NISTIR 5325

Conformance Assessment of Transport Layer Security Implementations

Wayne A. Jansen
Editor

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

NIST

NISTIR 5325

Conformance Assessment of Transport Layer Security Implementations

Wayne A. Jansen
Editor

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

December 1993

U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary

TECHNOLOGY ADMINISTRATION
Mary L. Good, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arati Prabhakar, Director

ABSTRACT

This paper presents a framework for evaluating conformance of a protocol implementation to the Security Protocol at layer 4 (SP4) standard. SP4 is one element of the Secure Data Network System (SDNS) architecture, used to provide security services at the Transport layer of the Open System Interconnection (OSI) reference model. SP4 also forms the basis of the ISO standard for the OSI Transport Layer Security Protocol (TLSP). Therefore, with few exceptions, the findings of the paper are applicable to TLSP. The paper explores the relationship between conformance assessment, interoperability assessment, and security evaluation of security protocols. The OSI conformance testing methodology and framework is reviewed, and a strategy is given for applying this methodology to SP4 implementations.

Keywords: OSI, Lower Layer Security Protocols, Conformance Testing, Security Evaluation, Interoperability Testing, SP4.

TABLE OF CONTENTS

1. INTRODUCTION

The Secure Data Network System (SDNS) [5] program began in August of 1986 through the sponsorship of the National Security Agency (NSA). The goal of the program is to establish a communications architecture and protocols for protecting both unclassified and classified computer networks, within an internationally recognized framework. Security Protocol 4 (SP4) [3,4] is one element of the SDNS, designed to provide security services at layer 4, the Transport layer, of the International Organization for Standardization (ISO) reference model for Open Systems Interconnection (OSI) [1].

The SP4 standard builds upon the services of either the connectionless or connection oriented Transport layer protocol. It should be viewed as an extension to those protocol standards, rather than as an independent layer protocol. In the OSI architecture, the Transport layer has the sole responsibility to provide reliable end-to-end communications between peer end-systems. SP4 services, therefore, nicely complement those provided by Transport protocols. SP4 functionality is situated near the bottom of the Transport layer and consists of a simple encapsulation/decapsulation mechanism that protects Transport protocol data units within a cryptographically secure envelope. SP4 extends the OSI Transport connectionless and connection oriented services to provide or support the following security services defined in the OSI Security Architecture addendum to the reference model [2]:

(1) Data Integrity,

(2) Data Confidentiality,

(3) Data Origination Authentication, and

(4) Access Control.

The SP4 standard identifies other security functions on which it depends. These functions include key management, security management, and cryptography. Key management is needed to establish and maintain keying material used by SP4; security management is needed for event reporting and auditing; and cryptography (i.e., employment of specific cryptographic algorithms) is needed to support Data Integrity, Data Confidentiality, and Authentication services. These functions are normally collocated in an end-system, with an SP4 entity.

This paper investigates the conformance assessment of an SP4 implementation and the implications of such a procedure. Since SP4 is compliant with the OSI reference model and security architecture, emphasis is placed on the OSI conformance testing methodology [9]. Two other related assessment methods, interoperability assessment and

security evaluation, are also reviewed. Like conformance assessment, both are concerned with the correctness of an implementation, albeit from different perspectives.

An implicit assumption made throughout this paper is that for an SP4 implementation to be trustworthy, the SP4 layer protocol entity must be part of the Trusted Computing Base (TCB) [15] for a distributed system. Figure 1 illustrates this view of SP4. A TCB refers to the combination of protection mechanisms within a computer system responsible for enforcing a security policy. In a distributed network environment, this is referred to as a Network Trusted Computing Base (NTCB) [13].

