOS. [Ref. 27]

1. Product Overview

The VSLAN implements a Network TCB distributed over a LAN of various host systems and interface components. The Network TCB provides interconnectivity between user systems according to a defined security policy, and performs access control, identification, authentication and audit. Enforcement of the user's defined security policy is accomplished by hardware, software, and firmware built into the system. The desired security policy is input via parameters by the Network Security Officer (NSO). The NSO is the individual responsible for administering security on the network. [Ref. 27]

A secure LAN consists of a single VERDIX Network Security Center (VNSC) and multiple Verdex Network Security Devices (VNSDs), which are very similar to the TIUs discussed in Chapter II. The VNSC provides the capabilities for the NSO to control and audit security aspects of the network. The VNSD is the LAN interface that addresses functional areas of access control, encryption and communications. The VNSD mediates incoming and outgoing packets based on the defined security parameters implemented by the NSO through the VNSC. [Ref. 27]

a. The Verdex Network Security Center

The VNSC manages the security operations of the VSLAN. The VNSC is a dedicated workstation which includes secure network management software and a built in secure LAN interface. The VNSC generates authentication keys for network initialization and communicates transmit and receive security policies for users of the LAN. Additionally, the VNSC maintains audit trails of network activity and generates audible and visual alarms when security violation attempts occur. [Ref. 27]

The VNSC programs a Personal Identification Device (PID) for each user. The users communicate an initialization request to the VNSC by inserting their PID in the VNSD key receptacle. The VNSC then authenticates the trusted VNSD, and alerts if the initialization fails authentication. Proper authentication establishes a trusted path of communication between the VNSC and the VNSD. The VNSC then downloads the data access rules to the VNSD. These data access rules define "security windows" through which data can be received or transmitted consistent with the predefined security

policy. The windows define the levels and categories of data which can be received and transmitted. The "receive security window" defines data the node can receive from the LAN, and the "transmit window" defines the data the node may transmit to the LAN. Complete audit trails are maintained on all security related events. The software for VNSC includes all system and application software required for network and security management. The software cannot be modified by the user. The VNSC is a specially configured computer equipped with audible alarms. It also includes a VGA monitor and audit printer. The VNSC interfaces directly to the IEEE Ethernet/802.3 LAN. [Ref. 27]

b. The Verdix Network Security Device

The Verdix Network Security Device (VNSD) is the secure interface to the VSLAN. It is a trusted interface that functions as a multilevel, multi-compartment component and mediates the flow of data between LAN nodes. The VNSD enforces the network security policy by verifying every attempted data transfer against the data access rules implemented by the VNSC. The VNSD checks that the security label of the data is consistent with both the transmit and receive windows. All data not satisfying the transmit and receive security checks are rejected and the VNSC is alerted to the attempted violation. [Ref. 27]

The VNSD hardware is available in several board-level configurations. They are functionally identical, yet each provides for a different host bus interface. The VNSD contains a communication interface, data separation kernel, authentication key interface, encryption hardware, processor, and memory for the VNSD program and data. Interaction between the modules is performed via a local address/data bus driven by the master processor and Ethernet blocks. The VNSD is driven by the 16-bit Intel 80286 microprocessor and uses the Intel 82586 micro-controller to provide IEEE 802.3 media access. The board's RAM is divided into three banks. One dual ported memory bank is shared with the CPU and the host, and one is shared between the CPU and the Ethernet module. The remaining RAM is reserved for local memory for the VNSD CPU module. Each of the modules is logically separated and can only be accessed through the appropriate modules. [Ref. 27]

The software for the VNSD was developed by VERDIX and is stored as firmware on its board. The firmware executes all of the VNSD's functions, including enforcing security policy, transmitting and receiving data, auditing, encrypting, and initializing. [Ref. 27]

2. Communication Protocols

The VSLAN operates at the physical and data link layers of the Open Systems Interconnection (OSI)- Basic Reference Model. VSLAN utilizes the IEEE 802.3 protocols to handle the physical layer and a portion of the data link layer. The VERDIX implementation differs from the IEEE standard in one respect; the IEEE standard defines a two-byte length field, which indicates the length of the datagram. VERDIX uses this field to identify the source VNSD ID or principal ID (depending on whether a data or control association has been established). A specific length indicator is not included in the datagram. Instead, the receiving VNSD determines the end of the datagram by the quiescence of the line. It strips off the last 32 bits of the received message for comparison, and is able to determine the end of the data field. The "CSMA/CD Access Method and Physical Layer Specification," IEEE 802.3, does not require acknowledgement transmissions to indicate that datagrams have been received. [Ref. 27]

