Semaphore Network Encryption Report

MP 94B0000022
March 1994

Karen L. Johnson

Contract Sponsor CORE
Contract No. N/A
Project No. 028A
Dept. G022

MITRE
Bedford, Massachusetts

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 1994	

4. TITLE AND SUBTITLE

Semaphore Network Encryption Report

5. FUNDING NUMBERS

6. AUTHOR(S)

Karen L. Johnson

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

The MITRE Corporation
202 Burlington Road
Bedford, MA 01730-1420

8. PERFORMING ORGANIZATION REPORT NUMBER

MP 94B0000022

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

This paper documents the results of a preliminary assessment performed on the commercial off-the-shelf (COTS) Semaphore Communications Corporation (SCC) Network Security System (NSS). The Semaphore NSS is a family of products designed to address important network security concerns, such as network source address authentication and data privacy. The assessment was performed in the INFOSEC Core Integration Laboratory, and its scope was product usability focusing on interoperability and system performance in an existing operational network.

Included in this paper are preliminary findings. Fundamental features and functionality of the Semaphore NSS are identified, followed by details of the assessment, including test descriptions and results. A summary of test results and future plans are also included. These findings will be useful to those investigating the use of commercially available solutions to network authentication and data privacy.

14. SUBJECT TERMS

network security, data privacy

15. NUMBER OF PAGES

34

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Unlimited

ABSTRACT

This paper documents the results of a preliminary assessment performed on the commercial off-the-shelf (COTS) Semaphore Communications Corporation (SCC) Network Security System (NSS). The Semaphore NSS is a family of products designed to address important network security concerns, such as network source address authentication and data privacy. The assessment was performed in the INFOSEC Core Integration Laboratory, and its scope was product usability focusing on interoperability and system performance in an existing operational network.

Included in this paper are preliminary findings. Fundamental features and functionality of the Semaphore NSS are identified, followed by details of the assessment, including test descriptions and results. A summary of test results ard future plans are also included. These findings will be useful to those investigating the use of commercially available solutions to network authentication and data privacy.

ACKNOWLEDGMENTS

The author would like to thank Mandy Matthews, Harriet Goldman, Todd Wittbold, and Bill Conaway of The MITRE Corporation, and Paul Pieske, Howard Herbert, and Dave Thompson of SCC for their contributions to the successful implementation of this assessment and the development of this document.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

SECTION 1

INTRODUCTION

This report examines the NSS, a commercially available family of products designed to resolve important network security concerns. Fundamental features and functionality of the Semaphore NSS are identified, followed by details of assessment testing, including test descriptions and test results. A summary of test results and recommendations for future assessment is also presented.

1.1 BACKGROUND

Modern networks of distributed client-server architectures have contributed largely to the increased need for network security. Client-server architectures are extremely popular because they promote resource sharing among networked computer users. Relationships between users and services are defined such that commonly used services are easily accessible to a wide range of authorized users. This design, however, also increases the number of network access points available to intruders or other undesirables. Therefore, malicious attacks on the network such as network eavesdropping and computer address spoofing, are often simple to execute without detection. The large number of computer break-ins through client-server networks are convincing evidence that networked systems needs stronger protection against access by unauthorized sources. As a result, network security is a primary concern for modern computer networks.

Network security addresses the protection of computer information as it is sent across the network from one computer to another. For example, how to protect identification and authentication data (e.g., user IDs and passwords) exchanged between computers across the network is a recurring network security issue. Private and sensitive information traversing a network must be protected against unauthorized disclosure and/or modification as it travels between computers. The Semaphore NSS is one of a number of commercially available software and hardware products that have recently emerged as a potential solution to such network security problems.

SECTION 2

PRODUCT DESCRIPTION

The Semaphore NSS is a family of five products that includes four classes of Network Encryption Units (NEUs) and a Network Security Center (NSC). NEU classes include a personal computer encryption unit (NEU-PC) that protects an individual node, a work group encryption unit (NEU-WG) that can protect a group of up to fifteen nodes, a hub encryption unit (NEU-HB) that can protect a building or department of up to 180 nodes, and site encryption units (NEU-ST, NEU-RT) that can be placed at a router to protect all data leaving a geographic site. Each NEU contains a 32-bit Reduced Instruction Set Computer (RISC) processor and includes a datakey receptacle for NEU initialization. The NEU-PC, NEU-WG, and NEU-HB each contain two Attachment Unit Interfaces (AUIs) for connecting to Ethernet or ISO 8802.3 Local Area Networks (LAN). The NEU-ST supports serial V.35 network interfaces, whereas the NEU-RT supports IEEE 802.3. NEUs are connected to LANs between the network and the node(s) whose data it will protect. Nodes are defined as devices connected to the LAN such as workstations, PCs, and printers.

An example configuration of the NEU-WG[1] unit is shown in Figure 1. The figure illustrates how the work group unit may be networked to protect multiple nodes and indicates NSS simultaneous support for multiple protocols.

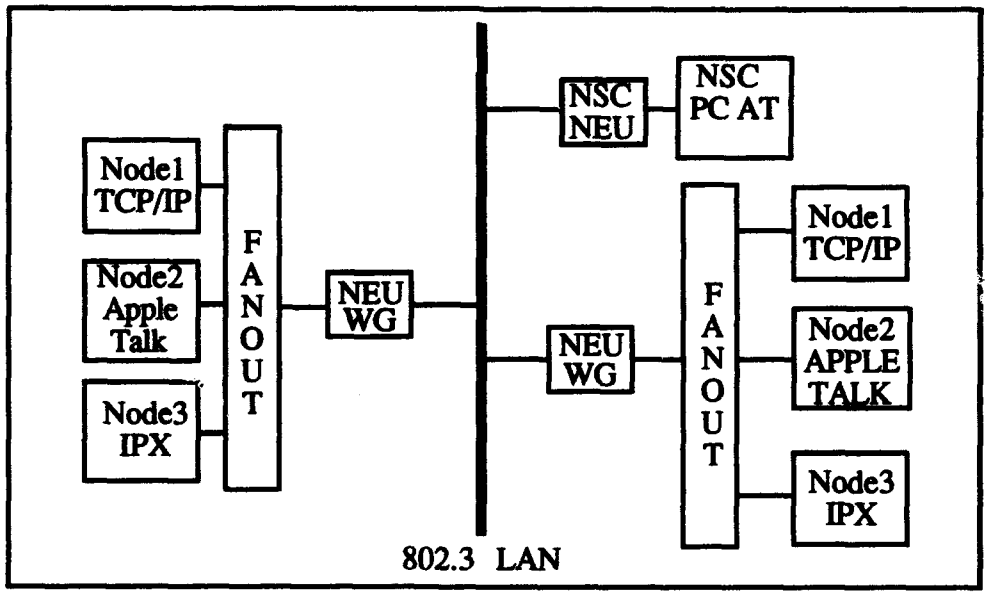

Figure 1. NEU-WG Network Configuration

[1] This report is based on an assessment of the NEU-WG unit, as it was the only unit available for testing at the time of this writing.

2.1 NETWORK SECURITY CENTER

The NSC provides a centralized access control database and a distributed certification mechanism used for authenticating interaction between NEUs. The NSC is required for NEU initialization, key management, network auditing, and managing network access.

The NSC hardware is an IBM PC/AT or compatible, and the NSC application software runs on Version 2.0 of the OS/2 operating system. Minimum hardware requirements for NSC operation includes a 33 MHz clock, 16 MB of RAM, 200 MB of hard disk, a 3.5-inch floppy drive, a Super Video Graphics Adaptor (SGVA) color monitor, a parallel port for a printer, and a serial port to connect the datakey loader. The units are shipped with six blank datakeys.

The datakey loader is used for programming or loading NSC and NEU access datakeys. NSC access keys (NAKs) are programmed during NSC software installation to provide authenticated access to the NSC application software. Three types of NEU access keys may be loaded after NSC configuration is completed. NEU initialization keys (INKs) are required to establish authentication of each NEU to the NSC prior to NEU network communication. Configuration of either of the other two NEU access keys, the cypto ignition key (CIK) and the front panel key (FPK) is required. The configuration and the use of optional keys is described later in the section entitled NEU Operational Modes.

2.1.1 NSS Configuration

All NSS configuration is performed at the NSC. The OS/2 operating system provides a user friendly graphical interface for configuring the secure network. Access control information for each NEU must be configured; data is entered to identify the NSC, NEUs on the network, nodes to be protected, the level of security protection for each node, NEU communities of interest, protocols to interpret, and NEU access keys to be created. One NEU must be configured as the "NSC NEU" and is dedicated for use by the NSC. An abbreviated pull-down map of the main NSC configuration menu is shown in Figure 2.

NSS configuration begins with the configuration of high-and low-level entities. High-level entities are network nodes such as workstations, printers, or servers that need cryptographic network protection and as such are designated protected network nodes (PNNs). The name and security protection level (i.e., encrypt, bypass) for each PNN is entered under the high-level *entities* menu command. The NSC and NEUs are also considered high-level entities. Low-level entities refer to protocols and addresses of PNNs. Information for these entities are entered under the low-level entities command menu. Mappings between high and low entities are subsequently established using the *relationships* menu. Individual entity and network summary reports can be generated from the *reports* menu and are useful for verifying the current configuration. The status of each NEU can be obtained via the *status* menu, and reports on audit events may be selected from the *audit trail* menu. The *other* command menu is used primarily to change the default system settings and to log out of the NSC application.