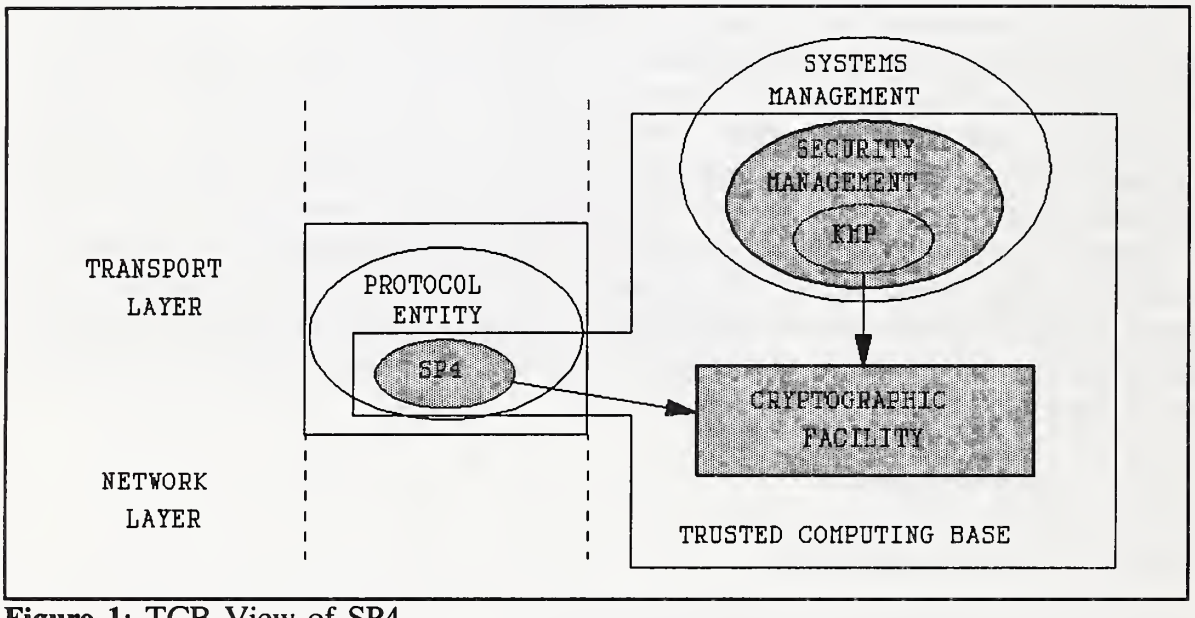

Figure 1: TCB View of SP4

The OSI Transport Layer Security Protocol (TLSP) [6] is a current ISO standard that provides security services similar to SP4. Since SP4 formed the foundation for TLSP, the two specifications are closely related. Therefore, most of the comments and conclusions in this paper apply equally to TLSP.

2. OVERVIEW OF ASSESSMENT

2.1 Conformance Assessment

Conformance assessment of OSI protocols is defined in a multi-part standard [9] that provides the basic framework and methodology for conformance testing. The scope of the standard ranges from abstract test suite specification and executable test derivation to the conformance assessment process, and includes test methods and a formal notation for describing test cases. The assessment procedure has two distinct parts: a static conformance review of the Protocol Implementation Conformance Statement (PICS) and dynamic conformance testing of the implementation.

The PICS defines, in a tabular form, the range of functionality (i.e., capabilities and options) afforded by an implementation. Product manufacturers are expected to provide PICS for their implementations according to the PICS proforma established by standardization groups for an OSI protocol. By reviewing the PICS, a determination can be made of whether or not the functionality provided by a product meets the conformance requirements. The PICS also can be used as a guide for selecting appropriate test cases against which to assess the conformance claims of an implementation. The methodology also requires a Protocol Implementation Extra Information for Testing (PIXIT) to identify additional information about an implementation to facilitate testing, such as address values, timers, and parameter settings.

Conformance testing for OSI is the process of verifying that the external behavior of an implemented data communications protocol agrees with the requirements specified in the defining standard. The OSI conformance testing methodology relies on a black box testing approach. That is, the internals of the box, or in this situation the protocol implementation under test, are unexaminable and unknown. How the protocol functionality is implemented is not part of the methodology. Instead, emphasis is placed on external behavior.

The external behavior of an OSI protocol implementation is observable through the protocol data units (PDUs) exchanged with a test system, and is the foundation for the design of test scenarios. OSI conformance test scenarios contain negative as well as positive tests. That is, test scenarios include test cases involving the use of invalid PDUs and otherwise inappropriate PDU behavior. Conformance testing can determine whether PDUs are correctly exchanged, services are correctly provided, options are correctly treated, errors are correctly handled, and events are correctly reported.

While conformance testing increases the probability that different implementations of a set of selected protocols will interwork properly, it is no guarantee of full interoperability, given the typically large number of protocol options and unconstrained parameters. Supplementary interoperability assessment is also required.

2.2 Interoperability Assessment

Similar to conformance assessment, the focus of interoperability assessment is testing. Interoperability testing is concerned with the end-to-end operation of one or more OSI implementations, exercising all services with various semantic values, and checking rendition and expected behavior. For example, in the case of messaging systems, the data content must be correctly relayed across several end-systems and correctly rendered to the recipients. Moreover, the distribution and handling within the end-system must behave as expected.