The protocols residing at VSLAN data link layer include the IEEE 802.3 Media Access Control protocol, an encryption protocol, and a logical link protocol. Except for the length of the data field, VSLAN Media access protocol conforms to the IEEE standard. Because of the need for reliable communication between the VNSC and the VNSD, the VSLAN protocol suite includes a logical link control protocol. This protocol provides a reliable data transfer service for network control datagrams only. This is accomplished by specifying separate data and acknowledgement datagrams. The receiver accepts only datagrams in sequence and generates acknowledgements that identify the received datagrams by sequence number. Packets prepared by the logical link protocol are treated as data by the encryption protocol. The Data Encryption Standard (DES), described in Chapter II, is primarily used as a data integrity mechanism, instead of a mechanism to control security policy. [Ref. 27]

The VSLAN operates transparently to higher layer protocols (e.g., X.25) implemented on hosts. Because of its independence from these upper layer protocols the VSLAN system can be used to integrate a variety of host systems. Even though the VSLAN can support communications between different host systems, host systems must implement compatible upper layer protocols suites to be able to communicate with one another. [Ref. 27]

C. SUMMARY

The above information provides a brief overall description of two commercial products that have met formal DoD evaluation criteria. The XENIX operating system provides MLS for the host while the VERDIX Secure LAN provides for the security and proper routing of information across the LAN medium. An overall view of the system can be seen in Figure 7.

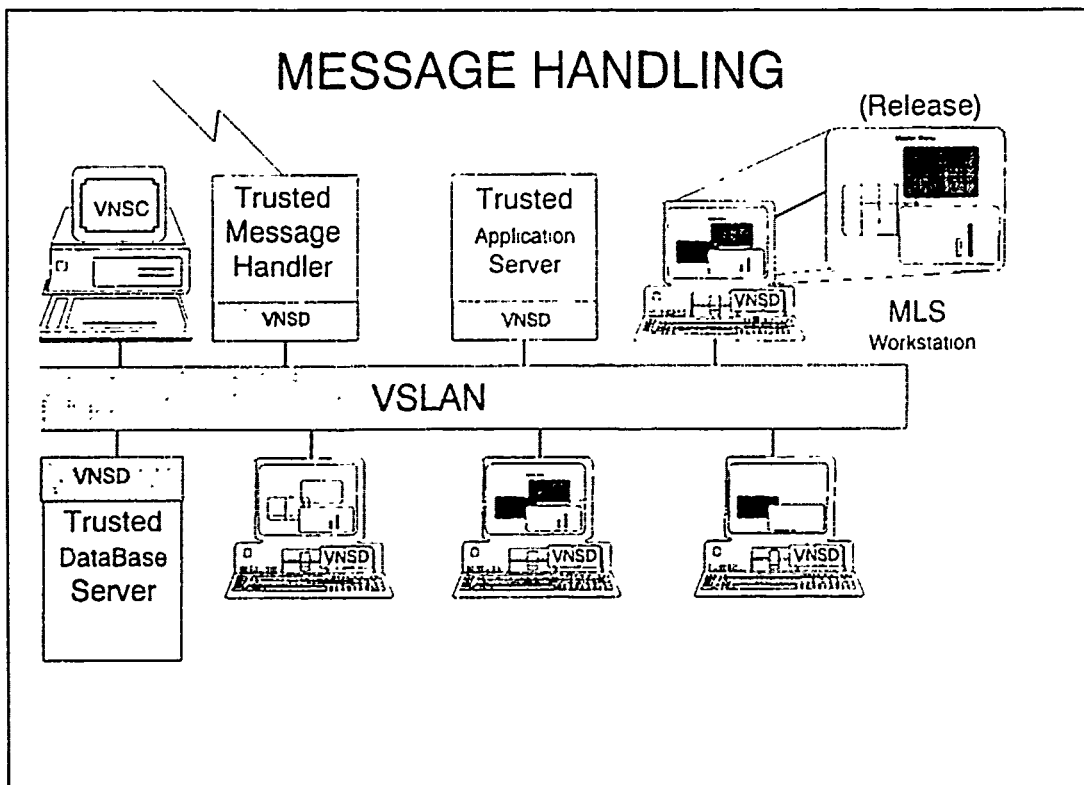


Figure 7 Example of VERDIX secure local area network

VI. A MULTILEVEL SECURE SHIPBOARD LAN PROPOSAL

The purpose of this chapter is to present a hypothetical multilevel secure shipboard LAN installation using the MMS, the MDS, the XENIX Trusted Operating System and the VERDIX Secure Local Area Network, described in the previous chapters. The hypothetical LAN will be based on the requirements of a medium-sized ship; a generic destroyer and/or cruiser scenario will be developed. By generic the author is implying a general description of node location and desired classification processing capabilities. Specific ships will differ due to their ADP assets (number and type of computers) and command prerogative of how certain administrative processes will function (e.g., what nodes can process Secret and below as opposed to Confidential and below). The generic ship description is developed from the author's eight years of shipboard experience on four different ship classes which include one Frigate, one Destroyer, and two Guided Missile Cruisers.