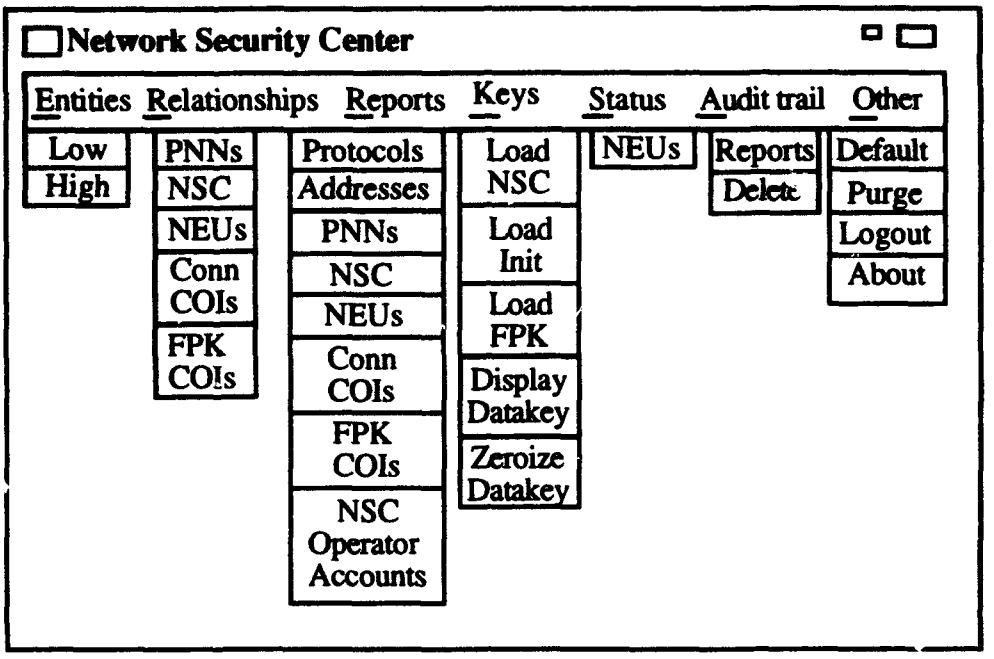

Figure 2. Network Security Center Configuration Menu

After configuration information is determined to be accurate, datakeys must be programmed for the NEUs. The *keys* menu is used for programming or loading datakeys. The first configuration datakey to load will be the NSC NEU initialization key. No other NEU initialization key may be loaded until the NSC NEU is initialized and online. Once the NSC NEU is initialized and operational, other NEU initialization keys may be programmed and other NEUs may be initialized.

2.2 NEU INITIALIZATION

Each NEU INK contains a Data Encryption Standard (DES) traffic encryption key (TEK) and network addressing information (NSC, NEU, and router addresses) required for network connectivity between the NEU and the NSC. An NEU must be physically attached to the network and capable of communicating with the NSC for initialization to successfully complete. NEU initialization is started by inserting, turning, and then removing its INK as prompted by the NEU display. During initialization, each NEU generates Rivest, Shamir, and Adleman (RSA) public and private keys and a unique RSA digital ID certificate.

A combination of RSA and DES cryptographic keying technology is employed at NEU initialization to implement security for the network. RSA cryptographic keys are used for network authentication and key distribution. All other network traffic is encrypted with DES TEKs. RSA encryption incorporates a central certification authority that validates ID certificates for use on the network; the NSC is the certifying authority for the NSS. Each

NEU-generated ID certificate contains its RSA public key and is validated by obtaining the RSA cryptographic signature of the NSC. The DES TEK on the NEU INK is used to secure the initial transport of the unsigned ID certificate from the NEU to the NSC for certification. The signed certificate is returned to the NEU authorizing it for secure communication with other NEUs. Key management and distribution is thereafter placed into each NEU. Successful completion of NEU initialization establishes "network authentication" and "automated and distributed key management" among NEUs. The steps for completing NEU initialization are illustrated in Figures 3, 4, and 5.

2.3 NETWORK AUTHENTICATION

Network authentication is described in Figure 3 by depicting the ID certification process. Figure 3 shows a single PNN NEU and the NSC NEU connected via a LAN. The PNN NEU ID certificate needs to be certified. Each NEU encrypts its RSA ID certificate with the DES traffic encryption key received from its INK. The encrypted ID certificate is sent across the network from the NEU to the NSC. The NSC decrypts the NEU ID certificate using the shared DES traffic encryption key and then, as the certifying authority, cryptographically signs the NEU ID certificate with its NSC RSA private key. The signed ID certificate is returned to the NEU. The NEU now has credentials for authenticated network communication to other NEUs.

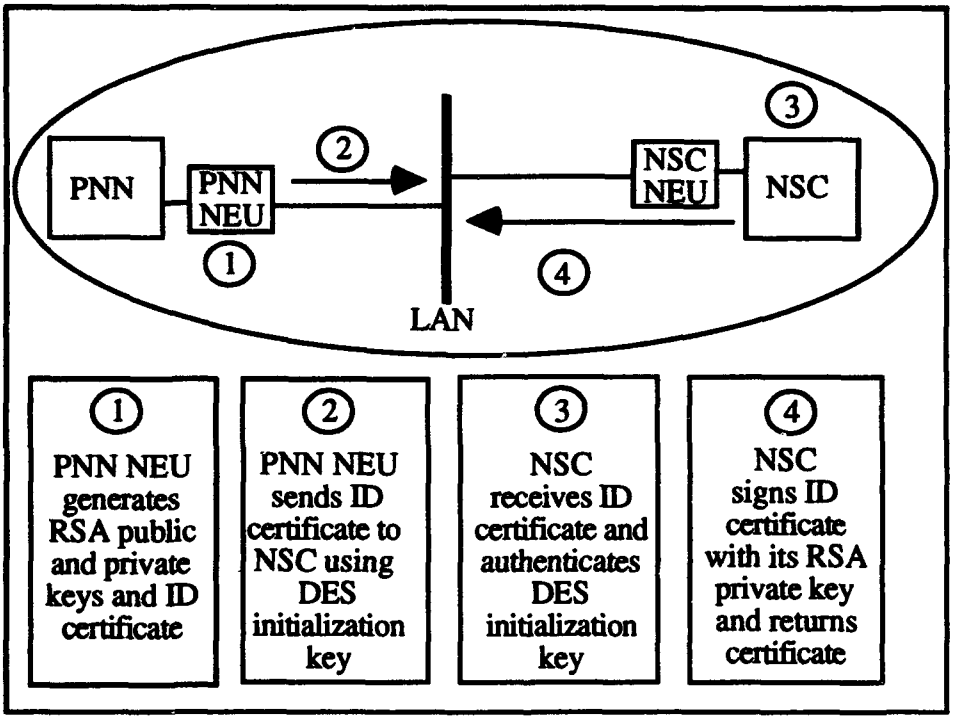

Figure 3. NEU Initialization: ID Certification Process

2.4 AUTOMATED AND DISTRIBUTED KEY MANAGEMENT

The NSC-certified ID certificate and the RSA keys generated by each NEU are used to automate and secure the distribution of DES TEKs between NEU pairs. Each NEU automatically negotiates and generates a DES TEK for each NEU with which it wishes to communicate. DES TEK distribution is negotiated between NEUs by an RSA cryptographic exchange of an NEU randomly generated check value. The RSA verified check value is used to authenticate the receipt of NEU-generated DES TEKs from the network.

After receiving its authenticated ID certificate (as shown in Figure 3), each NEU first negotiates with the NSC NEU to create a new DES traffic encryption key to be shared only between it and the NSC NEU. Negotiation for key distribution is indicated in Steps 5 through 10 of the NEU initialization process as illustrated in Figures 4 and 5.

