NISTIR 90-4228

NEW NIST PUBLICATION
December 1989

PROTOTYPING SP4 A SECURE DATA NETWORK SYSTEM TRANSPORT PROTOCOL INTEROPERABILITY DEMONSTRATION PROJECT

Charles Dinkel
Noel Nazario
Robert Rosenthal

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
National Computer Systems Laboratory
Computer Security Division
Gaithersburg, MD 20899

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary

Lee Mercer, Deputy Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Raymond G. Kammer, Acting Director

NIST

NISTIR 90-4228

PROTOTYPING SP4 A SECURE DATA NETWORK SYSTEM TRANSPORT PROTOCOL INTEROPERABILITY DEMONSTRATION PROJECT

Charles Dinkel
Noel Nazario
Robert Rosenthal

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
National Computer Systems Laboratory
Computer Security Division
Gaithersburg, MD 20899

January 1990

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
Lee Mercer, Deputy Under Secretary for Technology
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Raymond G. Kammer, Acting Director

TABLE OF CONTENTS

PROTOTYPING SP4
A SECURE DATA NETWORK SYSTEM TRANSPORT PROTOCOL INTEROPERABILITY DEMONSTRATION PROJECT

Charles Dinkel, Noel Nazario, and Robert Rosenthal
Computer Security Division
National Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, Maryland 20899

ABSTRACT

The NIST Secure Data Network System (SDNS) project implements computer to computer communications security for distributed applications. The internationally accepted Open Systems Interconnection (OSI) computer networking architecture provides the framework for SDNS, which is a project of the National Security Agency (NSA). SDNS utilizes the layering principles of OSI to implement secure data transfers between computer nodes of local area and wide area networks. SDNS implements SP4, a security protocol at the OSI Transport layer (layer 4) that provides end-to-end reliable transparent data communications with confidentiality and integrity security services. Laboratory prototypes of SP4 formed the basis of proposed voluntary national standards and will form the basis for future security enhancements for the Government Open Systems Interconnection Profile (GOSIP).

KEY WORDS

Computer security, conformance testing, local area networks (LAN), network security, protocol security, SDNS, transport protocols

---

The mention of certain vendor products in this report in no way implies endorsement or recommendation of any kind.

PREFACE

The Computer Security Act of 1987 (P.L. 100-235), focuses attention on the need to protect sensitive government information. The National Institute of Standards and Technology (NIST) is assigned the responsibility for developing standards and guidelines to improve the Federal Government's management and use of computer and related telecommunications systems. Included in this effort is developing cost-effective security mechanisms for providing privacy and security of sensitive information in Federal computer systems.

In addition to its responsibilities for the development of standards and guidelines, NIST's National Computer Systems Laboratory (NCSL) provides technical assistance to federal agencies and conducts a program of research. This program supports both standards development and technical assistance, and includes the development of test methods, the conduct of laboratory based activities, and collaborative research with other organizations.

In all areas of standards development, NIST has adopted the approach of working closely within the voluntary standards community to encourage National and international standards that meet the requirements of the U.S. Federal Government. The networking standards community bases its work on the International Standard Organization's (ISO) Basic Reference Model for Open Systems Interconnection (OSI). This model, recognized internationally as a framework under which computer-to-computer communications protocols are developed, forms the basis for NIST's standards development and implementations activities for computer networks.

1. PROJECT SUMMARY

1.1 Computer Network Security - Why Needed?

The Open Systems Interconnection (OSI) standards being adopted by government and industry make it possible to interconnect computer systems manufactured by different vendors. Maintaining the confidentiality, integrity, and availability of data transmitted between these interconnected computers poses new problems. Users of networked computers need assurance that the systems with which they are communicating are not only "open", but also secure from unauthorized modifications, undetected loss, and unauthorized disclosure. Standard security protocols must provide for the verification of the identities of both the senders and receivers of data to ensure that computers and connecting communications are secure.

1.2 Why Security at Layer 4 (SP4)?

The Transport layer of the 7-layer OSI model provides reliable end-to-end transparent data communications through a network. The Transport layer security protocol (SP4) provides confidentiality and integrity services to data being transmitted between computers. NIST decided to focus initial network security work at layer 4 for several important reasons:

a. Security at the Transport layer (SP4) is independent of network technology

b. The security protocols developed for the transport layer had matured to the point where vendors could begin building prototype implementations.

c. SP4 had the potential to become a government and industry standard.

1.3 NIST's OSI Security Laboratory

The OSI Security Laboratory was established to provide a resource where interested researchers from government and industry can experiment with new network security ideas. Three vendors, Digital Equipment Corporation, IBM, and Hughes Aircraft Company are currently using the laboratory to test and demonstrate a subset of the Transport Layer security protocols (SP4).

1.4 Results

a. Interoperability of the Hughes and Digital prototype SP4 implementations has been achieved.

b. The success of the NIST project prompted NSA to release ten Secure Data Network System (SDNS) documents for public review.

c. The SP4 protocol specification has been accepted by the American National Standards Institute (ANSI) as a New Work Item.

1.5 Future Work

The results achieved in the OSI Security Laboratory demonstration of SP4 justify follow-up work. NIST is planning to develop a reference implementation of SP4 and related conformance test methodologies and to initiate work in the area of Key Management. The use of labels in SP4 is another item that is under investigation. Integrated Services Digital Networks (ISDN) security activities may lead to the establishment of an OSI/ISDN security laboratory.

2. INTRODUCTION

This report describes the results of work that NIST completed as part of its commitment to provide solutions and develop standards for, computer network security. The approach that NIST adopted was to work in partnership with the National Security Agency (NSA) and industry to demonstrate security at the Transport layer of the OSI model.

NIST is active in developing federal, national and international security standards based on laboratory results in network security. An OSI Security Laboratory was established to permit engineers from NIST, IBM, Digital and Hughes to cooperatively develop prototype implementations of Transport layer security protocols (SP4). Interoperability demonstrations of the SP4 implementations provided by the three vendors were conducted in the laboratory. An important goal of this effort is to develop commercial markets for security products based on U.S. Government and industry requirements.