A. SHIPBOARD LOCAL AREA NETWORK OVERVIEW

The primary purpose of the hypothetical LAN is to provide the capability of processing various classified organizational messages between the Main Communications Center, hereafter referred to as Radio Central, and various nodes throughout the ship. The ultimate goal is the termination of message paper reproduction for the internal distribution of AUTODIN messages throughout the ship (which parallels a goal of the DMS with the NTCC and its OTC subscribers). The secondary goal is to provide a medium to replace the paper-based Secret information account. Chapter One discussed the potential use of CD-ROM techniques in distributing tactical information. The LAN should be designed for future upgrades to incorporate this type of features as they become more readily available. The tertiary goal is to provide the foundation for an Office Automation System allowing for various levels of security that will conform to Privacy Act requirements. An example would be the generation of personnel evaluations

and subsequent processing, including reviewing and final approval, all conducted on the multilevel secure LAN.

1. Specific Required Attributes

Specific attributes for the hypothetical LAN are somewhat parallel to those of the MMS, described in Chapter IV, and include:

- Provide connectivity between NAVMACS, GateGuard, VNSC, and LAN nodes
- Provide message separation by classification
- Eliminate manual outgoing processing and incoming distribution of Unclassified to Secret AUTODIN messages.

2. Functional System Description

The following is a system description of the hypothetical LAN which includes assumptions concerning connectivity and compatibility of application programs. These will be highlighted as discussed. The hypothetical LAN is based on systems which have been described in the previous chapters. The intent is to draw upon existing developments and relate them to indicate that a multilevel shipboard secure LAN is feasible.

a. Communications Suite and Interfaces

The communications suite of the ship is assumed to be the NAVMACS V3 variant. The NAVMACS software will be modified to send all addressed messages to both PR1 and TP2. A BIU or BIC is installed to connect NAVMACS to GateGuard. GateGuard has a communications port with STU-III access to receive messages from the servicing NTCC while the ship is in port. GateGuard is installed in the Radio Central which is either manned or physically locked and alarmed. The NAVMACS interface simply allows incoming messages to be transferred to GateGuard in their DoD predefined format (JANAP 128 or modified ACP 126).

b. GateGuard, MMS, and LAN Interfaces

GateGuard will be interfaced to a shipboard MMS. A method of emulating a STU-III connection of the highest security level will have to be developed. This will allow the MMS to accept Unclassified to Secret message traffic from the GateGuard during the same transfer. Otherwise, a GateGuard capable of separating message traffic by classification will be required. Three ports would carry the associated classified traffic. Essentially the GateGuard would emulate the NTCC's LDMX connection to the MMS.

A MDS system will be required upstream of the MMS to interrupt the message and determine to which shipboard subscriber mailboxes the messages should be posted. The MMS at the NTCC is able to read the DoD format of the message which includes the Plain Language Addressee and associated Routing Indicator which every Navy command is assigned. This is how a subscriber account is identified at the NTCC. At the shipboard level an application interface will be required to read the message and determine which shipboard subscribers should receive the message. A shipboard subscriber will have to be defined as an individual node or an organizational title position within the command, such as Commanding Officer or Executive Officer. The application program would modify or append a local shipboard RI to the message that the MMS would recognize. Another option is to simply post all messages of the same classification to one subscriber account and then allow authorized nodes access to the files within the account. The MMS would then append the E-mail header to the DoD formatted message and post it to a subscriber's mailbox as it is currently programmed to do at the NTCC. A MDS system would then poll each subscriber mailbox and generate a message summary profile allowing subscribers to review critical information about messages posted to their respective mailbox accounts or all messages contained in a designated classification mailbox. The MMS would then be fitted with a VNSD on three communication ports connected to the shipboard LAN (one each for Unclassified, Confidential, and Secret).

Another option is a single communication port with one VNSD since the VNSC can program communication authorization between various VNSDs. The VNSD would be equivalent to the

STU-III and SACS, being programmed with transmit windows for each node and providing encryption capability the STU-III provides. The VNSC would be installed in the Radio Central and the NSO would program the required transmit and receive windows for each node. Another way of describing the author's proposal is that the MMS would function as a file server for the LAN. Files and messages with the E-mail header (the E-mail header would not be required to be stripped off as it is in the MMS NTCC configuration) would be posted in mailbox accounts, and if a node is authorized to communicate with the mailbox a file transfer or E-mail transfer could take place.

A MDSUIP would be incorporated to provide the capability for viewing messages selected from the message summary profile. The file will be read to the user workstation memory for viewing. If the user desires a copy of the message a file transfer will be required. Assuming the VNSC and VNSD are installed and programmed, an authorized file transfer will take place and the responsibility for providing multilevel security at the workstation will be transferred to the XENIX trusted operating system. This assumes the MDSUIP is compatible with the VERDIX and XENIX software.