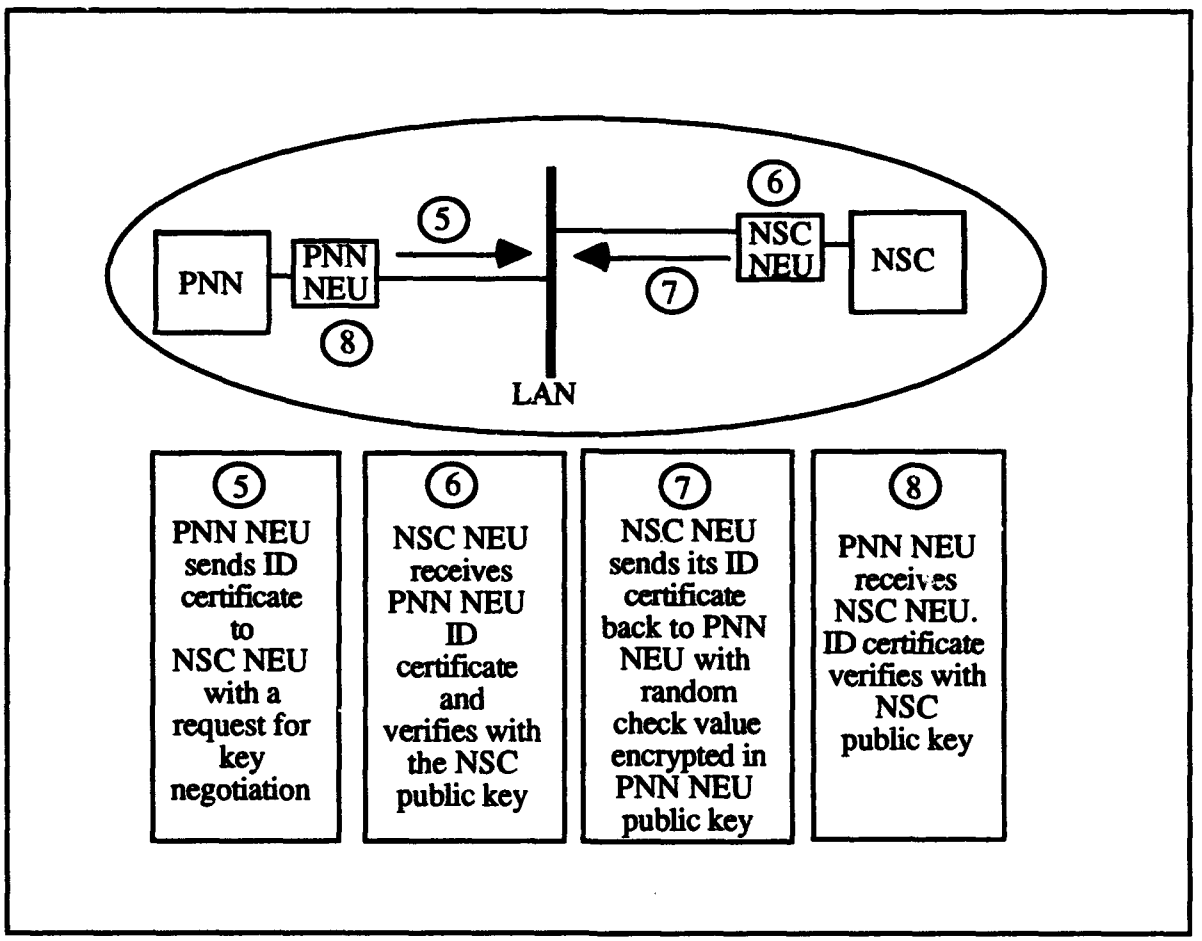

Figure 4. NEU Initialization: Request for Key Negotiation

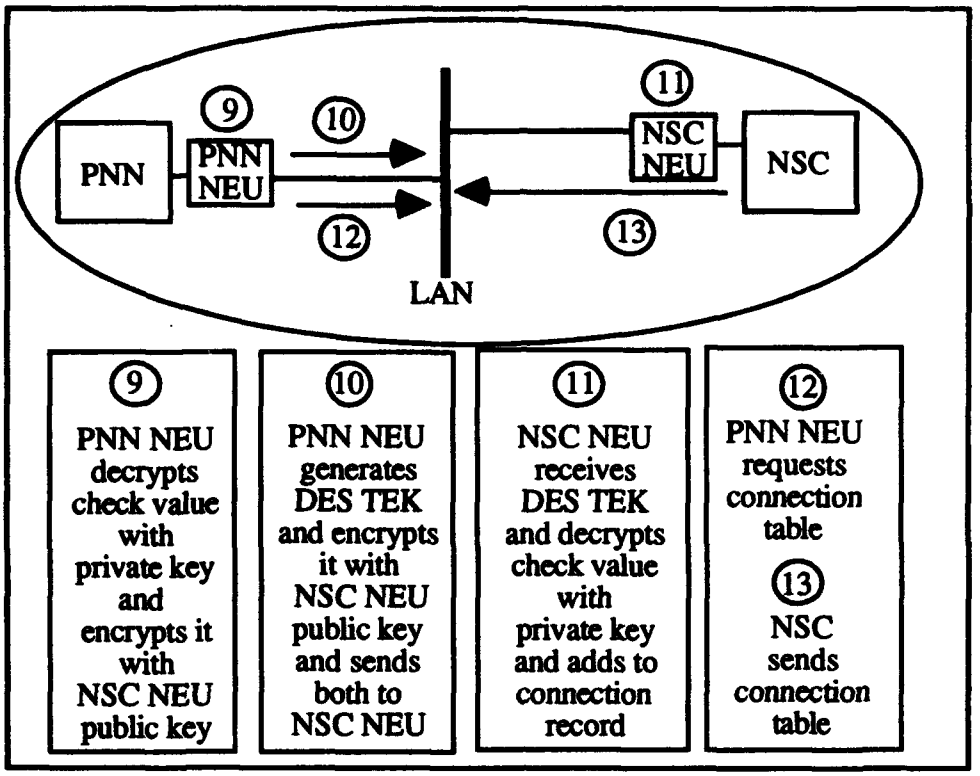

Figure 5. NEU Initialization: TEK Generation and Download of NEU Connection Table

In Figure 4, the NEU sends its ID certificate with a request for key negotiation to the NSC NEU. The NSC NEU verifies the NEU ID certificate and sends back its own ID certificate and a random check value encrypted in the NEU's public key. The NEU verifies the NSC NEU's ID certificate, decrypts the check value, reencrypts the check value in the NSC NEU's public key, creates a DES TEK also encrypted in the NSC NEU's public key, and sends the encrypted check value and DES TEK to the NSC NEU. After verifying the check value, the NSC NEU stores the DES TEK received in its "connection table."

NEU access controls are specified in connection tables generated by the NSC as part of NEU configuration. Connection tables contain NEU source and destination address pairs that tell each NEU with whom it is allowed to communicate. Initially, NEU connection tables reside only on the NSC. However, each NEU needs this information to establish independent key management and distribution. Because the connection table contains sensitive information, the download of the table from the NSC to the NEU must be secured. DES TEKs stored in the NSC NEU connection table are used to secure the download of the connection table from the NSC to the NEUs.

Once an NEU has its connection tables, it then negotiates the creation and transport of a DES TEK with each destination NEU identified in its table. Each NEU generates a DES

TEK to use for securing communication between destination NEUs configured in its connection table. Each DES TEK distributed to a destination NEU is stored in the receiving NEU's connection table until needed for encrypting or decrypting traffic between that NEU pair. Key management and distribution is automated as each NEU has the means to perform these functions both securely and independently.

2.5 NEU-TO-NEU ACCESS CONTROL

As previously discussed, each NEU determines with whom (other NEUs) it can communicate from access control information received in its connection table. The procedure for establishing secure communications between NEUs begins again with Step 5 as shown in Figures 4 and 5. To communicate with another NEU, a local NEU sends its ID certificate to that remote NEU. The remote NEU verifies the ID certificate using the central authority's (NSC) public key. The remote NEU then sends its ID certificate back along with a random check value encrypted in the local NEU's public key. The local NEU checks the authentication of the remote NEU's ID certificate using the NSC's public key. When the local NEU is satisfied that the remote NEU's certificate is authentic, it decrypts the check value received and reencrypts it using the remote NEU's public key. The local NEU then sends the remote NEU the encrypted check value and a newly generated DES traffic encryption key that it has also encrypted with the remote NEU's public key. Only the remote NEU will be able to retrieve the encrpyted DES key to use for decrypting traffic between the two NEUs. The remote NEU decrypts the check value and adds the DES TEK to the connection record for this NEU pair. Steps 5 thorough 13 are repeated for each destination address in each NEU's connection table. After completing DES TEK exchanges for all host in its connection table, the NEU waits for data to process.

All data entering the NEU through its node interface is subjected to access control checks performed by the NEU and is either encrypted, discarded, or passed through onto the network unencrypted. Likewise, data entering the NEU from the network is also checked and either decrypted, discarded, or passed out unmodified through the node interface. Access control checks, used to determine how data is handled, are based upon the assigned hosts' addresses and data transmission protocols configured in the NEU connection table.

2.6 HOST-TO-HOST DATA FLOW AND PROTOCOL SUPPORT

The NEU provides a reasonable amount of flexibility with regard to host system data link and network protocol support. The encryption/decryption of all valid data link layer ISO 8802.3 or Ethernet frames is supported. Network layer protocols recognized by the NEU include DOD IP, Novell IPX, and DECnet Phase IV; AppleTalk routing was not available at the time of testing but is now available. At the link level, all data above the layer two *type/length* field is encrypyted and decrypted in conformance with the IEEE-STD-802.10B frame structure and the DES Cipher Block Chaining (CBC) mode defined in ANSI-STD-X3.106. At layer three, all data above the layer-three header is encrypted using the DES CBC mode.

Network layer formats are modeled after IEEE-STD- 802.10B.[2] The NEU interprets protocol-type fields at both layers two and three. To encrypt at the network level, the NEU must be able to distinguish network protocols because data fields are different for different protocol types. The NEU modifies the type field of encrypted frames or datagrams based upon access control information contained in its configuration tables. The protocol-type fields in conjunction with internal configuration tables are used by the NEU to determine whether data should be encrypted, decrypted, bypassed, or discarded.

A heterogeneous network supporting multiple network protocols (IP, AppleTalk, and IPX) is depicted in Figure 6. Typical host-to-host data flows on this network diagram will occur between hosts supporting like (i.e., the same) protocols. For example, TCP/IP users exchange data across the network with other TCP/IP users, and AppleTalk users communicate across the network only with other AppleTalk users, etc. Each host connected to fanout A is configured as a PNN of NEU A. Likewise, each host connected to fanout B is configured as a PNN of NEU B.