3. BACKGROUND INFORMATION FOR SP4

The Security Protocol at Layer 4 of the OSI 7-layer architecture is called SP4. The OSI architecture is defined by International Standard IS-7498, a document issued by the International Organization for Standardization (ISO). The SP4 protocol document is based on the Security Architecture addendum to OSI, IS-7498/2. SP4 provides Integrity and Confidentiality services at the bottom of the Transport Layer (layer 4), right on top of the Network Layer (layer 3).

Layer 4 is the first place in the OSI architecture where reliable end-to-end connections are established. All the addressing information in layer 3 and below remains in the clear. For this reason SP4 can provide transparent protection regardless of the type of network used; e.g. wide area or local area.

SP4 makes no assumptions about the encryption algorithm(s) used. It also assumes that some other trusted entity is responsible for providing pairwise cryptographic associations that support local security policies.

SP4 takes the information from layer 4 and above and encapsulates it. If the Integrity Service is requested, the encapsulation consists of a cryptographic checksum performed over all the information from Transport and above. The result of the checksum is appended to the end of the packet. If Confidentiality is requested, the packet plus the integrity checksum, if present, is encrypted.

There are two major options in SP4; SP4-E and SP4-C. SP4-E stands for "End-to-End" SP4 protection. This option provides a single cryptographic association to protect all communications between any pair of end systems. The E option supports a connectionless security service as described in IS-7498/2. SP4-E provides protection for either connection-oriented or connectionless Transport.

SP4-C is "Connection-oriented" SP4 protection. Under this option every Transport connection is protected by an individual cryptographic association. It provides a finer key granularity than SP4-E. This is a connection-oriented security service as specified in IS-7498/2. SP4-C protection can only be provided when a connection-oriented Transport service is available.

4. SP4 INTEROPERABILITY PROJECT DESCRIPTION

4.1 GOSIP Security

The Government Open Systems Interconnection Profile (GOSIP), FIPS 146, identifies standard OSI network protocols and specific options for use in federal Government distributed computer network applications. Taken together, these standard protocols and options form a profile. Today, GOSIP does not include a security profile, but does includes a chapter on security that provide for a security label consistent with the Internet Protocol Security Option. The appendix to GOSIP identifies security as the highest priority advanced requirement for future versions of GOSIP.

NIST works with the National Security Agency (NSA) and industry to bring proposals for security technology standards to the voluntary standards community. The goal is to develop internationally accepted standards that can be implemented in network security products, that meet the U.S. Government's security requirements and can be marketed internationally by U.S. industry. The GOSIP security profiles will reflect these international standards where appropriate.

4.2 The Secure Data Network System (SDNS) Project at NIST

At the present time there are no base standards for computer network security. One of NIST's objectives in participating in the SDNS project was to assist in developing a framework of base standards for security. Working with IBM, Digital and Hughes, NIST was able to develop a set of agreements for demonstrating the interoperability of SP4 prototype implementations.

The SP4 protocol specification has been modified and updated as a result of work accomplished in the NIST OSI Security Laboratory. This specification has been submitted to ANSI where it is expected it will serve as the basis for a national, and eventually, an international (ISO) standard for security. Once base standards for security exist, these can be submitted to the NIST Workshop for Implementors of OSI to begin the process of establishing stable implementation agreements. These agreements often serve as catalysts to the development and marketing of actual vendor products.

While it is recognized that detailed security mechanisms would differ for classified and unclassified applications, both would benefit from a common security foundation. The OSI Basic Reference Model provides the foundation. Through participation in the Secure Data Network System (SDNS) project of the National Security Agency, NIST expects to exploit the potential economic benefits derived from standardizing security built on that foundation. NIST's SDNS activities will help define the architecture and protocols within the framework of the OSI computer network model to provide data communications with security. In addition, requirements for a key management system will be specified and vendors encouraged to develop interoperable equipments that implement SDNS Protocols.

Three phases of the SDNS project were defined. Phase 1, completed in mid 1987, developed a security architecture based on the OSI model and defined a key management system for use on commercial data networks.

Phase 1A, focused on the development of protocols for Phase 1.

Phase 2 will result in a family of low cost interoperable off-the-shelf security products for use in personal computers, micro and mini-computers, modems and host computers. These devices will provide protection for local area networks (LANS), electronic mail (E-Mail), and public and private data networks.

4.3 SDNS Status

NIST has taken an active role in national and international standards activities for computer networks; and at industry's request, NIST sponsors the NIST Workshop for Implementors of Open Systems Interconnection. Workshop documents record stable implementation agreements of OSI protocols among the organizations participating in the NIST Workshop. The Workshop's Special Interest Group on Security has reviewed the SDNS documents dealing with security protocols at layer 3 (SP3) and at layer 4 (SP4). Current work involves defining the security services and information that must be provided by a Key Management System to SP4.

The dotted lines in Figure 1 illustrate the possible locations for security protocols in the GOSIP, FIPS 146. NIST's computer network security standards activity focuses on development of security profiles that include SP3, SP4, security management, security for electronic mail (X.400), and possibly SP2 security.

In April 1989, NSA released the SP4 specification into the public domain. The ANSI committee responsible for data communications (X3S3.3) reviewed the SP4 document during its April 1989 meeting and approved it for placement as a New Work Item for ISO standardization. This contribution serves as base text for use in preparation of Addenda to the ISO 8073 (OSI Connection Oriented Transport Protocol Specification) and ISO 8602 (OSI Connectionless Transport Service) documents.