3. Nodes

The hypothetical LAN will consist of the following nodes, generic location, and security classification processing requirements:

1. Commanding Officer's In Port Cabin - located in the Commanding Officer's in port cabin, required to process Secret and below.
2. Executives Officer's stateroom - located in the Executive Officer's stateroom, required to process Secret and below.
3. Administrative Office - located in the Administrative Office, required to process Secret and below.
4. Personnel Office - located in the Personnel Office, required to process Confidential and below.
5. Supply Departmental Office - located in the Supply Departmental office, two workstations may be active, required to process Confidential and below.
6. Combat Systems Departmental Office - located in the Combat Systems Departmental Office, required to process Secret and below.

7. Operations' Departmental Office - located in the Operations' Departmental Office, required to process Secret and below.
8. Engineering Departmental Office - located in the Engineering Log Room, required to process Confidential and below.
9. Command Master Chief's Office - located in the Command Master Chief Office, required to process Confidential and below.
10. 3M Coordinator's/Ship's Maintenance Officer Office - located in the designated office space, required to process Confidential and below.
11. Electronic Repair Shop - located in the Electronic Technicians' workspace, required to process Confidential and below.
12. Main Communications Center (Radio Central) - located in Radio Central, required to process Secret and below.
13. Combat Information Center (Three separate workstations) - located in CIC, required to process Secret and below.
14. Pilot House - located in the Pilot House, required to process Secret and below.
15. Various Officer staterooms - located throughout the ship, required to process Confidential and below.
16. Various administrative offices - offices that certain ship configurations will allow depending on space and command priority, examples include a Command Career Counselor office and an Educational Services Officer office. Additionally these offices may coexist with an existing office but require a separate node, an example would be the Command Career Counselor and Command Master Chief sharing an office space but having two separate nodes within the same space.

4. Assumptions

The author has made certain assumptions in the theoretical LAN which include:

- The topology and transmission medium, coaxial cable or optical fiber, are physical characteristics that support the LAN. Specific discussion and requirements have been intentionally omitted, assuming that they will not limit the operation of the applications.
- Application processes described in the previous chapters will be compatible or be made compatible with relatively easy effort.
- The MMS will act as the file server for the organization's messages. Other processes and applications may be required to be installed to provide separate functions for the LAN. The author has assumed the MMS has the capability to do this.
- Database management programs are available and compatible with the XENIX trusted operating system.

5. Application Scenarios

The following scenarios are provided to assist in understanding the application processes the author has described.

a. Scenario One : Secret Message

A Secret message scenario is described below.

1. A Secret general service message is addressed to USS ONE and transmitted over the fleet broadcast while the ship is underway. The NAVMACS V3 determines the message is addressed to its ship from the user entered Command Guard List. The subject of the message is "Electronic Warfare Alert." The message is received by NAVMACS and is downloaded to GateGuard through the BIU.
2. GateGuard transfers the message to MMS through the STU-III emulation connection. The MMS retrieves the message, appends the E-mail header for internal processing, and posts the message to the command's Secret subscriber mailbox account.
3. The MDS polls the Secret mailbox account and recognizes the new message. Specific format fields are written to the message summary profile. The command's message summary profile is transmitted to all nodes on the LAN. (The frequency of transmitting updated message summary profiles will be input by the command system administrator.)
4. The Commanding Officer logs on to his PC in his stateroom. He inserts his PID into his node's VNSD which identifies him as the Commanding Officer and his associated pre-programmed transmit and receive windows. He reviews the message summary profile and desires to review the scenario's message. THE MDSUIP requests the message be read to the Commanding Officer's node memory. The VNSD on the MMS recognizes that the transmit and receive windows are allowed for the Secret classification and the message with the E-mail header appended is read into the memory of the CO's computer. (The author has suggested leaving the E-mail header appended to allow for the feasibility of utilizing the E-mail application program which may make it easier for application program compatibility.) The CO reviews the message and desires a permanent copy of the message. He now initiates a file transfer of the message. Again the VNSDs recognize that the communication process is authorized and a file transfer is conducted. Once the file is received the Xenix operating system recognizes the message classification and files the message in an appropriately protected area of the computer memory through the implemented data base management system.

b. Scenario Two: Command Mandated Special Category Message

The purpose of this scenario is to demonstrate the flexibility the proposed system could offer. This scenario is predicated on the author's experience that individual Navy commands desire to internally route certain Unclassified messages in accordance with the Commanding and Executive Officers' prerogative.

1. An Unclassified general message, without any Navy standard special handling instructions is received by USS ONE. The ship is in port and the message was transferred to the ship's GateGuard by the servicing area NTCC's MMS. The contents of the message include social security numbers of personnel who tested positive for substance abuse from the command's most recent random urinalysis. The Executive Officer has mandated that this type of message will only be delivered to his MMS subscriber account due to previous incidents of unauthorized disclosure of similar message results.