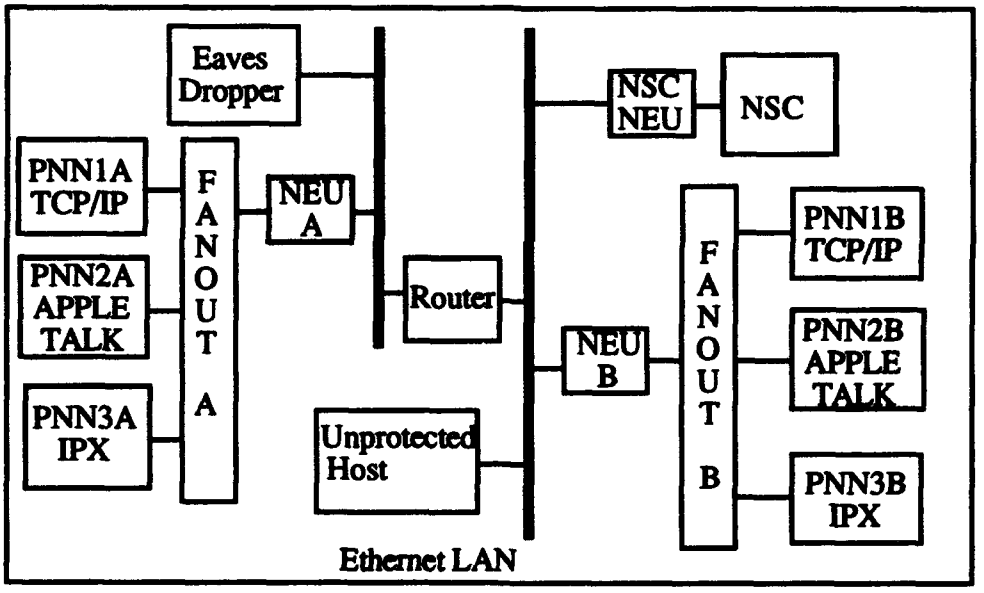

Figure 6. Network Data Encryption

2 Semaphore adds a security association ID and a management-defined field (MDF) to each encrypted data packet as indicated by the 802.10B specification.

3 Although this example illustrates encrypted packet transformation for a TCP/IP packet, IP packet transformation is the same regardless of the transport protocol type (i.e., TCP, UDP) identified in the IP packet header.

Suppose that the TCP/IP hosts (PNN1A and PNN1B) are required to exchange sensitive information across the network.[3] To prevent disclosure of this data to possible network eavesdroppers attached to the Ethernet LAN, it is desirable to encrypt all of the data that is passed between these two TCP/IP hosts. Because the NEU processes multiple protocols and different protection levels (i.e., encrypt, bypass), TCP/IP packets may be encrypted while all other traffic is simply passed through.

In Figure 6, all data leaving Fanout A must pass through NEU A to reach hosts connected to Fanout B. NEU A and NEU B have been configured to encrypt TCP/IP packets and to bypass (passed through unencrypted) AppleTalk and IPX; protocols that are not configured will be rejected. Data flow of a TCP/IP packet (PNN1) from host PNN1A to host PNN1B is as follows: PNN1 leaves PNN1A unencrypted and arrives at NEU A, NEU A encrypts PNN1 and sends encrypted PNN1 across the router to NEU B, NEU B decrypts PNN1 and sends unencrypted PNN1 to PNN1B. NEU data encryption and decryption of packet PNN1 is transparent to source (PNN1A) and destination (PNN1B) hosts. Details of NEU data encryption and decryption are discussed in the next section that describes the NEU to NEU data flow.

2.7 NEU-TO-NEU DATA FLOW

As described earlier, the configuration or connection table of each NEU contains node address pairs, a DES traffic encryption key, and several access control variables. Source addresses in IP packets entering the NEU are compared to NEU table addresses. A source address found in the table triggers further checks of access control variables that are used to determine whether the packet will be encrypted or simply passed onto the network without alteration. If a host address is not found in the table, the packet is either discarded or passed onto the network in accordance with configuration data.

When IP packet PNN1 arrives at NEU A, the source address in the packet is checked for existence in NEU A's connection table. The source address is identified and NEU A determines that packet PNN1 is to be encrypted based upon access control variables for source address PNN1A. The NEU encryption process increases the length of each packet by placing a protected header inside each packet. Figure 7 illustrates the transformation of packet PNN1 by the encrypting NEU A.

The protocol field in the unencrypted (clear) IP packet header is modified by NEU A to identify PNN1 as a Semaphore-encrypted data packet and to ensure that other nodes on the network discard the encrypted packet gracefully. All data above the layer-three header is encrypted using the DES CBC mode defined in ANSI-STD-X3.106. The network layer format requires a Security Association ID and an SCC MDF, Version 00h. These fields are clear data inserted into packet PNN1 between the IP header and the encrypted data. All other data above the IP header is encrypted.

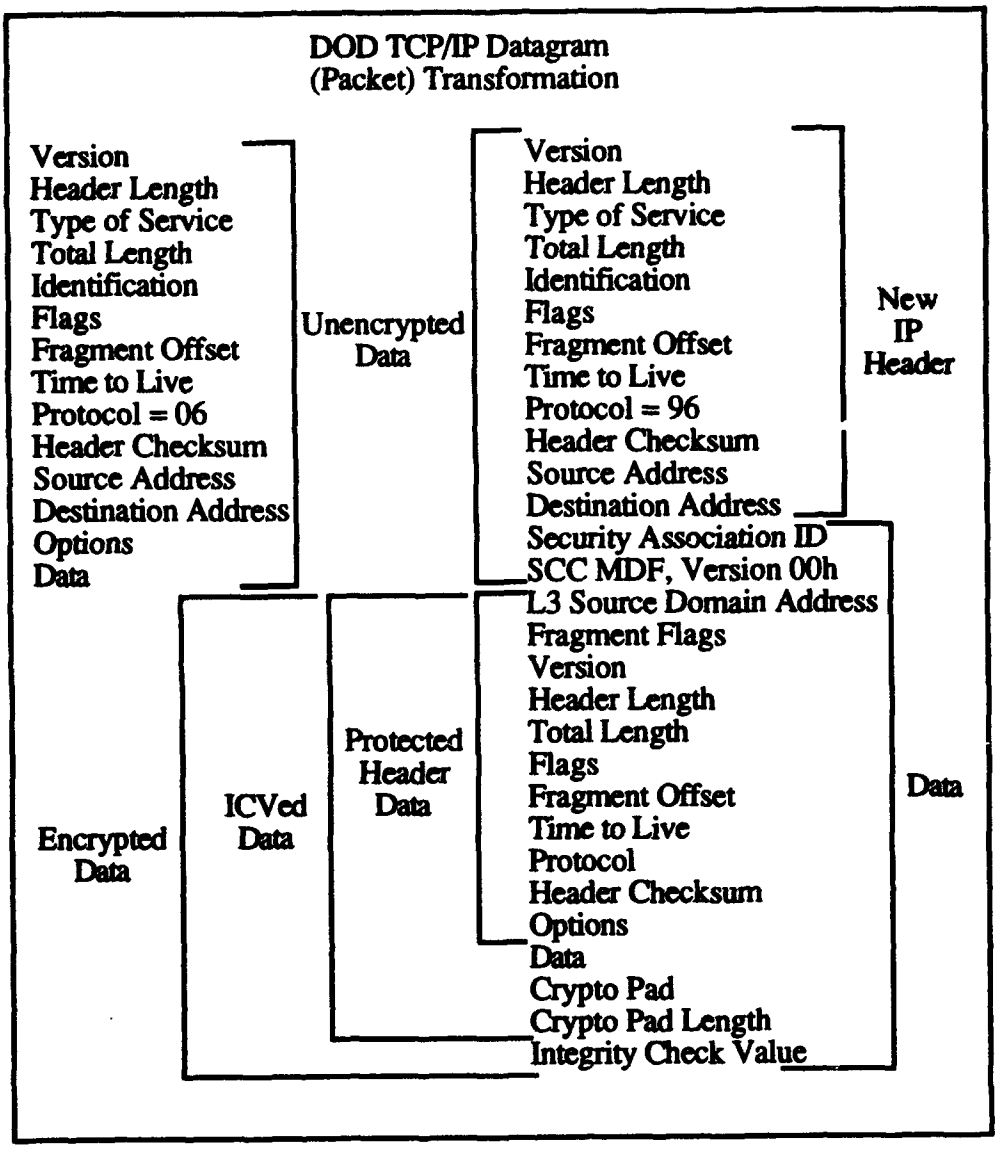

Figure 7. NEU IP-Packet Transformation

The Security Association ID is a fixed 4-byte field that "defines a cooperative relationship between NEU's." NEU A and NEU B share cryptographic keying information and security management objects represented by the security association ID. The SCC MDF is a 10-byte field "defined to allow the transfer of information that may facilitate, but is not required for, the processing of the PDU." The first byte is the SCC MDF version. Byte two is used to designate the confidentiality algorithm (CA) and the integrity check value algorithm (ICVA) used to encrypt PNN1. The remaining bytes (3 through 10) represent an initialization vector, of length 8-bytes used by DES CBC.

NEU A places a "protected header" as well as additional information required to perform cryptographic integrity checks into the data portion of PNN1. The information in the protected header is used for source authentication and other header integrity checks. It includes the following fields extracted from the clear IP header of PNN1: source address, version, header length, total length, fragmentation flags, time to live, protocol, and the header check sum. Crypto pad and crypto pad length fields are placed after the data, and finally an 8-byte integrity check value (ICV) is placed at the end of the packet. The ICV is computed prior to packet encryption during DES CBC. All data after the IP header, excluding the security association ID and the SCC MDF, is encrypted.