The following SDNS documents have also been released for public review:

SDNS.301 - Security Protocol 3 (SP3)
SDNS.601 - Key Management Profile - Communication Protocol Requirements for Support of the SDNS Key Management Protocol
SDNS.701 - Message Security Protocol
SDNS.702 - SDNS Directory Specifications for Utilization with the SDNS Message Security Protocol
SDNS.801 - Access Control Documents
SDNS.802 - Access Control Specification
SDNS.902 - Key Management Protocol - Definition of Services Provided by the Key Management Application Service Element
SDNS.903 - Key Management Protocol - Specification of the Protocol for Services Provided by the Key Management Application Service Element
SDNS.906 - Key Management Protocol - SDNS Traffic Key Attribute Negotiation

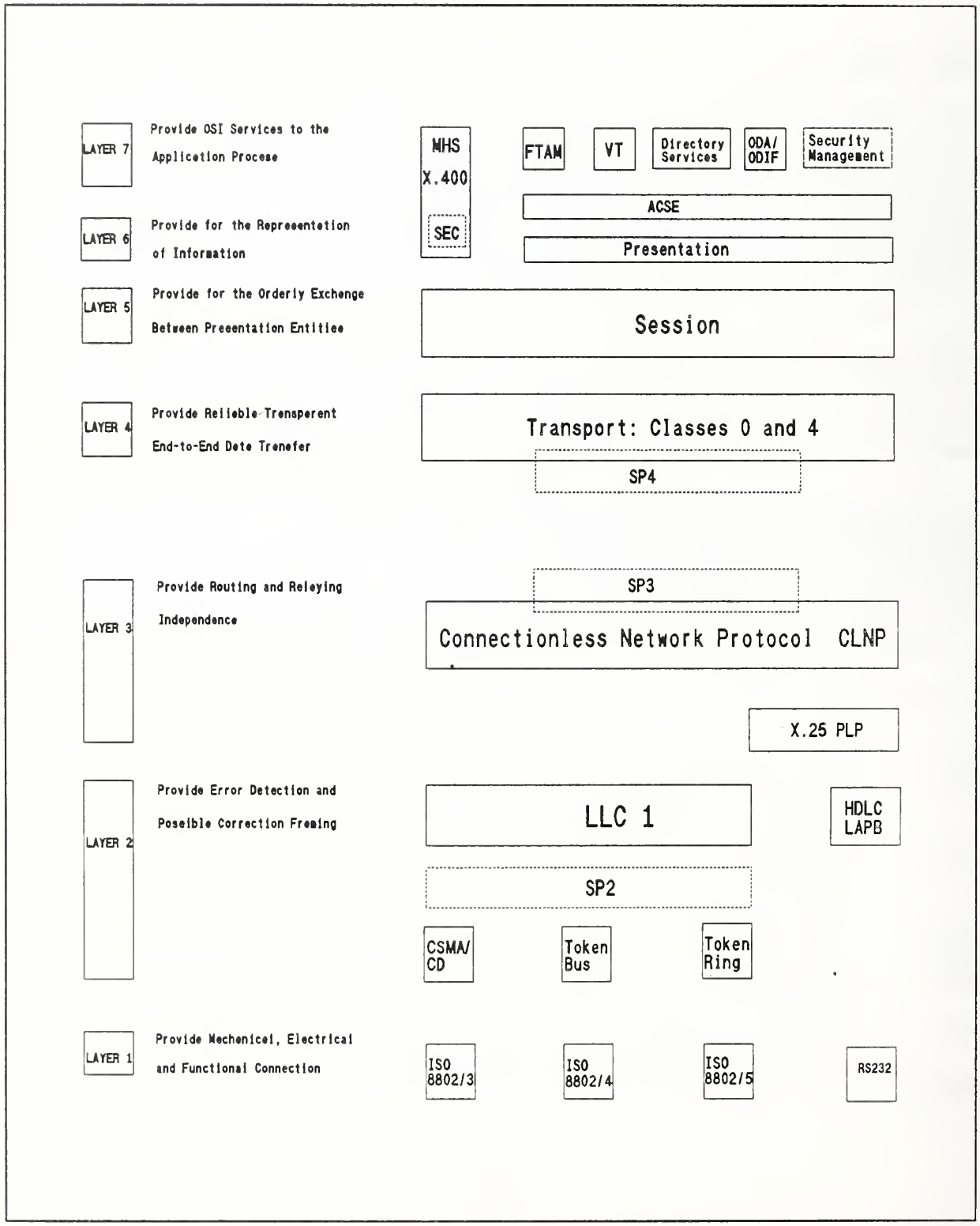

Figure 1 SDNS Protocols in a GOSIP Profile

4.4 SP4 Protocol Development

SDNS SP4 Implementors Meetings were held approximately every two months at NIST. During these meetings, the participants, representatives from IBM, Hughes, and Digital, met with NIST engineers and reviewed the status of the SP4 implementations, updated the set of Demonstration Agreements, and recommended changes and corrections to implementations in the laboratory. The Demonstration Agreements were a subset of the SP4 protocol specifications that the three vendors agreed to implement in their prototypes. Appendix 3. is an outline of those agreements.

Laboratory sessions permitted the vendor representatives to discover differences and "bugs" that prevented their SP4 implementations from interoperating. Information from this work was reviewed at the SP4 Protocols Meeting and agreements modified and/or confirmed. This allowed the vendors to return to the laboratory with a clearer understanding of what had to be done to their hardware and software to achieve interoperability.

5. OSI SECURITY LABORATORY PROGRAM

NIST's OSI Security Laboratory was established as a direct result of a recognized need for improved computer network security. Current research focuses on security at the Transport Layer (SP4), where reliable end system computer to end system computer communications is provided.