2. The MDS system recognizes the message by contents and subject line. The MDS interacts with the MMS to post the message to the Executive Officer's individual subscriber account. Another option is to utilize a manual MMS operator to screen all received messages and post them to appropriate subscriber accounts.

3. The MDS later polls the Executive Officer's MMS subscriber account and generates a message summary profile. The Executive Officer now has a unique message summary account and recognizes that he wants his own file copy of this message.

4. He inserts his PID into his node's VNSD and establishes a link with the MMS's VNSD. Both VNSDs recognize that transmission and receipt windows have been authorized and the requested file transfer takes place.

c. Scenario Three: All Navy Message

This scenario describes the routing of a message addressed to all Navy commands, commonly known as an ALNAV. Additionally, a MDS interface will be assumed not to exist. As mentioned in the previous example a manual MMS operator will be employed. Although this scenario does not eliminate human intervention in internal message routing procedures, it does offer an extreme reduction in the number of personnel required to disseminate paper message traffic. This scenario provides the possibility of an interim solution to a shipboard multilevel secure LAN while a MDS/MMS interface is developed.

1. An Unclassified ALNAV message is received by USS ONE while underway. The NAVMACS V3 is monitoring the fleet broadcast and determines that the message should be received by the ship. NAVMACS downloads the ALNAV message to GateGuard.

2. An MMS operator polls GateGuard for recently received messages. The GateGuard transfers the ALNAV to the MMS where the message is posted awaiting operator intervention to program specific subscriber accounts to which the message should be posted. The MMS operator reviews the message and based on written routing guidance determines the message should be delivered to all individual subscriber accounts.

3. As individuals logon to their nodes through out the day they insert their PIDs and establish communications with the MMS's VNSD. Again transmit and receive windows are recognized and the individual subscriber accounts are downloaded to their respective nodes. (Measures would be

required to prevent one node from downloading a large account and subsequently preventing other users from utilizing the network.)

d. Scenario Four: Personnel Evaluations

This scenario describes the use of VSLAN without reference to a NAVMACS communication interface. Its purpose is to show a feature of VSLAN multilevel security feature that is not communications related, but requires multilevel security characteristics. The mandatory access control policy that VSLAN employs mediates access between defined subjects and datagrams. Each datagram has a unique sensitivity label associated with it indicating its security level. [Ref. 27] "A security level is defined as the combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information. The VSLAN supports up to 16 classifications and 64 categories." [Ref. 27]

This means the network can be used for much more than providing a communication medium for the three classifications of messages that NAVMACS would be authorized to download to GateGuard. Administrative information could easily be classified and categorized as required or desired by an individual ship. Evaluations are a prime example.

1. The regular annual evaluation reporting date for First Class Petty Officers is approaching and the Executive Officer desires all draft evaluations to be submitted to his node for review and editing. Certain nodes throughout the ship are programmed with transmit and receive windows corresponding to the command's desired security and sensitivity policy. In this case the Executive Officer has informed the NSO that he desires only departmental office nodes to communicate with him regarding the subjects' evaluations.
2. A Chief Petty Officer drafts a evaluation on the appropriate departmental node and it is reviewed by the departmental chain of command. Once the Department Head approves the evaluation he transmits it on VSLAN to the Executive Officer's node. This assumes compatibility between the application program for drafting the evaluation, the node's multilevel secure operating system, and the VSLAN operating system.
3. The Executive Officer reviews all the First Class Petty Officers' evaluations and sends them to the Personnel Office for printing. (This scenario does not discuss factors of how the Executive Officer completes his review. It only shows how the VSLAN can be used to automate the evaluation process ensuring privacy of all individuals concerned.)

An overview of two options of the author's proposed LAN is shown in Figure 8.