Although interoperability testing also uses a black box approach, it contrasts from conformance testing in several ways. Perhaps the most striking is the change from a test environment involving a validated test system and instrumented implementation, to an operational environment involving many different implementations as counterparts to the testing. Another significant difference is that the OSI conformance testing methodology is concerned primarily with evaluating a single layer or small group of layers, while interoperability testing involves the entire seven layer stack or, in the case of intermediate systems, the lower-level three-layer stack. Interoperability testing also emphasizes positive as opposed to negative testing, in contrast to conformance testing.

Interoperability testing alone is not a substitute for conformance testing. There always exists the danger of obtaining implementations that are interoperable with each other, but not necessarily conformant to the protocol standard. Because of the emphasis on positive testing, there is also the possibility that interoperability tests would not uncover some types of errors. Therefore, both types of testing are needed to preclude isolated islands of interoperable but non-conformant implementations.

At present, interoperability testing is not the subject of international standardization, due to a lack of broad consensus of a methodology and framework. Most interoperability testing is conducted on an ad hoc basis, to meet the demands of a particular situation. Implementations intended for a specific management domain may be subjected to interoperability tests as part of the requirement for membership. Many commercial implementations go through such a phase prior to and during vendor demonstrations at international trade shows and conferences. As demonstration software matures into products, reasonable product interoperability becomes the norm.

2.3 Security Evaluation

A security evaluation assesses products to determine the degree of trust that can be placed in them with regard to the secure processing of information. An evaluation is done without regard to the specific operational conditions and circumstances in which a product may be used (e.g., inside a shielded vault), but does take into consideration the

computer system operating environment. The objective of the security evaluation is to perform a technical assessment of the trust properties. Three general security issues that must be addressed are: the confidentiality of the data, the integrity of the data and the system, and the availability of service. The goal or main requirement is to assure that the system behaves according to an organization's security requirements that, in turn, reflect the defined security policy of the organization. To guarantee that this requirement is met, the security functionality of an implementation must work correctly and effectively.

Evaluations of commercial products in the U.S. are carried out through the Department of Defense (DoD) Trusted Product Evaluation Program (TPEP). The TPEP evaluates systems that meet the DoD's program objectives based on the criteria defined in the DoD TCSEC [7]. The TCSEC defines a hierarchy of classes that represent increasing levels of confidence in the trustworthiness of a computer system to protect information. The TCSEC identifies features to be evaluated, such as login, access controls, and audit; and assurances to be obtained, such as least privilege, testing, and documentation. Features are mechanisms that provide security functionality, while assurances indicate the degree of trust, and give a measure of the degree to which features work correctly and are effective.

In contrast to conformance and interoperability evaluation techniques, security evaluations are limited to only the security relevant portions of the system. However, an evaluation at higher levels of assurance may be extensive, especially if one considers the attention given such areas as covert channels. Furthermore, testing is only one aspect of a security evaluation. Other aspects include ensuring that the product is produced and distributed according to appropriate controls and standards, and ensuring that well documented procedures exist for the operational use of the product. The goal of an evaluator is to gain a deep understanding of a product and how it meets stated security objectives, not merely to determine whether it passes a set of predefined tests.

TCSEC evaluations are normally carried out in parallel with product development. Features (i.e., security mechanisms) not only must be operable and correct, but also must be implemented to resist tampering and leakage. From a testing perspective, assurance is gained through testing the implementation's security functionality and susceptibility to penetration. An evaluator has access to internal documentation and is involved in the product development cycle. Security evaluations under the TCSEC can be considered a form of white box testing, since the internals of the box can be observed and controlled, and specifications of the internal design are available for analysis. White box testing is typically more stringent than black box testing since it allows test case design to establish some measure of minimum execution coverage with respect to the structural properties of software and hardware under evaluation.

2.4 SP4 Characteristics

Several characteristics of the SP4 standard are important to note, since they have an effect on the various forms of assessment. They are:

(a) Absence of Assurance Requirements,

(b) Algorithm Independence,

(c) Optional Security Services, and

(d) Embedded Functionality.