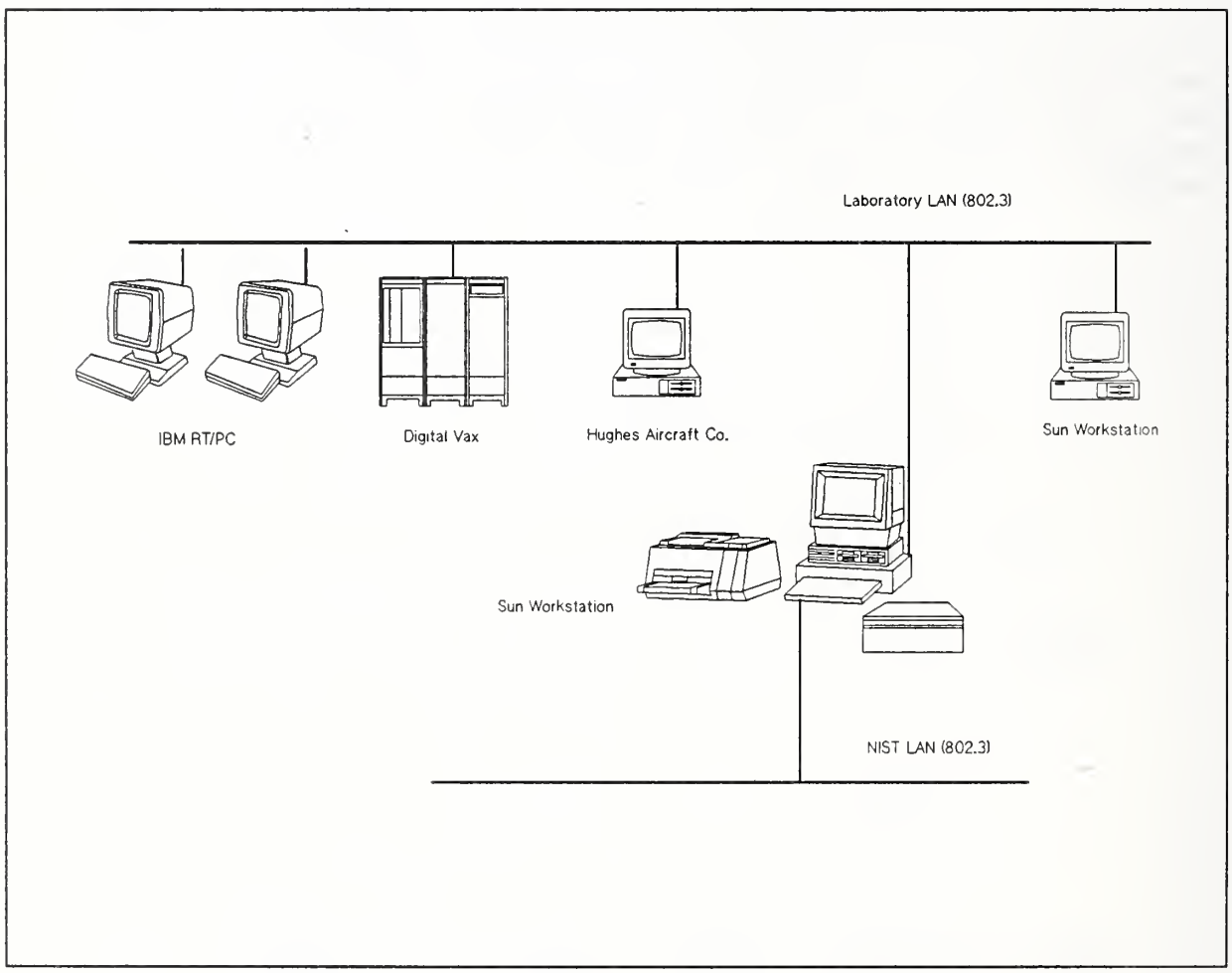

Figure 2 SDNS SP4 Laboratory Configuration

The objectives of NIST's OSI Security Laboratory Program are:

- Develop OSI security standards that would be useful in government and commercial applications;
- Develop and perform interoperability demonstrations of OSI security equipment;
- Develop automated conformance testing methodologies for the standards;
- Develop conformance tests of security devices implementing the standards;
- Maintain compatibility between the public OSI security standards and the Secure Data Network Systems (SDNS) specifications.
- Stimulate the development of commercial products compatible with OSI standards

Figure 2 illustrates the laboratory layout and the configuration for the computers that are participating in the SP4 interoperability tests. The NIST IEEE 802.3 local area network extends through a gateway to OSINET.

Appendix 1 lists the milestones met in developing the laboratory.

Appendix 2 is a list of the guidelines for use of the OSI Security Laboratory proposed by NIST and agreed to by the SP4 vendors.

6. SP4 INTEROPERABILITY TESTING

6.1 Establishing the SP4 Laboratory

IBM, Hughes Aircraft Company and Digital Equipment Corporation (SDNS contractors for SP4) agreed to provide NIST with the following:

- A duplicate of the prototype SP4 development system that was being used for Phase IA of the SDNS project.
- Copies of the software and source code being used for its implementation.
- A commitment of time from a person or persons knowledgeable of the implementation (hardware and software) to participate in defining the interoperability demonstration, modify the software to perform the demonstrations, and assist NIST in performing the initial demonstrations.

A fourth company, Sun Microsystems Inc., (not an SDNS contractor) provided NIST with a model 3/280 micro computer system and source code for the SunLink OSI software. Throughout this project Sun Microsystems has furnished technical support as well as upgrades to their software products when new releases were issued.

NIST engineers installed the cabling required for an IEEE 802.3 bus utilizing Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the access method. This local area network (LAN) was configured as a subnetwork of the main computer network spanning the NIST campus.

Two Sun computers, a model 3/280 on loan from the company and a model 3/50 Workstation owned by NIST were the first machines connected to the laboratory subnetwork. The 3/280 was delivered with two 575 megabyte disk drives, a 10 1/2 inch magnetic tape drive, and a color monitor. This computer was configured as the gateway between the laboratory subnetwork and the NIST network.

Sun provided NIST with version 3.5 of the Sun Operating System and version 5.2 of the SunLink OSI Source Code. Under the software licensing agreement Sun Microsystems had approved a NIST request that it be permitted to modify the OSI code to include Transport Layer security.

Two IBM RISC Technology Personal Computers (RT/PC) were delivered to NIST in November 1988. Engineers from IBM assisted NIST personnel in installing the units and connecting them to the 802.3 subnetwork in the laboratory. Documentation needed to operate the PC's and run the SP4 demonstration test scripts was furnished by IBM.

In January 1989 Digital Equipment Corporation and Hughes Aircraft Company provided computer hardware, software and documentation required to demonstrate their versions of the SP4 protocols. Shortly thereafter, all three vendors met with NIST engineers to begin the process of demonstrating interoperability.

7. VENDOR IMPLEMENTATIONS OF SP4

Three vendors, Digital, IBM, and Hughes agreed to participate in the NIST SP4 Interoperability Project. A brief description of each vendor's prototype implementation follows.

7.1 IBM SP4 Implementation - Description and Features

The IBM implementation of SP4 was developed as part of the IBM-funded ARGO project at the University of Wisconsin. The overall objective of the ARGO project was to implement a suite of computer networking software based on the international standards for Open System Interconnection. The software was designed to run on an IBM RT/PC model 125 computer workstation using a version of the 4.3 BSD Unix operating system. The IBM SP4 prototype developed as part of the ARGO project incorporates part of the set of SDNS standards and protocols designed to provide secure communications in an OSI environment.