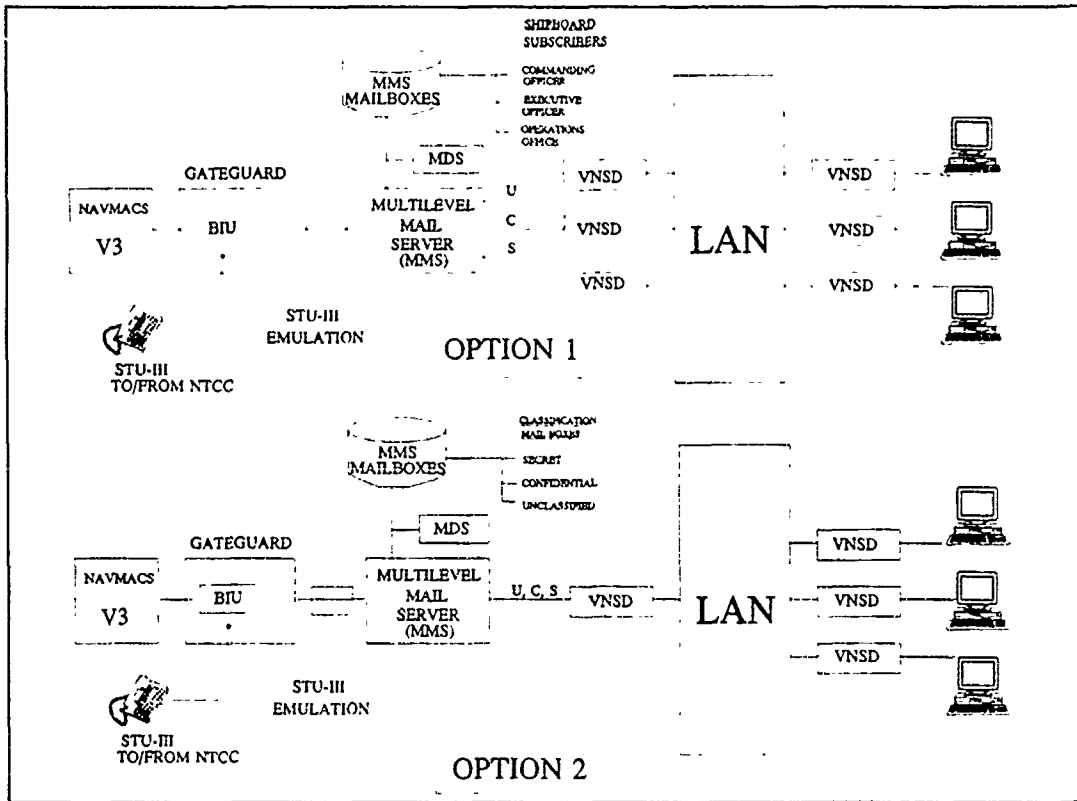


Figure 8 Two options for a MMS, NAVMACS and LAN interface

B. COST INFORMATION

Although the author has not discovered a similar government system to which to compare costs, cost information is available on selected components of the hypothetical LAN and are summarized below. It should be noted that the node description previously provided is the basis for total costing. Although various nodes were listed under several headings the author will assume that 16 nodes are required.

- Complete Trusted XENIX System [Ref. 28]
 (16 at \$3,995) \$63,920
- VNSC [Ref. 29](hardware & software, \$17,500

- VNSD [Ref. 29]
(16 at \$4,250) \$68,000
- GateGuard System [Ref. 23: Appendix C] \$3,350
- 3B2/600G AT&T Computer (Non-Tempest) [Ref. 23: Appendix C] \$3,354
- MMS 300MB Non-removable disk (Non-Tempest) [Ref. 23: Appendix C] \$4,620
- MMS 550MB Removable disk storage (Tempest) [Ref. 23: Appendix C] \$7,000
- MMS Complete software [Ref. 23: Appendix C] \$5,190
- Miscellaneous (e.g., Cables, STU-III SACS) \$50,000
- Total \$222,934

The author considers the above cost factors to be liberal, meaning actual cost will likely be greater. Regardless it does provide insight and leads the author to conclude that the cost of installing a shipboard multilevel secure LAN is practical, and further investigation should be pursued.

VII. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The results of this study indicate a shipboard multilevel secure local area network is feasible. The Navy initiatives with the DMS are considered to be a primary contributing factor to the developmental process required to implement a shipboard MLS LAN. The key parallel factor between the Navy DMS initiatives and the shipboard MLS LAN is the implementation of the MMS at NTCCs. The capability to segregate messages by classification and then distribute them to authorized subscribers is what has been developed for the NTCCs' operations. This is the exact requirement needed on ships. The system should be able to be modified to accommodate the requirements of a LAN. Additionally, the required connectivity for the data source of ship messages, the fleet broadcast, is available. Syncrotech Corporation established that various NAVMACS variants could be connected to GateGuard. Operating systems for the LAN and node computers are commercially available and properly certified by DoD standards.

The Navy initiatives with DMS have focused on easing the message processing capabilities at shore commands. The MMS was designed to serve the NTCCs and the MDS was designed to support Naval shore commands and their associated LANs. The purpose of the NTS system is to get messages to fleet units, yet under the DMS initiatives, no fleet unit has been incorporated into research development. The NAVMACS/GateGuard connectivity solution has not been pursued beyond the Syncrotech Corporation report. NAVMACS II is considered to be the future answer to an LAN interface yet a MLS LAN has not been addressed. NAVCOMPARS is not even considered in the Navy DMS plan, other than a statement that it warrants future consideration. LAN installations on the GEORGE WASHINGTON and YELLOWSTONE were initiated by the individual ships. One must

conclude that the DMS initiatives may benefit shipboard application requirements and an avenue for mutual pursuit should be established.

B. RECOMMENDATIONS

The ability of the MMS to be installed on a ship and act as a file server for the LAN should be further investigated. This will require coordination within OP-094. The command responsible for implementing DMS within the Navy and the command which conducted the study for Commercial Fiber Optic LANS For Naval Ships [Ref. 14] are both under the cognizance of OP-094. This thesis shows that mutual coordination would be beneficial.