The NEU supports fragmentation and reassembly of packets that exceed the maximum (1500 bytes) data length for IEEE 802.3 frames; fragmentation is performed prior to packet encryption as specified by IEEE-STD-802.10B. If fragmentation occurs, NEU A will also place a fragment ID field into the protected header.

NEU A passes the encrypted PNN1 onto the Ethernet LAN for forwarding by the router. The router interprets the unencrypted IP header information and forwards PNN1 to NEU B to be decrypted. NEU B determines the DES key to use for decrypting PNN1 based upon the security association ID. When decrypting, NEU B performs source authentication by comparing the decrypted protected source address with that received in the unencrypted IP packet header. A data integrity check is also performed by NEU B in which the ICV is recomputed on the decrypted data. If there is a mismatch of protected source address or ICV data, the packet is discarded. Packets (including fragments) received by NEU B are decrypted and reassembled into the exact format as originally received by NEU A. NEU B must queue and reassemble all IP fragments before forwarding. The decrypted packet PNN1 is forwarded from NEU B to PNN1B in its original format.

2.8 NEU OPERATIONAL MODES

The following items are selectable from the front panel of the NEU: Zeroize (erases all cryptographic and other operating parameters), bypass (all data will be bypassed through the NEU, no ciphering of data), cipher (encrypting, bypassing, or blocking data based upon the access control table configuration), Signal Quality Error Test (SQET) on or off (defaulted to off, set to an as required basis by host), and self-test (a diagnostics program to test all internal circuitry and operational parameters and test failures denoted by an error message number).

Access to operational modes from the front panel requires a programmed Front Panel Key (FPK) or an operational CIK. The FPK must be programmed at the NSC. Two push buttons on the front panel of the NEU are provided for viewing and selecting items. Pressing the menu button will cycle through the choices, pressing the select button displays options for each item, and pressing both buttons will invoke the selected operation or change the selected parameter.

SECTION 3

ASSESSMENT TESTING

The primary objective of assessment testing was to examine the Semaphore NSS in an existing operational network. Specifically, the NSS was integrated into the INFOSEC Core Laboratory to examine product usability by performing interoperability and system performance testing. Tests were devised to maximize the operational capability of the NSS; interoperability tests incorporated other network devices (i.e., bridges and routers) and NSS network protocol support; system performance tests included data throughput measurements at the application level. The base test network configuration is depicted in Figure 8.

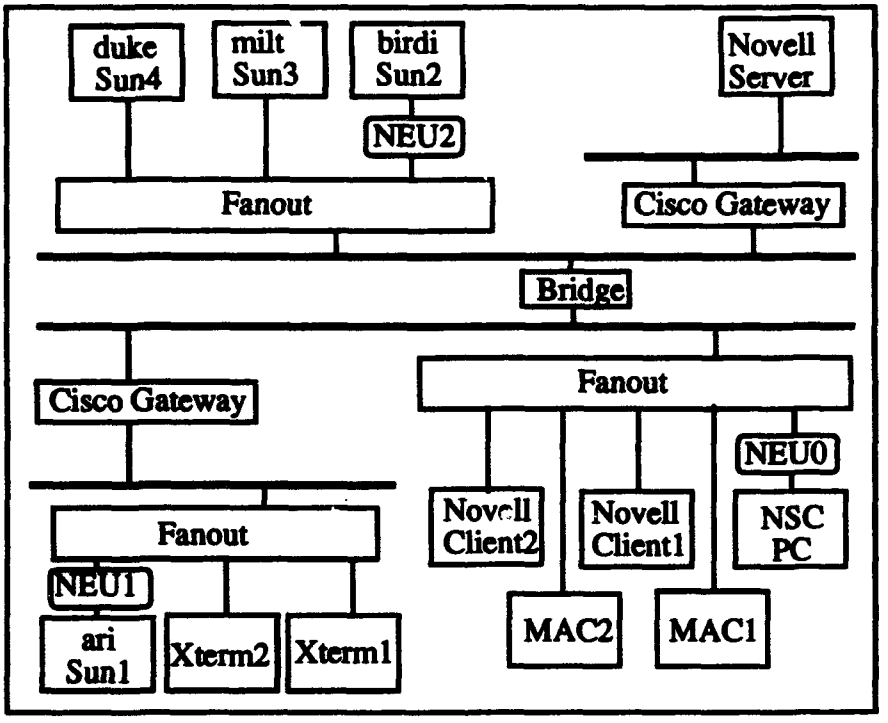

Figure 8. Base Test Network Configuration

3.1 INTEROPERABILITY TESTS

Interoperability testing and coexistence testing were conducted between standard network components (i.e., DEC LAN bridge and Cisco Gateway) to examine NEU protocol support for TCP/IP, AppleTalk, and Novell IPX protocols, respectively. Host types included in this test were Sun Workstations, MACs, and PC AT compatibles. Where applicable, tests results are indicated by PASS or FAIL. Unexpected failures are noted.

1. TCP/IP protocol support:

Configure two NEUs for ciphered network communication between two Sun workstations. Perform Telnet and file transfers between the two Sun hosts across LAN components and observe encrypted packets on the network via a network monitor for the following cases:

a. Establish ftp connection from Sun1 host to Sun2 host across:

   1. Local Subnet - PASSED as expected.
   2. Different Subnets across DEC LAN Bridge and Cisco gateway - PASSED as expected.

b. Establish Telnet connection from Sun1 host to Sun2 host across:

   1. Local Subnet - PASSED as expected.
   2. Different Subnets across DEC LAN Bridge and Cisco gateway - PASSED as expected.

2. AppleTalk protocol support (current units only support AppleTalk encipherment at the data link layer only):

Configure two NEUs for ciphered network communication (at the link layer) between two Macintosh computers. Establish an AppleShare connection between the two computers across LAN components, and observe encrypted packets on the network via a network monitor for the following cases:

a. Initiate an AppleShare connection from MAC1 to MAC2 - Failed Unexpected.

b. Initiate an AppleShare connection from MAC2 to MAC1 - Failed Unexpected.

   Note: Unexpected failure was due to a faulty LAN adapter. When the AppleShare connection was initiated in either direction, the NEU protecting MAC1 failed after 30 to 60 seconds. The NEU failure was indicated by an audible alarm and cycling error codes across its liquid crystal display (LCD). The faulty NEU was returned to Semaphore for repair.

3. Novell IPX protocol support:

Configure two NEUs for ciphered network communication between the DOS PC Novell client and the server. Establish a NetWare connection between Novell Client and Server PC's across LAN components and observe encrypted packets on the network via a network monitor for the following cases:

a. Copy a DOS file from a PC server to PC client across:

1. Local subnet - not tested.
2. Different Subnets across DEC LAN bridge and Cisco gateway - not tested.

Note: Novell client/server testing will be performed upon arrival and installation of Novell NetWare software (Version 4.0).

3.2 THROUGHPUT AND PERFORMANCE TESTS

Throughput and performance tests were conducted across various network components (i.e., host, bridges, and gateways). Host types were Sun workstations and the network protocol tested was Sun TCP/IP. A network general sniffer and Hewlett-Packard (HP) LAN analyzer were utilized to generate, collect, and monitor data. NEU sensitivity to packet size and interframe delay was tested, and performance measurements were collected at the application level in bytes per second.

1. Throughput Test: Packet Size and Interframe Delay Sensitivity

Set up traffic generator and LAN analyzer to collect throughput measurements as shown in Figure 9. For varied frame sizes, adjust the delay time between Ethernet frames to increase the throughput. For each frame size in bytes (46, 60, 576, 1024, 1400, 1460, and 1514), collect clear text throughput data and then encrypted throughput measurements. Frame sizes and maximum throughput values observed are recorded in Table 1.

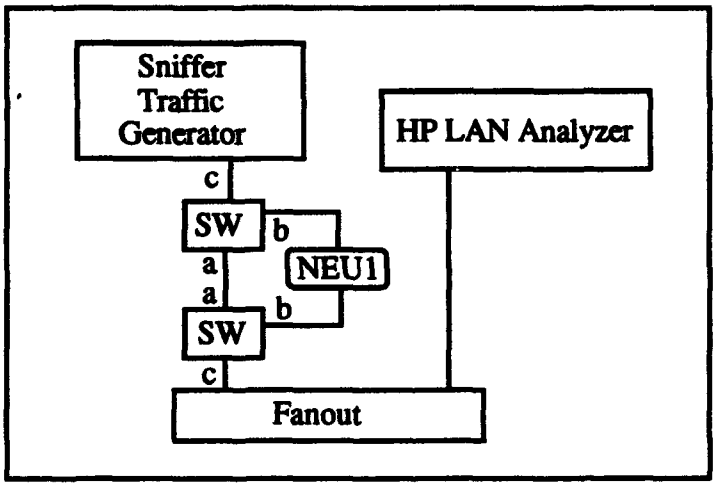

Figure 9. NEU Throughput Test Configuration

Frame Size (Bytes)		Maximum Throughput Observed	
Selected	Actual	Frames/Sec	Kbit/Sec
46	Collisions Observed (Illegal Packet Size)		
60	104	4167	3867
576	616	1861	9345
1024	1064	1105	9513
1400	1440	823	9576
1460	1504	769	9330
1514	Fragmentation	——	——
Note: NEU fragmentation first observed at 1476 Bytes			

Table 1. Throughput Rates

2. Performance at the Network Application Level:

   a. TCP/IP Test: File transfer rates between Sun Workstations using FTP.