The subset of SP4 features implemented in the IBM RT/PC's includes:

- SP4-C
- Full-software implementation of SP4
- Full OSI stacks
- XOR cryptography
- OSI over TCP addressing
- Access control mechanism
- Security parameter negotiation
- Simulations of certain malicious attacks

The Key Management Protocol (KMP) services related to the exchange of credentials and the traffic encryption key attributes were implemented by IBM. However, those services that required the existence of a Key Management Center (KMC), such as retrieval of the Compromised Key List, were not implemented. Instead, stub interfaces to those portions of the protocol were provided.

The transport layer on which the IBM SP4 prototype is based contains the connection-oriented transport service. Within the connection-oriented transport entity, only classes 0 and 4 of the ISO transport protocol are implemented. The IBM prototype implements the Security Encapsulation function, the Data Encipherment function (confidentiality), the Integrity function (unique sequence numbers, final sequence numbers, direction indication), the Security Label function (single security labels only) and the Security Padding function.

In the IBM prototype a simple key creation device is simulated by software. A data base for the storage of traffic encryption keys is also implemented.

Access control is provided by the IBM system. Whenever access control decisions are necessary, a stub procedure, which queries an operator for a yes or no decision is used. The access control functions supported in this way include:

- The determination of security options, permissible security levels, security labels, and traffic encryption key attributes proposed by the initiator of a cryptographic association between two SDNS users;
- The selection of the same items by the responder of a cryptographic association between two SDNS users.

The security options sets supported by the IBM prototype are:

- Confidentiality
- Integrity
- Confidentiality and integrity

For these option sets key granularity per-transport-connection or per end system can be selected. The cryptographic algorithm provided by the IBM prototype is a "exclusive OR" (XOR) function.

7.2 Digital Equipment Corporation SP4 Implementation - Description and Features

Digital's SP4 prototype implementation was created by modifying an existing product called a Digital Ethernet Secure Network Controller (DESNC). These controllers are external encryption devices. A standard DESNC performs DES (FIPS PUB46-1) encryption at layer 2. The modified DESNCs implement SP4-E connectionless security services and incorporate a procedure to negotiate cryptographic associations. At least one VAX Station node is required to control the security devices on the LAN.

The controlling VAX node contains a database with information about the encryption devices and the network configuration. It contains the names of the encryption devices, their network addresses, date of modification, the name of the firmware image being run, and the type of audit conducted. The information in the database is loaded into the devices to control their operation and set alarms to flag relevant events. A system administrator can review information in the database and reports from the DESNCs to detect unauthorized modification.

A DESNC can be used to furnish security services to non-Digital hosts as well. In the OSI Security Laboratory, a DESNC is used to provide transparent OSI security services to a Sun model 3/50 workstation. Because the DESNC is able to distinguish between OSI and non-OSI data packets, it can encrypt OSI data without interfering with any other network traffic.

SP4 features implemented by Digital in their prototype device include:

- SP4-E
- External device controlled by a Vax node on the LAN
- Hardware DES cryptography
- Messaging application on top of TP4
- OSINET addressing
- Peer address checking
- Simple key management scheme

7.3 Hughes Aircraft Company SP4 Implementation - Description and Features

The Hughes prototype SP4 device is implemented as an embedded intelligent communications controller capable of being installed in a variety of workstations. The prototype used in the OSI Security Laboratory is installed in a model 286 Personal Computer.

The embedded intelligent communications controller card performs all the communications protocol processing as well as providing a hardware implemented cryptographic function, ie. DES.

The controller board consists of an 80286 microprocessor running in protected mode, 512K bytes of DRAM, a subnetwork interface (IEEE 802.3 or ethernet in the current version) and an embedded cryptographic device. A multi-tasking real-time protected mode operating system is provided for the board. Under this operating system, protocol and cryptographic software functions can be implemented as individual tasks which enforce process isolation.

The Hughes prototype SP4 device is based on version 1.2 (dated 07/12/88) of the SP4 specification and implements the SP4-E option.

The following features of the SP4 security protocols are also implemented:

- SP4-E
- On-board hardware card with dedicated 80286 microprocessor operating in protected mode, DES hardware, and IEEE 802.3 implementation
- Messaging application on top of TP4
- OSINET addressing
- Peer address checking
- Simple key management scheme

The data encipherment function chosen for the Hughes prototype SP4 device is the DES algorithm. Process isolation keeps the actual key value out of user process space.

The Hughes prototype SP4 device implements a Key Management Protocol. This protocol allows for an electronic key management in which the two end-systems desiring to communicate first authenticate themselves to each other. Both create the same pairwise traffic encryption key, and then negotiate the security services that they will use on information protected using that key.

8. RESULTS OF LABORATORY TESTING OF SP4 PROTOTYPES

8.1 SP4 Interoperability Demonstration

In the OSI Security Laboratory the feasibility of secure OSI was demonstrated by using SP4. Digital, IBM, and Hughes each chose a different method for implementing the SP4 protocols. IBM selected a software approach. The DESNC device used by Digital is hardware. Hughes' technique involved both hardware and software. The variety in approaches clearly demonstrated the implementation independence and flexibility of the SP4 protocol specification.

The focus of the SP4 interoperability demonstration was on providing integrity and confidentiality security services over an unprotected network. Related issues, such as key management and cryptography, though very important with respect to achieving interoperability, are not covered in the SP4 specification, but in other SDNS documents.

8.2 Hughes/Digital Interoperability Demonstration

Interoperability of the Hughes and Digital implementations of SP4 was achieved in the OSI Security Laboratory. Both systems use the OSINET addressing scheme specified in the GOSIP agreements, the same protocol exchange to obtain keys, support integrity and confidentiality services using the Data Encryption Standard (DES) in the Cipher Block Chain Mode, and the SP4-E option of the standard.

Digital and Hughes implemented the first three layers of the OSI architecture stack plus SP4 and Transport Class 4 (TP4). An application for message handling was provided directly on top of TP4.

8.3 IBM Interoperability Demonstration

IBM implemented all seven layers of the OSI model in software. They chose to use the SP4-C option of the specification. A stub procedure was used to provide access control and service negotiation security. The application programs provided by IBM run in the X-Windows environment.