The VERDIX Secure LAN and Trusted Information Systems' XENIX trusted operating system should be considered for shipboard use. Their NCSC B1 certification should facilitate rapid implementation if application software is or can be made compatible.

The GateGuard/NAVMACS interface should be implemented regardless of the status of NAVMACS II acquisition. If the NAVMACS V3 and Gateguard can be connected and a multilevel secure LAN installed on a medium-size ship, the lessons learned could be applied to larger ships. It seems sensible to start on a small scale and work upwards; for example, evaluate the LAN on a destroyer and then on an aircraft carrier.

The message center integration is not the only requirement for a multilevel secure LAN. Electronic libraries are rapidly approaching, and integration will be required. Investigation of the MMS to connect to CD-ROM should be conducted to facilitate implementation of these libraries.

The ships of the Navy should not be the last entities within the Navy to take advantage that a LAN offers. The NTS system is designed to get messages to the fleet - - the end user of the information. The officers and crews of the ships should not be left to wade through a paper-based information system.

APPENDIX A

SUMMARY OF EVALUATION CRITERIA CLASSES

The classes of systems recognized under the trusted computer systems evaluation criteria are as follows. They are presented in the order of increasing desirability from a computer security point of view. [SOURCE: Department of Defense "Trusted Computer System Evaluation Criteria," DoD 5200.28-STD, December 1985, Appendix C, pp. 93-94.]

Class (D): Minimal Protection

This class is reserved for those systems that have been evaluated but that fail to meet the requirements of a higher evaluation class.

Class (C1): Discretionary Security Protection

The Trusted Computing Base (TCB) of a class (C1) system nominally satisfies the discretionary security requirements by providing separation of users and data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis, i.e., ostensibly suitable for allowing users to be able to protect project or private information and to keep other users from accidentally reading or destroying their data. The class (C1) environment is expected to be one of cooperating users processing data at the same level(s) of sensitivity.

Class (C2): Controlled Access Protection

Systems in this class enforce a more finely grained discretionary access control than (C1) systems, making users individually accountable for their actions through login procedures, auditing of security relevant events, and resource isolation.

Class (B1): Labeled Security Protection

Class (B1) systems require all the features required for class (C2). In addition, an informal statement of the security policy model, data labeling, and mandatory access control over named subjects and objects must be present. The capability must exist for accurately labeling exported information. Any flaws identified by testing must be removed.

Class (B2): Structured Protection

In class (B2) systems, the TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in class (B1) systems to be extended to all subjects and objects in the ADP system. In addition, covert channels are addressed. The TCB must be carefully structured into protection-critical and non-protection-critical elements. The TCB interface is well-defined, and the TCB design and implementation enable it to be subjected to more thorough testing and more complex review. Authentication mechanisms are strengthened, trusted facility management is provided in the form of support for system administrator and operator functions, and stringent configuration management controls are imposed. The system is relatively resistant to penetration.

Class (B3): Security Domains

The class (B3) TCB must satisfy the reference monitor requirements that it mediate all accesses of subjects to objects, be tamper-proof, and be small enough to be subjected to analysis and tests. To this end, the TCB is structured to exclude code not essential to security policy enforcement, with significant system engineering during TCB design and implementation directed toward minimizing its complexity. A security administrator is supported, audit mechanisms are expanded to signal security-relevant events, and system recovery procedures are required. The system is highly resistant to penetration.

Class (A1): Verified Design

Systems in class (A1) are functionally equivalent to those in class (B3) in that no additional architectural features or policy requirements are added. The distinguishing feature of systems in this class is the analysis derived from formal design specification and verification techniques and the resulting high degree of assurance that the TCB is correctly implemented. This assurance is developmental in nature, starting with a formal model of the security policy and a formal top-level specification (FTLS) of the design. In keeping with extensive design and development analysis of the TCB required of systems in class (A1), more stringent configuration management is required and procedures are established for securely distributing the system to sites. A system security administrator is supported.