      1. Configure Sun1 behind NEU1 and configure Sun2 behind NEU2 on LAN across bridge and gateway as shown in Figure 10.

         - Set up directory of ten files ranging in file size (22 to 2,000,000 bytes).
         - Establish an ftp session between Sun1 and Sun2.
         - Transfer directory of files ten times using mput, then ten times using mget between Sun1 and Sun2 in clear text, and then repeat identical file transfers encrypted across NEU.

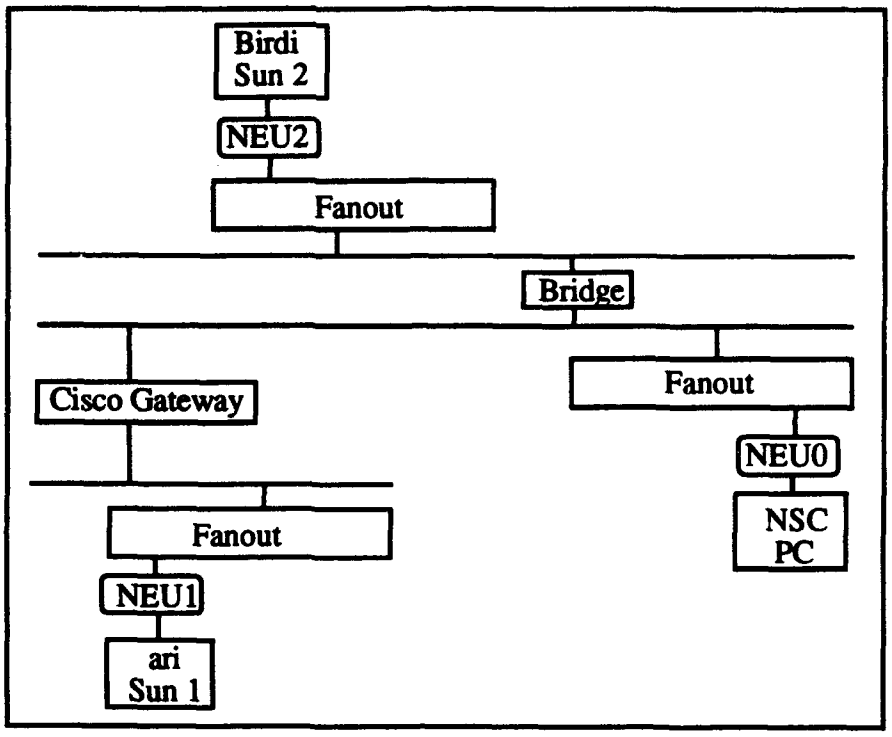

Figure 10. NEU Network Configuration for File Transfers Across Bridge and Gateway

- Average transfers rates for each file size are recorded in Tables 2 and 3.

File Size Bytes	mput (Sun default TCP segment size of 1460)			
	Avg Total Number of Seconds		Avg KBytes Per Second	
	Clear Text	NEU	Clear Text	NEU
513	.001	.001	425	421
1005	.001	.001	771	745
5437	.003	.002	2080	2070
20170	.009	.009	2250	2290
49789	.049	0.94	1010	53
100594	0.15	2.72	673	37
355220	0.54	12.75	655	29
662528	0.97	12.05	683	55
1015808	1.46	19.92	694	51
2359296	3.46	47.19	681	50

Table 2. mput File Transfers Rates Across LAN Bridge and Cisco Gateway

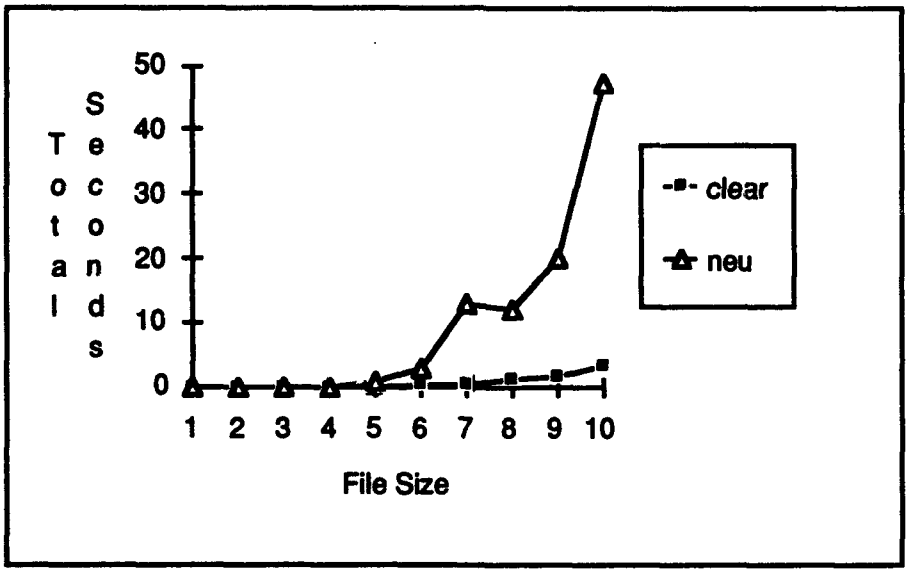

Table 2a. Graph of mput File Transfers Rates Across LAN Bridge and Cisco Gateway

File Size Bytes	mget (Sun default segment size of 1460)			
	Avg Total of Seconds		Avg KBytes Per Second	
	Clear Text	NEU	Clear Text	NEU
513	.001	.001	343	357
1005	.001	.002	657	609
5437	.128	.121	42.2	75.30
20170	.184	.231	124	84.90
49789	.244	7.34	201	38.27
100594	.348	7.57	312	70.66
355220	.529	25.96	657	57.71
662528	.909	47.38	714	41.32
1015808	1.41	48.10	692	46.50
2359296	2.86	85.60	809	26.90

Table 3. mget File Transfers Rates Across LAN Bridge and Cisco Gateway

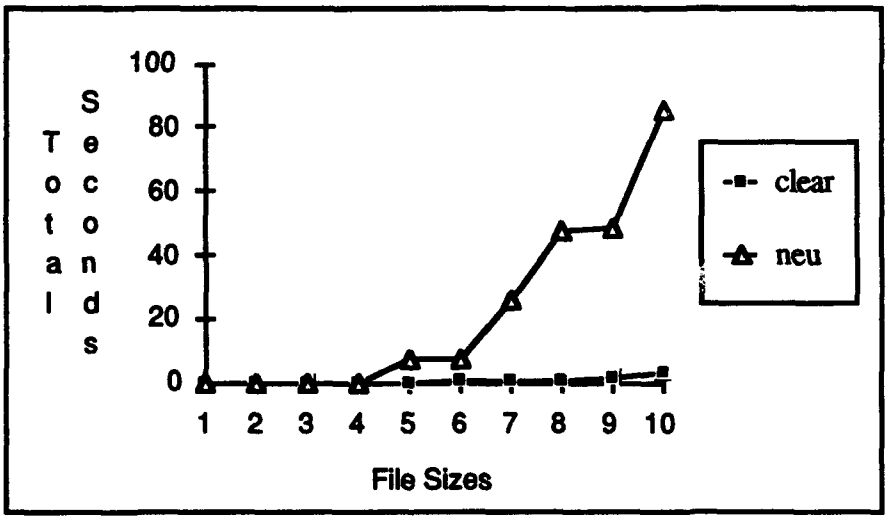

Table 3a. Graph of mget File Transfers Rates Across LAN Bridge and Cisco Gateway

Trials in Tables 3 through 5 were derived using default Sun TCP parameters. However, total transfer times (across the NEU) were observed to improve by approximately one-third to one-fourth of the times indicated in each table when specific TCP parameters were modified. For example, in Table 4, the total file transfer time in seconds for the 2.3 MB file is 93 seconds. Reduction of the TCP retransmit threshold parameter from three to one reduced this average file transfer rate from 93 to 24 seconds. Maximum file transfer rates through the NEU were observed using a modified TCP maximum segment size of 1400 bytes across different subnets.

On a local subnet, Sun workstations ignore the TCP maximum segment size when transmitting data and the default maximum segment size (observed at 1460) or a negotiated size is used. Because additional information is added to each packet by the NEU, fragmentation results on the black side of the NEU. Slow reassembly of fragmented packets by the NEU additionally causes retransmissions of packets by the host. The combination of delays due to NEU fragmentation and host retransmissions significantly reduces throughput and total transfer times.

2. Reconfigure Sun1 and NEU1 to reside on the same local subnet as Sun 2 and NEU2 as shown in Figure 11.

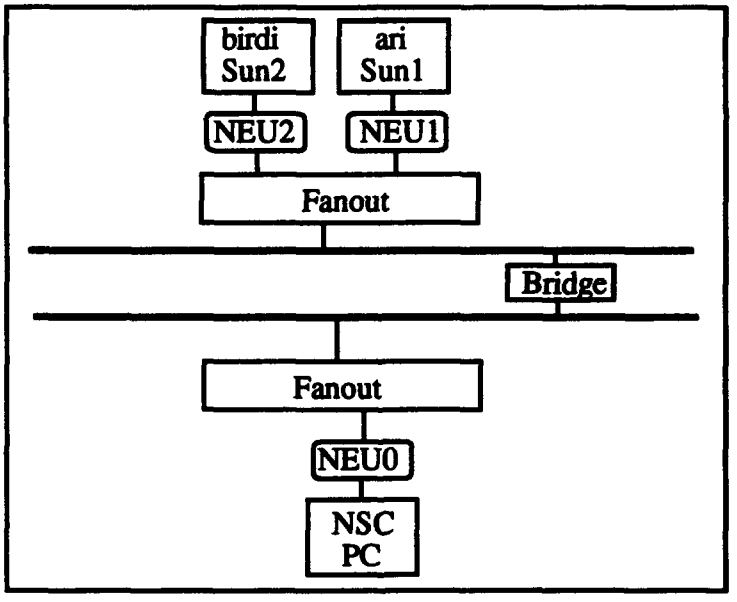

Figure 11. NEU Test Configuration for File Transfers Between Suns on the Same Subnet

3. Display graphics across XTERM connection between Suns in clear text and then encrypt by NEU as shown in test configuration Figures 3 and 4.