Although concerned with the provision of security services through specific types of security mechanisms, the SP4 standard does not contain any requirements on the level of confidence in the security provided by an implementation of the protocol. That is, the SP4 standard is a functionality specification devoid of assurance requirements for the implementation and the operating environment. Therefore, an implementation may fully conform to the SP4 standard, yet be inherently insecure. For example, there are no guarantees that a system correctly implementing SP4 either employs algorithms with an appropriate strength of mechanism, or controls access to transmitted information once it resides in the system. The level of assurance provided by an SP4 implementation depends on factors outside the scope of the standard. That assurance can be gained only by evaluating the implementation according to an established set of criteria, such as the DoD Trusted Computer System Evaluation Criteria (TCSEC) [7] or Trusted Network Interpretation [15] of that criteria.

The SP4 standard is mechanism dependent, but algorithm independent. For example, the Data Confidentiality service is provided through an encipherment mechanism, but the underlying cryptographic algorithm is left open in the specification. Furthermore, an SP4 implementation may legitimately support only a subset of the optional elements indicated in the standard. To compensate for the openness and flexibility in the standard, implementors' groups are expected to develop security sub-profiles for generic applications. That is, the characteristics of the required security functionality must be stipulated before an implementation can be constructed.

A security sub-profile specifies the general security objectives and operating environment assumptions, a target range of assurance, and suites of protection algorithms, in addition to the set of security features selected from those offered by the protocol. Therefore, a protection profile not only tightens the functionality specification, but also supplements it with assurance requirements. Few examples of security sub-profiles exist. Probably the best known example is that done for Message Handling Systems based on the X.400 standard [10].

In practice, a fully capable SP4 implementation is an implementation of a Transport protocol with embedded SP4 functionality. Because of the dependency on the Transport protocol, conformance testing of SP4 implementations is expected to be tied closely to Transport layer conformance testing procedures. The next chapter discusses this in more detail. The implication of the dependency for a security evaluation is that both the SP4 and Transport layer protocol implementations would require evaluation.

2.5 Relationships between Approaches

Clearly, the objective and scope of the three categories of assessment are quite different. Conformance assessment is the most functionally precise, since it provides testing at the level of detail of the functional standard, on a protocol-by-protocol basis. Interoperability assessment is a bit broader since it concerns a group of layer protocols and their operational aspects, and seeks functional compatibility among many implementations. Security evaluation is somewhat orthogonal to both. In the case of SP4, it is broader in scope than conformance testing of a protocol entity, yet narrower than interoperability testing of an entire end-system. The target of a security evaluation, the trusted computing base, lies somewhere in between. Similarly, while the objective of a security evaluation goes beyond functionality and seeks adherence to assurance requirements, only the correctness and effectiveness of the implementation from a security perspective are of concern. Therefore, it is possible to successfully evaluate an SP4 implementation that lacks conformance to the standard and does not interoperate with other implementations.

Although OSI conformance testing does not directly address trust-related factors of an implementation, a successful conformance testing result suggests a level of assurance for the implementation. That result could be provided to a security evaluation to satisfy some portion of the functional testing requirements of the TCB. Since systems may be exploited through an external interface such as that provided by OSI, consideration could be given to incorporate extended functionality testing based on design information, and penetration testing with the conformance testing methodology. That is, contrary to the traditional view of separate conformance and security evaluations, conformance testing could be integrated into the security evaluation process and be made a part of the evaluation procedure for a distributed system that relies on a lower layer security protocol such as SP4.

One interesting difference between conformance and security evaluations is in the structure of the processes and the roles that the organizations play in them. The security evaluation of a product is normally done through a sponsoring governmental agency, includes product development as part of the process, is conducted at a secure government facility using procedures not completely disclosed to the public, and continues until the criteria level is met or the developer gives up. A conformance evaluation on the other

hand is normally initiated by the developer, is conducted after product development, is evaluated at a government accredited facility through publicly available test procedures, and renders a pass/fail verdict within a comparatively short period of time. Whereas the security evaluation process is centered around the concerns of the evaluation agency, the conformance evaluation process is oriented more toward the developer. In particular, the black box nature of conformance testing avoids disclosure of proprietary information by the developer.

Interoperability testing appears to logically fall after successful conformance and security evaluations take place. Ideally, a rigorous conformance testing campaign would limit the effort needed for interoperability testing, making it merely an exercise in system configuration and parameter determination. In this respect, interoperability testing is complimentary to both conformance testing and security evaluation.

3. SP4 CONFORMANCE TESTING

3.1 Strategy for Testing

This section applies the OSI Conformance Testing Methodology and Framework to SP4 and develops a consistent approach for conformance testing of an implementation, to meet the dynamic conformance conditions. The procedure is predicated on the following assumptions:

(a) Communication hardware/software products for OSI will provide an exposed interface (i.e., an external interface to the user) from the Transport layer protocol entity.