LIST OF REFERENCES

1. USS GEORGE WASHINGTON (CVN-73), UNCLASSIFIED Letter Ser 03/00239, with enclosures, to Chief of Naval Operations (OP 55). Subject: Request for funding of GEORGE WASHINGTON'S Information System (GWIS), 26 February 1991.
2. Williams, L.G., Commander, US Navy, "Fiber Optic Local Area Networks For Naval Ships," paper presented to Professor E.M. Long, George Mason University, Fairfax, Virginia, 25 April 1991.
3. Wheeler C.E., Mallon P.J., and Shotwell, H.L., SNAP-II A Post Implementation Review of User Concerns on Selected Ships, Master's Thesis, Naval Postgraduate School, Monterey, California, March 1986.
4. Schneidewind, N.F., "Proposed Technology and Procurement Policy for SNAP III." Report prepared for Naval Sea Systems Command, Naval Postgraduate School, October 1986.
5. Hamblen, D., "The LAN Solution," CHIPS, p.27, July 1991.
6. Giauque, M.S., "The Loop for Tactics," Surface Warfare, pp.2-5. November/December 1991.
7. Stallings, W., Local Networks: An Introduction, p. 336, Macmillan Publishing Co., 1984.
8. Shirey, R. W., "Security in Local Area Networks," Proceedings, IEEE Computer Networking Symposium, IEEE Computer Society Press, December 1982.
9. Fitzgerald, J., Business Data Communications : Basic Concepts, Security, and Design Third Edition, p.496, John Wiley & Sons, Inc., 1990.
10. Graubart R.D., and Woodward P.L., "A Preliminary Naval Surveillance DBMS Security Model," Proceedings, IEEE Symposium on Security and Privacy, IEEE Computer Society Press, April 1982.
11. Varadharajan, V., "A Multilevel Security Policy Model for Networks," Proceedings, Ninth Annual Joint Conference of the IEEE Computer and Communications Societies, The Multiple Facets of Integration, IEEE Computer Society Press, June 1990.
12. Sidu, Deepinder P., and Gasser, Morrie, "A Multilevel Secure Local Area Network." Proceedings, IEEE Symposium on Security and Privacy, IEEE Computer Security Press, April 1982.
13. Computers at Risk: Safe Computing in the Information Age. System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, p.133., National Academy Press, 1991.
14. Director, Space, Command and Control (OP-O94), "OP-O94 Study: Commercial Fiber Optic LANS for Naval Ships (DRAFT Version)," p. 11., 22 April 1991.
15. Defense Intelligence Agency, Communications Handbook for Intelligence Planners (U), p. 4-16, 1986.

16. Commander, Naval Telecommunications Command, Naval Telecommunications Procedures, Fleet Communications (NTP-4C), June 1988.
17. Syncrotech Software Corporation, "GateGuard/NAVMACS Analysis Report, Contract Nr. N00039-89-C-0082, Task Nr. 20, Memorandum Nr. 002," 26 April 1991.
18. Rogers, C., Naval Computer and Telecommunications Station, Washington. Code N912, Defense Data Network E-Mail to the author, 28 OCT 91.
19. Shelton, Deborah J., An Overview of the Naval Telecommunications System, Master's Thesis, Naval Postgraduate School, Monterey, California, March 1990.
20. Rogers C., Naval Computer and Telecommunications Station, Washington. Code N912, Defense Data Network E-Mail to the author, 6 October 1991.
21. Defense Communication Engineering Center, "DMS Management System Requirements Document (U)," prepared by AT&T/Harris, p. 1-1. Contract No. DCA100-88-C-0015, July 1990.
22. Naval Telecommunications Automation Support Center, Naval Communications Unit Washington, Cheltenham, Maryland. "Department of the Navy Defense Message System Transition Plan, Draft," p. 1-2, January 1991.
23. Naval Computer and Telecommunications Station, Washington, Naval Telecommunications Systems Development Directorate, Cheltenham, Maryland. "Functional Description: MULTILEVEL MAIL SERVER (MMS)," p. 2-3. NCTS Washington Document No. 15X1035 FD-01, May 1991.
24. Naval Telecommunications Automation Support Center, Cheltenham, Maryland. "Message Dissemination Subsystem: Functional Description," NAVTASC Cheltenham MD Document No. 15X0025A FD-01A, p. 3, June 1990.
25. Trusted Information Systems, "Trusted Application : Multilevel Secure Local Area Network," Product Description Advertisement, not dated.
26. Trusted Information Systems, Inc., Letter, with Enclosure, to the author 22 October 1991.
27. VERDIX Corporation, "VSLAN Secure Local Area Network: Product Overview," 8 January 1991.
28. Trusted XENIX Retail Price List, August 1, 1991.
29. Bowles, G.B., Verdix Corporation Secure Products Division Head, Facsimile to the author, 30 January 1992.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
Cameron Station
Alexandria, Virginia 22304-6145
2. Superintendent 2
Attn: Library, Code 52
Naval Postgraduate School
Monterey, California 93943-5000
3. Professor Norman F. Schneidewind 1
Code AS/Ss
Department of Administrative Sciences
Naval Postgraduate School
Monterey, California 93943
4. Professor Dan C. Boger 1
Code AS/Bo
Department of Administrative Sciences
Naval Postgraduate School
Monterey, California 93943
5. Mr. Charley Rogers 1
Code N912
Naval Computer and Telecommunications Station
Washington, DC
In Care Of:
Naval Communications Detachment
Cheltenham, Maryland 20397-5310
6. Mr. Art Justice 1
Code 41
Naval Ocean Systems Command
San Diego, California 92152-5000
7. LCDR John W. Riley III 1
6931 Yellow Bluff Road
Panama City, Florida 32404