It was not possible to achieve interoperability between the IBM and either the Digital or Hughes versions of SP4 for several reasons. IBM based its implementation on an earlier version of the SP4 specification. IBM's addressing scheme uses OSI over TCP (Transport Control Protocol) rather than OSINET addressing. Other differences are with the Key Management Application and the cryptographic algorithm used. For demonstration purposes IBM used an XOR function rather than the DES algorithm used by the other two vendors.

8.4 Alignment of SP4 Implementations

In June 1989, NIST and the vendors met to identify how each of the three SP4 implementations mapped onto version 1.2 of the SP4 specification document. Issues that prevented interoperability, recommended changes to each vendor's prototype to achieve alignment and alternatives were outlined. Because this effort was beyond the scope of work originally agreed to, the vendors were not able to commit the resources required to make modifications to their SP4 implementations. Since a strategy leading to interoperability of the Digital, Hughes and IBM implementations has been developed, NIST has encouraged the vendors to complete this objective during the 1990 fiscal year and has offered continuing laboratory support.

9. CONCLUSIONS

The OSI Security Laboratory has proven to be successful as a resource where interested researchers from government, and industry, can experiment with new ideas in network security, try new approaches for common problems, and develop new solutions. The laboratory provided a neutral working environment that fostered cooperation among the three vendors and ensured the integrity of the experiment. The vendors, Digital Equipment Corporation, IBM, and Hughes Aircraft Company are currently using the laboratory to test and demonstrate a subset of the Transport Layer security protocols (SP4).

Interoperability of the Hughes and Digital SP4 implementations has been achieved. IBM's SP4 prototype was designed using an earlier version of the specification. NSCL has proposed that all three vendors align their prototypes with the most recent version of the SP4 document as the approach for achieving interoperability.

The laboratory exercise, with actual implementations of SP4, has assisted NIST in its efforts to advance this technology in the voluntary standards community. Through its involvement in national and international standards organizations, NIST assisted the X3S3.3 committee of the American National Standards Institute (ANSI) adopt the SP4 specification as a New Work Item. It is felt that this process will lead to base standards in security that can be brought into the GOSIP arena for approval as stable implementors agreements.

The National Security Agency (NSA) has released the SP4 specification for public review. Additional SDNS documents have also been released. Through its partnership with NSA, NIST will review these protocol documents and where appropriate take the necessary action to have them adopted as Federal Information Processing Standards (FIPS).

Although current efforts in the OSI Security Laboratory focus on Transport Layer security, it is possible that future work will involve Network Layer security (SP3), and Integrated Services Digital Networks (ISDN) security. Preliminary discussions have been held with vendors who have expressed an interest in implementing SP3. ISDN activities may result in the establishment of a joint OSI/ISDN security laboratory. Work in the areas of key management and labels is also proposed.

10. FUTURE SP4 EFFORTS

10.1 NIST SP4 Reference Implementation and Conformance Test Methodology

One of the objectives of NIST's work in Transport Layer security is to develop an SP4 reference implementation. A Formal Description Language (FDL) such as Estelle has been proposed for the development of this reference implementation

To assist in this work, a Sun model 3/260 computer system has been purchased. This computer features a 327 megabyte disk drive, a 1/4 inch cartridge tape drive and color monitor.

The development and implementation of a conformance test methodology for SP4 security devices complement this work. Conformance tests of computer products help validate a manufacturer's claim that a product conforms to a standard. For users, conformance testing reduces risks and uncertainties associated with efforts to link products of different manufacturers. A conformance test methodology provides vendors with the incentive needed to accelerate the development and marketing of a product.

NIST's conformance testing methodology will provide procedures for accrediting testing facilities to conduct follow-on work. Documentation will be provided that will permit other organizations and laboratories to perform SP4 protocol conformance tests in an automated fashion.

LIST OF ABBREVIATIONS

ANSI	American National Standards Institute
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DES	Data Encryption Standard
DESNC	Digital Ethernet Secure Network Controller
DIGITAL	Digital Equipment Corporation
E-MAIL	Electronic Mail
FIPS	Federal Information Processing Standard
FDL	Formal Description Language
GOSIP	Government Open Systems Interconnection Profile
HUGHES	Hughes Aircraft Company
IEEE	Institute of Electrical and Electronics Engineers, Inc.
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
KMC	Key Management Center
LAN	Local Area Network
NIST	National Institute of Standards and Technology
NCSL	National Computer Systems Laboratory
NSA	National Security Agency
OSI	Open Systems Interconnection
SDNS	Secure Data Network System
SP2	Security Protocol - Layer 2
SP3	Security Protocol - Layer 3
SP4	Security Protocol - Layer 4
SP4-C	Security at Layer 4 per Transport Connection
SP4-E	Security at Layer 4 End System to End System
TP4	Transport Class 4

REFERENCES

SDN.401	SDNS Secure Data Network Systems - Security Protocol 4 (SP4); Revision 1.2, 1988-07-12
FIPS PUB146	Federal Information Processing Standards Publication 146, Government Open Systems Interconnection Profile (GOSIP), August 24, 1988
FIPS PUB46-1	Federal Information Processing Standards Publication 46-1, Data Encryption Standard, Reaffirmed January 22, 1988
EK-DESNC-UG-001	DESNC Installation/User's guide - Digital Equipment Corp., Maynard, MA.
ISO7498	Information Processing Systems - Open Systems Interconnection - Security Architecture (Part 2)
ISO8073	Information Processing Systems - Open Systems Interconnection - Connection Oriented Transport Protocol Specification - Addendum 2: Class Four Operation Over Connectionless Network Service
ISO8602	Information Processing System - Open Systems Interconnection -Protocol for Providing the Connectionless - Mode Transport Service
ISO802.3	ANSI/IEEE Standard Draft International Standard - Carrier Sense Multiple Access with Collision Detection

APPENDIX 1 OSI SECURITY LABORATORY MILESTONES

As one of its milestones in support of the SDNS project, the National Computer Systems Laboratory (NCSL) of NIST undertook the development of an OSI Security Laboratory in FY88. The purpose of the laboratory is to permit engineers and computer scientists from NIST and participating vendors to:

- Develop security protocols for computer network security
- Develop a demonstration system showing interoperability of devices implementing the Security Protocol at Layer 4 (SP4)
- Develop and conduct conformance tests for SP4

Planning for the OSI Security Laboratory was begun in October 1987 following approval to renovate two adjoining chemical laboratories in the Technology Building. Physical and electrical layouts were developed by NIST engineers. The plans were approved in November and the extensive work required to remodel the area was begun in January 1988. This phase of the work was completed in March 1988. Engineers from NIST coordinated these activities. The work was accomplished by technicians from the NIST Plant Division and included:

- Removal of all chemical laboratory services including hot/cold water, gas burners, and other miscellaneous equipment
- Removal of fume hood and cabinets
- Removal of the partitions separating the two rooms to permit conversion to a double module laboratory
- Installation of additional lighting
- Site security provided by installation of cipher lock and heat and smoke sensors
- Installation of electrical raceway and receptacles
- HVAC renovation
- Painting of entire laboratory space

While renovation work was underway a contract was issued for installation of a raised floor system, carpeting, and an entrance ramp. The renovation work in the laboratory space, including the raised floor, was completed on April 30, 1988.

A layout for computers and workstations for the laboratory was developed by NIST engineers. Meetings were held with representatives of four suppliers of computer furniture to discuss requirements and estimated costs.

Final installation of the furniture and telecommunications center was completed in August 1988. Lines for three phones were also installed that same month.

Following completion of all renovation work, a Sun model 3/50 workstation was installed in the laboratory. Additional computer equipment installed on the 802.3 LAN in the OSI Security Laboratory includes:

- Sun model 3/280 system - to be used for monitoring data packets during interoperability tests
- Sun model 3/260 system - to be used for developing the NIST SP4 reference implementation
- Two IBM PC/RT's
- Digital VAX station and two DESNC encryption boxes
- Hughes Aircraft Company SP4 implementation using an IBM PC

APPENDIX 2 OSI SECURITY LAB GUIDELINES

1) All documentation, software, and hardware used in the lab will be unclassified.

2) All NIST personnel who receive any proprietary products must, before their receipt, be informed of the proprietary nature of the product.

3) NIST will provide reasonable protection for all proprietary information, hardware, software, and documentation including locked storage cabinets and a Cipher lock on the door of the lab.

4) Hardware loaned to NIST will be afforded reasonable protection against theft, damage, and destruction. Maintenance of the equipment will be provided by the vendors in accordance with the vendor agreements.

5) Equipment provided by the vendors will be used in interoperability demonstrations conducted in the Security Lab. Equipment will be demonstrated only with permission of the vendor.

6) Failures that occur during the interoperability demonstrations will not be disclosed to other than the technical representatives of the vendor of the device being demonstrated.

7) NIST will destroy any proprietary software stored in any CPU or other storage medium which cannot be returned to the vendor after completion of the demonstrations.

APPENDIX 3 NIST SP4 DEMONSTRATION AGREEMENTS
VERSION 1.8 (11/18/88)

PHASE 1 - Demonstrations without security
PHASE 2 - Demonstrations with minimum intersection subset
PHASE 3 - Demonstrations with full connection capability

A. ALGORITHMS

ISSUES	ALTERNATIVES	SELECTED PARAMETERS	SELECTED BY NIST DEC,IBM,HAC, ALL
A1. Certificate generation	A. Manually generated, fixed format [32] (Backus-Naur method)	A	ALL
A2. Traffic key generation	A. TEK ::= (RNI [8] XOR RNR [8])	A	ALL
A3. Data encryption	A. CBC with E ::= XOR W/TEK B. CBC with E ::= DES	A B	NIST, IBM, HAC DEC, HAC, NIST
A4. MAC (not used in Phase 2)	A. MAC ::= XOR (Di,IV, MAC-K) B. ANSI X9.9 (FIPS 113) C. MAC ::= 0 [64]	A	NIST, IBM
A5. MDC	A. MDC ::= XOR (Di) B. XOR (Do) ¦¦ XOR (De)	A	ALL
A6. MAC key generation	A. Complement even bits of traffic key (TEK) B. None	B	ALL
A7. MI generation	A. Random no. [8]	A	ALL
A8. Encryption mode	A. CBC	A	ALL

B. SERVICES

ISSUES	ALTERNATIVES	SELECTED PARAMETERS	SELECTED BY NIST DEC,IBM,HAC, ALL
B1. **Access control**	A. Incoming and outgoing	A	NIST, IBM
	B. Incoming only		
	C. None	C	DEC
B2. **Key Transfer**			
B2.1 NKRQ; NKRS	A. Subset as agreed	A	ALL
	B. Full SDNS		
B2.2 SSRQ; SSRS	A. Subset as agreed	A	ALL
	B. Full SDNS		
B2.3 KMP to KMC	A. None	A	ALL
B2.4 Staged rekey	A. None	A	ALL
B2.5 Key update	A. None	A	ALL
B2.6 CKL support	A. None	A	ALL
	B. DOD label -see cert.		
B3. **Data Protection**			
B3.1 Base services	A. Any combination of C, I (negotiated)	A	
	B. Same as A. plus no security on other connection		
	C. C & I only; no label	C	ALL
B3.2 Expedited data (ED) (connection keying only)	A. Terminate connection when ED SN's wrap	A	NIST, IBM
	B. N/A	B	DEC, HAC
B3.3 Order of C and I	A. E (MDC (PT))	A	ALL

ISSUES	ALTERNATIVES	SELECTED PARAMETERS	SELECTED BY NIST DEC,IBM,HAC, ALL
B4. **Error Handling**			
B4.1 Detected errors	A. Access permission failures (I & O) Certificate failures (I) MDC failures (I) MAC failures (I) FSN failures (I) SN repeated failures (I) Unencapsulated TPDU on secure connection Incorrect Direction Indicator (I) Security Label failures (I) KMAE failures	A	NIST, IBM
	B. Local Handling	B	ALL
B4.2 Printed errors	A. Print upon operator request	A	NIST, IBM
	B. Console/File alarm/ audit	B	DEC
	C. Local Handling	C	ALL