Repeat steps for test number one above. Average transfer rates for mputs and mgets are recorded in Tables 4 and 5.

File Size Bytes	mput			
	Avg Total Number of Seconds		Avg KBytes Per Second	
	Clear Text	NEU	Clear Text	NEU
513	.001	.001	379	414
1005	.001	.001	772	766
5437	.002	.003	2080	2120
20170	.009	.009	2093	2310
49789	.041	7.12	1200	40.92
100594	.105	16.24	925	32.08
355220	.472	31.90	735	26.11
662528	.908	51.70	712	26.76
1015808	1.37	56.70	723	31.10
2359296	3.16	93.90	73	24.60

Table 4. mput Transfers Rates Between Suns on Same Subnet

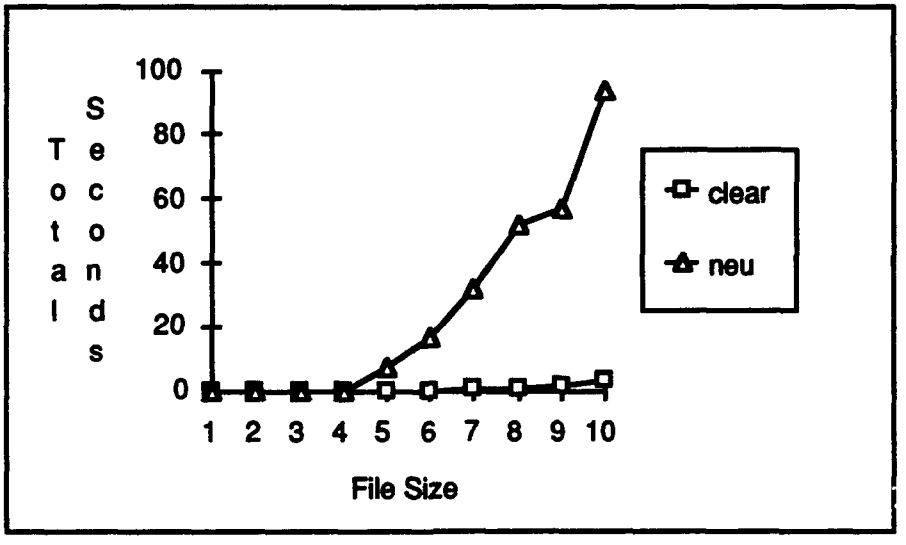

Table 4a. Graph of mput Transfers Rates Between Suns on Same Subnet

File Size Bytes	mget			
	Avg Total # of Seconds		Avg KBytes Per Second	
	Clear Text	NEU	Clear Text	NEU
513	.001	.001	670	.344
1005	.001	.002	677	.628
5437	.002	.002	2250	.2260
20170	.009	.803	2390	26.2
49789	.035	44.31	1390	21.74
100594	.181	32.73	556	27.27
355220	.433	36.36	751	34.79
662528	.829	49.11	802	32.92
1015808	1.21	79.00	815	12.73
2359296	2.71	152.00	850	15.00

Table 5. mget File Transfers Rates Between Suns on Same Subnet

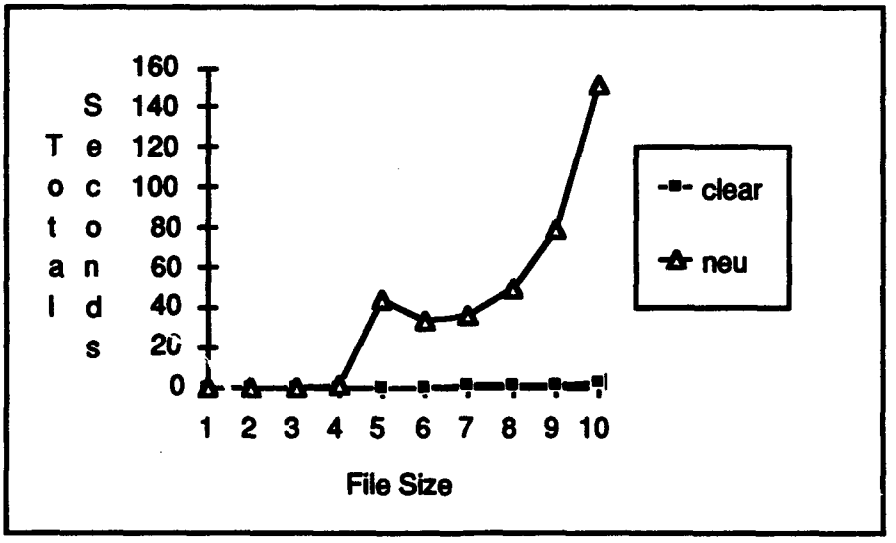

Table 5a. Graph of mget File Transfers Rates Between Suns on Same Subnet

Actual and graphic transfer rates for 10 samples each are recorded in Tables 6 and 7.

Total Frames		Frames Per Second		Total Seconds	
Clear Text	NEU	Clear Text	NEU	Clear Text	NEU
.4906	.4823	9.62	5.92	57.84	94.16
.4882	.4742	9.64	5.22	57.78	106.76
.4876	.4876	9.64	4.87	57.75	114.31
.4883	.4771	9.64	5.48	57.80	101.56
.4879	.4792	9.65	5.19	57.70	107.38
.4882	.4807	9.67	5.45	57.59	102.20
.4874	.4839	9.66	5.59	57.68	99.64
.4887	.4811	9.68	5.40	57.51	103.15
.4874	.4846	9.66	5.08	57.65	109.60
.4874	.4809	9.67	5.22	57.60	106.61

Table 6. Data Points: mjackson.mpg (724576 bytes) Across Bridge and Gateway

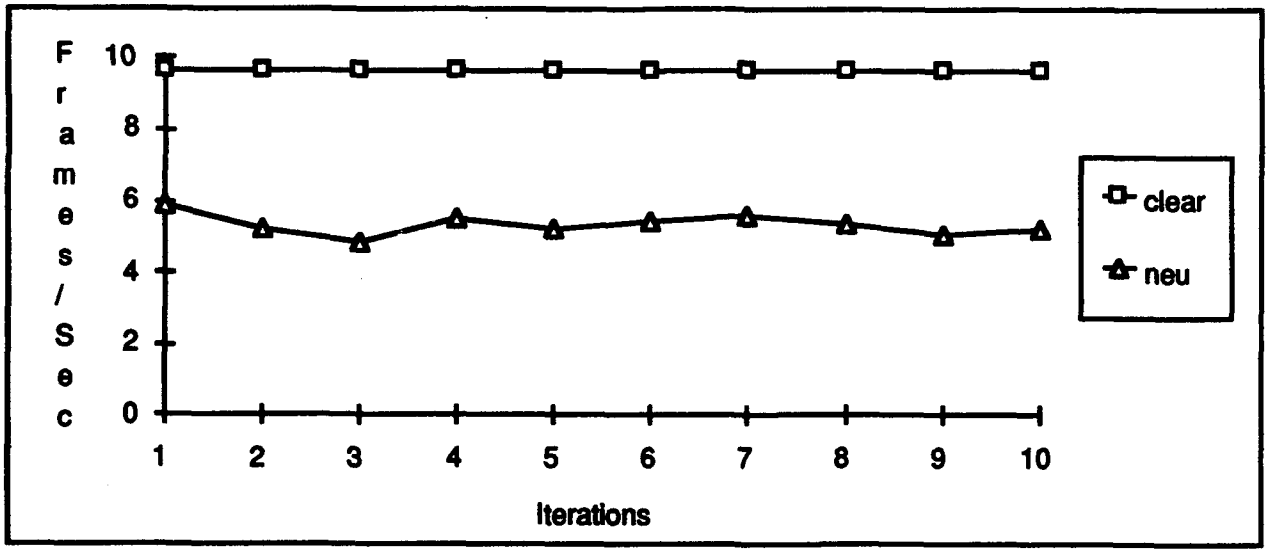

Table 6a. Graph: mjackson.mpg (724576 bytes) Across Bridge and Gateway

Total Frames		Frames Per Second		Total Seconds	
Clear Text	NEU	Clear Text	NEU	Clear Text	NEU
.4854	.7189	11.13	1.74	50.05	319.90
.4851	.7227	11.19	1.78	49.77	312.52
.4852	.7192	11.13	1.74	50.02	320.36
.4847	.7461	11.16	5.92	49.92	94.09
.4844	.7201	11.13	1.75	50.01	317.76
.4843	.7207	11.17	1.75	49.86	316.49
.4850	.7213	11.18	1.80	49.83	308.71
.4853	.7233	11.22	1.75	49.67	318.06
.4847	.7486	11.17	3.27	49.84	169.91
.4848	.7442	11.16	5.94	49.90	93.70