(b) Implementations of the SP4 protocol are not guaranteed to provide an exposed interface, and are most likely embedded within the Transport protocol entity.

(c) Based on its functionality, SP4 may be considered as the lowest sub-layer of the Transport layer protocol.

The implication of these assumptions is that an SP4 implementation must be tested indirectly, through the interface to the Transport protocol entity. The approach taken is to build upon extant testing requirements for the Government Open System Interconnection Profile (GOSIP) [12]. The abstract test method proposed for SP4 follows a coordinated single-layer embedded test method. This approach assumes that explicit test coordination procedures can be used with the Transport implementation containing and/or supporting SP4 functionality. Figure 2 illustrates this test method for SP4. The system under test must involve a Transport implementation whose normal non-security services have been successfully tested. Here the Transport protocol interface is used as the point of control and observation (PCO) for the upper tester, in lieu of an exposed SP4 interface. SP4 behavior is exercised and analyzed indirectly through the Transport interface. The PCO for the lower tester is the underlying Network service interface.

For the coordinated test method, the upper tester for the SP4 implementation under test (IUT) contains a test responder capable of processing a test management protocol (TMP) and performing the indicated actions on the IUT. The composition of the lower tester is a bit more complex. It must be capable of realizing Transport services by processing executable test scenarios, while maintaining a correspondence with the peer test responder of the upper tester. In addition, the lower tester can normally manipulate Transport PDU (TPDU) encodings for exception generation, and record messages concerning the progress of the test scenario and the detailed TPDU exchanges. From the latter information, a verdict analysis can be performed.

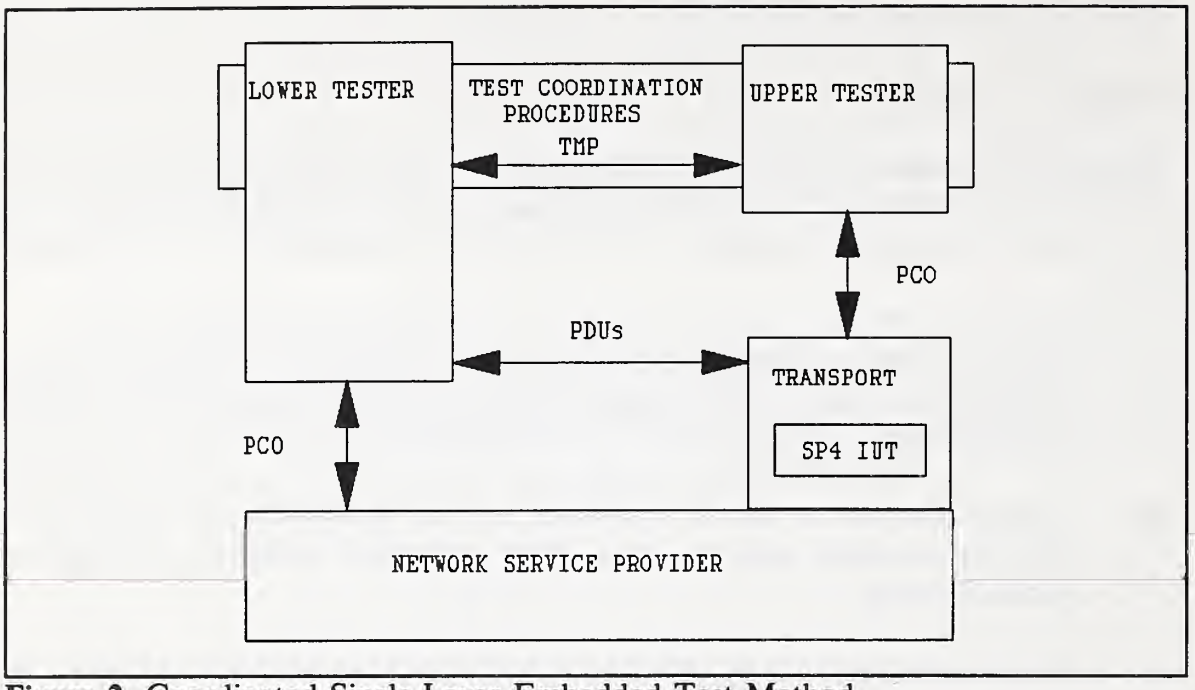

Figure 2: Coordinated Single-Layer Embedded Test Method

3.2 Other Testing Considerations

Other concerns about SP4 conformance testing that are related to security, include the following issues:

(a) Determination of the default cryptographic algorithms for testing,

(b) Key management support for establishing and maintaining traffic encryption keys,

(c) The control and selection of security services, and

(d) The method for collecting security event reports.