C. PROTOCOLS

ISSUES	ALTERNATIVES	SELECTED PARAMETERS	SELECTED BY NIST DEC,IBM,HAC, ALL
C1. **Physical**	A. IEEE 802.3 B. Ethernet C. Vertix	A	ALL
C2. **Data link**	A. IEEE 802.2, 802.3 B. Ethernet	A	ALL
C3. **Network**	A. CLNP B. Inactive subset C. No fragmenting D. NSAP address - use GOSIP E. CLNP padding	A B C D E	DEC, HAC, IBM DEC ALL ALL DEC
C4. **Transport**			
C4.1 User stack	A. SP4 (STE) B. SP4 with security bypass (Only used by KMAE) C. SP4 and TP4	B	IBM
C4.2 Security stack	A. TP4 B. SP4 with security bypass	B	IBM
C5. **Session**			
C5.1 User stack	A. None B. Kernel	A	DEC, HAC
C5.2 Security stack	A. Kernel B. None	B	DEC, HAC
C6. **Presentation**			
C6.1 User stack	A. None B. Presentation Kernel	A	DEC, HAC
C6.2 Security stack	A. Presentation Kernel B. None	B	DEC, HAC
C7. **Application**			
C7.1 User stack	A. NBS demo; ACSE B. NBS demo; None	B	DEC
C7.2 Security Stack	A. KMS; ACSE		

D. SDNS SP4 OPTIONS (See SDN.401)

ISSUES	ALTERNATIVES	SELECTED PARAMETERS	SELECTED BY NIST DEC,IBM,HAC, ALL
D1. Transport security granularity	A. SP4C (connection oriented)	A	
	B. SP4E (end to end)	B	DEC, HAC
	C. Both	C	NBS, IBM

E. SECURITY PDU's USED

E1.1 Exchange credentials
1) NKRQ (INIT-KID, UNIV-ID, INIT-CRED)
2) NKRS (INIT-KID, RESP-KID, RESP-CRED)
Note: If using DES, set parity to odd. The DES parity bit is the LSB of each octet. UNIV-ID ::= 1; KID ::= per KMP spec

E1.2 Attribute negotiation
1) SSRQ (RESP-KID, MI, OPT-SET, MDC) - encrypted using DES
2) SSRS (INIT-KID, MI, OPT-SET, MDC) -
Note: Only IBM can send an ESTAT; if one is received it should be ignored

E1.3 Data Transfer
1) SE-TPDU (LI, SE, KID, MI, LI, FLAGS,
{ PAD }, TPDU, MDC)
KID - 4 bytes; FLAGS - 1 byte ("01" or "00")
MI - 8 bytes; LI - 1 byte
SE - 1 byte ("48")
{ } means present if needed
PAD - multiple of 8 octets for [MI .... MDC]

Format of a certificate ::= Type ";" Org";" UserID ";" Classification ";" TermDate Blank "."

The certificate is 32, 7 bit ASCII characters. Add blanks before the final period if required to get 32 characters.

```
Type ::= "1" ¦ "2" ¦ "3" ¦ "4"    (DES - 3; XOR - 4)
Org ::= "NIST" ¦ "IBM" ¦ "HAC" ¦ "DEC"
UserID ::= Letter ¦ Userid Letter
Classification ::= "U" ¦ "C" ¦ "S" ¦ "T"
TermDate ::= Year Month Day
Year ::= "88" ¦ "89"
Month ::= "01" ¦ ... ¦ "12"
Day ::= "01" ¦ ... ¦ "31"
Letter ::= "A" ¦ ... ¦ "Z"
Blank ::= "b" ¦ NULL ¦ Blank "b"
```

example: 3;NBS;Branstad;U;891231bbbbbbbb.
To form a credential concatenate the certificate with a 64 bit binary random number; left most bit is MSB, right most bit is LSB

KMP Error Conditions

1. Failure in creation of a Key - Abort -> Idle
2. Bad clear text field - AAbort -> Idle
3. Bad description or MDC - AAbort -> Idle
4. Service not provided { CKL not included
   { Estat -> Release -> Idle
5. Bad value in Protected field (Protocol violation) - Estat -> Release -> Idle
6. Negotiation failure - Estat -> Release -> Idle
7. Service not available at this time - Estat -> Release -> Idle
8. Access control failure - AAbort -> Idle

NBS-114A (REV. 2-8C)

U.S. DEPT. OF COMM. **BIBLIOGRAPHIC DATA SHEET** *(See instructions)*	1. PUBLICATION OR REPORT NO. NISTIR 90-4228	2. Performing Organ. Report No.	3. Publication Date JANUARY 1990

4. TITLE AND SUBTITLE

Prototyping SP4
A Secure Data Network System Transport Protocol
Interoperability Demonstration Project

5. AUTHOR(S)

Charles R. Dinkel, Noel A. Nazario, Robert Rosenthal

6. PERFORMING ORGANIZATION *(If joint or other than NBS, see instructions)*

NATIONAL BUREAU OF STANDARDS
U.S. DEPARTMENT OF COMMERCE
GAITHERSBURG, MD 20899

7. Contract/Grant No.

8. Type of Report & Period Covered

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS *(Street, City, State, ZIP)*

National Security Agency - Information Security Applications Group
9800 Savage Rd., SDNS SPO (C23)
Fort Meade, MD 20755-6000

10. SUPPLEMENTARY NOTES

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)*

The Secure Data Network System project, known as SDNS, implements computer to computer communications security for distributed applications. The internationally accepted Open Systems Interconnection (OSI) computer networking architecture provides the framework for SDNS. SDNS utilizes the layering principles of OSI to implement secure data transfers between computer nodes of local area and wide area networks. SDNS implements SP4, a security protocol at the OSI Transport layer (layer 4) that provides end-to-end reliable transparent data communications with confidentiality and integrity security services. Laboratory prototypes of SP4 formed the basis of proposed voluntary national standards and will form the basis for future security enhancements to existing Government Open Systems Interconnection Profiles (GOSIP).

12. KEY WORDS *(Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)*

Computer security; conformance testing; local area networks (LAN); network security; protocol security; SDNS; transport protocols

13. AVAILABILITY

☒ Unlimited
☐ For Official Distribution. Do Not Release to NTIS
☐ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.
☒ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES 39

15. Price A03

USCOMM-DC 6043-P80