Table 7. Data Points: mjackson.mpg (724576 bytes) Between Suns on Same Subnet

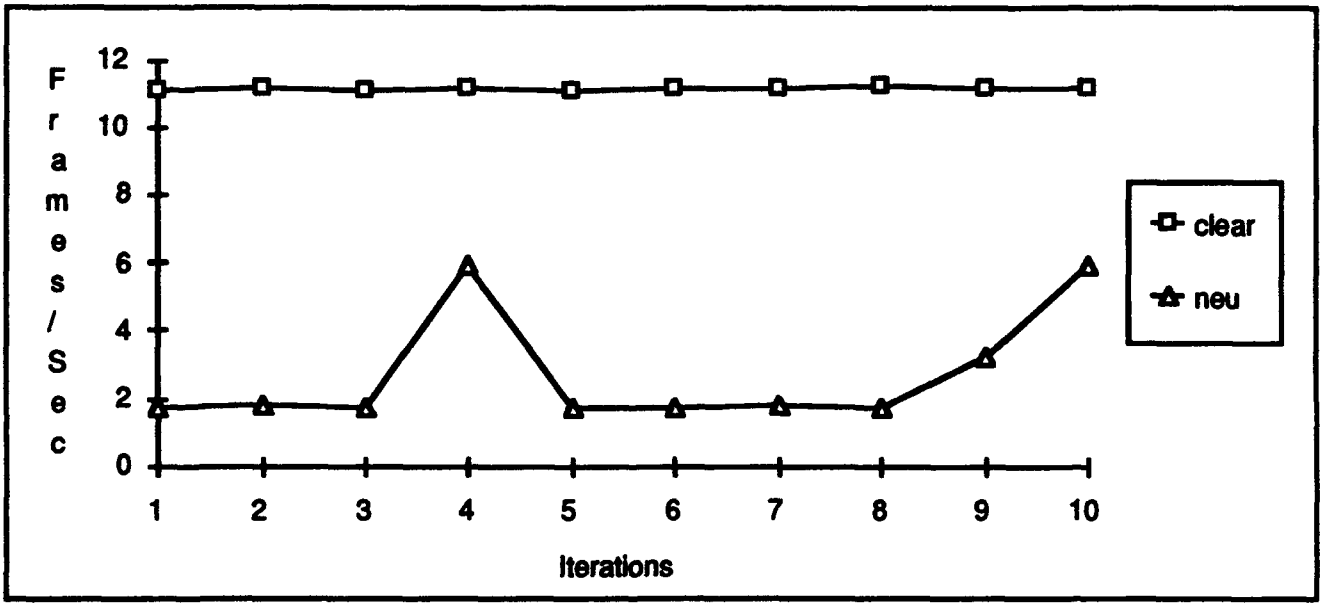

Table 7a. Graph: mjackson.mpg (724576 bytes) between Suns on Same Subnet

SECTION 4

SUMMARY OF TEST RESULTS

The summary of test results are grouped into four categories that were derived from areas of concern based upon test observations. Test categories are performance and throughput, hardware reliability, installation and maintenance, and user documentation.

4.1 PERFORMANCE AND THROUGHPUT

The raw throughput rates observed during testing were consistent with the Semaphore-projected rates of 9 MBits/Sec (800 packets/sec). However, the application-level data transfer rates observed were inconsistent and unpredictable. Software configurations were adjusted on Sun workstations to maximize file transfer rates; this involved adjustments to TCP maximum segment size and retransmission threshold parameters. Adjustments did improve throughput, but rates remained inconsistent.

Inconsistent and often slow file transfer rates (as described by Semaphore) were due to restricted buffer sizes of the NEU in conjunction with the NEU fragmentation reassembly process. When receiving fragmented packets, the NEU reassembly process was too slow to keep up with the volume of fragments received. As a result, retransmission of packets occurred from the source. Packet retransmissions increased with NEU packet fragmentation. Semaphore claims to have addressed these problems in the next release of its products. Additional buffer space will be available with the replacement of the current memory chips. The speed of the NEU fragmentation reassembly process will also be improved.

4.2 HARDWARE RELIABILITY

Hardware problems were uncovered during testing. Each of the original test units were observed to fail if disconnected from the network for some short (but undetermined) period of time. These units were replaced with newer ones containing firmware upgrades that corrected the failure. Subsequently, attempts to configure AppleTalk encipherment (link layer only) failed due to a faulty LAN adapter in one of the NEUs. This failure occurred only during attempts to initiate AppleTalk network connections. The faulty unit was returned to Semaphore for repair. Semaphore addressed hardware problems by replacing/repairing equipment with minimal turnaround and downtime.

4.3 INSTALLATION AND MAINTENANCE

Physical installation of the lightweight NEU was simple and fast. Out of the box, basic installation includes placement of batteries, plugging into an outlet, and connecting network cables. All initial configuration was performed at the NSC. Initialization of each NEU was started by inserting and removing (approximately two seconds) its programmed initialization

key. Completion of initialization takes a couple of minutes and occurs across the network. The NSC and NEU must exchange authentication information. The NSC downloads configuration data to the NEU. Once operational, maintenance is minimal; a good battery is the primary concern in case of power loss. However, the establishment of a practical maintenance and security policy is recommended. Maintenance software, such as Self-test and diagnostics, is available via the NEU front panel. Access is protected by requiring the insertion of a programmed FPK or CIK.

4.4 USER DOCUMENTATION

Issues with the product documentation were a concern. Although satisfactory for initial and basic TCP/IP configurations, the documentation was determined to be incomplete and unsatisfactory for administering other tasks, such as configuring for link level encryption. In particular, there were no instructions available for configuring AppleTalk or any of the link-level protocols. The documentation also cited product functionality as if it were currently available for use, whereas it is not. Additionally, the user-friendly configuration menus, although straightforward and easy-to-use, were found to be tedious and time-consuming. Deficiencies found in the documentation and configuration menus are being corrected in conjunction with enhancements of soon-to-be-released products.

SECTION 5

FUTURE WORK

Effective resolution of issues described in section 4 were expected with the release of Semaphore site units (NEU-RT and NEU-ST). The site units will have added functionality that is more applicable to current needs. In addition to site-to-site network protection, support for Frame Relay, SNMP, and AppleTalk routing (the NEU-WG test units, model 3013, support AppleTalk at the link layer only) will be available in these new product releases. The new and improved NEU-WG model 3013A is currently available and addresses the performance and fragmentation problems uncovered during testing. Semaphore asserts that performance is significantly improved with the new units. Semaphore has also proposed the development of a board-level version of the NEU for placement into a host computer. The schedule for development and release of the board-level product is undetermined at this time.

The primary focuses of this preliminary examination of the NEU-WG unit were interoperability, performance, and ease of use. Future integration testing is recommended for the new Semaphore products that will more closely fit our sponsors' needs. At that time, it is recommended that network security vulnerabilities (i.e., replay) and security features be more closely examined. Performance tests should also be rerun on the new and improved units.

BIBLIOGRAPHY

August 1993, Semaphore Communications Corporation, *Network Security Center User Guide*, Version 2.0, Santa Clara, CA.

September 1993, Semaphore Communications Corporation, *Semaphore Global Security Architecture*, White Paper, Santa Clara, CA.

10 June 1993, Semaphore Communications Corporation, *Network Security for the Next Generation*, Briefing Slides, Santa Clara, CA.

16 August 1993, Semaphore Communications Corporation, *NEU-RT, Technical Product Description* P/N 98-0004, Rev A Santa Clara, CA.

16 August 1993, Semaphore Communications Corporation, *NEU-ST, Technical Product Description*, P/N 98-0003, Rev A Santa Clara, CA.

IEEE, Inc., Standards for Local and Metropolitan Area Networks: 802.10B Interoperable LAN/MAN Security (SILS), IEEE STD 802.10-1992, IEEE, Inc., New York, NY.

LIST OF ACRONYMS

ANSI	American National Standards Institute
AUI	Attachment Unit Interface
CA	Confidentiality Algorithm
CBC	Cipher Block Chaining
CIK	Cryptographic Ignition Key
COI	Community of Interest
COTS	Commercial-off-the-shelf
DEC	Digital Equipment Corporation
DES	Data Encryption Standard
DOD	Department of Defense
FPK	Front Panel Key
HP	Hewlett-Packard Company
IBM	International Business Machines
ICV	Integrity Check Value
ICVA	Integrity Check Value Algorithm
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers, Inc.
INFOSEC	Information Security
INK	Initialization Key
IP	Internet Protocol
IPX	Inter-Network Pack Exchange
ISO	International Standards Organization
LAN	Local Area Network
LCD	Liquid Crystal Display
MAC	Macintosh
MB	Megabyte
MBits	Megabits
MDF	Management-Defined Field
mget	multiple get
MHz	Megahertz
mput	multiple put
NAK	NSC Access Key
NEU	Network Encryption Unit
NEU-HB	Network Encryption Unit-Hub
NEU-PC	Network Encryption Unit-Personal Computer
NEU-RT	Network Encryption Unit-Router

NEU-ST	Network Encryption Unit-Site
NEU-WG	Network Encryption Unit-Work Group
NSC	Network Security Center
NSS	Network Security System
PC	Personal Computer
PC AT	Personal Computer Advanced Technology
PDU	Protocol Data Unit
PNN	Protected Network Node
RAM	Random Access Memory
RISC	Reduced Instruction Set
RSA	Rivest, Shamir, and Adleman
SQET	Signal Quality Error Test
STD	Standard
SVGA	Super Video Graphics Adaptor
TCP	Transmission Control Protocol
TEK	Traffic Encryption Key
XTERM	X-Windows Terminal