These and other such items should be addressed in the PIXIT supplied with the SP4 implementation to be tested.

The coordinated single-layer embedded (CSE) test method requires that the Transport protocol be tested as a prerequisite to testing the SP4 functionality. Similarly, the cryptographic facility that supports the protocol entity should complete successful independent testing to avoid confounding the conformance test results. Standard algorithm test suites would be useful in testing the cryptographic facility and for simplifying configuration of the test system.

Unlike other protocols, lower layer security protocols have the unique property of silence in situations where a security violation occurs. That is, rather than responding to the source of the offending PDU, a security event is reported and the offending PDU is discarded. This type of behavior complicates verdict determination, since the verdict is dependent on the security event reporting function for the system under test. Realization of the CSE test method, therefore, may require shifting some of the responsibility for verdict determination onto the upper tester.

3.3 Characteristics of the Means of Testing

The realization of an abstract test method includes the test system, executable test suite, testing support tools, and documentation. The following items, drawn from the GOSIP conformance testing technical criteria [12], summarize the significant characteristics of the means of testing needed for the coordinated test method proposed:

(a) Capability to analyze PICS and PIXIT for the IUT and to select and parameterize tests to be run, and to configure the means of testing for communication with the System Under Test (SUT);

(b) Procedures to reconcile PDU and test data with the test purposes and yield a verdict for each test purpose;

(c) Capability to produce Conformance Test Reports, listing test cases executed and their verdicts, and detailing the IUT behavior in cases of failure;

(d) Capability to record the protocol data units exchanged with the IUT in a conformance log, and to review the structure and encoding of protocol data units after the test campaign is complete;

(e) Capability to assemble SE TPDUs according to the SP4 standard, and send them to an end-system under test over any supported medium;

(f) Capability to receive and disassemble SE TPDUs according to the SP4 standard, to validate the SE TPDUs received, and to record the results;

(g) Capability to construct invalid as well as valid SE TPDUs;

(h) Capability to monitor and to initiate SE TPDU exchanges with the SUT, and to record the results; and

(i) Capability to control and coordinate the SUT, in order to induce the SUT to generate specified types of SE TPDUs, including control and coordination with the Transport entity associated with the SP4 IUT.

4. ORGANIZATION AND PRODUCTION OF TEST SCENARIOS

4.1 Existing Transport Test Scenarios

Within the U.S. Federal Government, the Government OSI Profile (GOSIP) [11] is the procurement specification for agencies to use when acquiring open systems computer network products. GOSIP conformance testing procedures [12] have been established that follow the OSI conformance testing methodology. At the Transport layer, GOSIP mandates class 4 Transport for interoperability among compliant systems. The remaining classes have a less essential role in the specification, as does the connectionless Transport protocol. For this reason, and because class 4 functionality encompasses that of the other classes, only class 4 test cases are considered in the discussion that follows.

The abstract test cases for the class 4 Transport protocol fall into one of three categories of increasing complexity and functionality: basic interconnection tests, capability tests, and behavior tests. Basic interconnection tests establish a baseline capability and determine the ability of the implementation to open and close connections, and convey normal user data, and parameters. Capability tests continue to examine fully all mandatory capabilities and determine whether the implementation can convey expedited data, and more extensive amounts of normal user data. Behavior tests establish the extent to which the dynamic conformance requirements are met and examine the ability of the implementation to negotiate parameters, to be involved in more complicated exchanges, and to handle the full range of error conditions.

4.2 Proposed SP4 Test Scenarios

GOSIP test scenarios for class 4 Transport are not capable of providing insight into an SP4 IUT, other than to establish that fundamental communications capabilities are in good order. Furthermore, the behavior tests are no longer appropriate since they do not address the specific services offered by SP4. These security services are embodied in the security encapsulation (SE) TPDU, used exclusively by the SP4 protocol. None of the error conditions associated with the SE TPDU are part of the existing behavior tests.

The SP4 PICS proforma [8] suggests areas that should be included in the test suite coverage. Note that some areas may overlap with others since they may be merely different views of the same functionality. Tests should exist for the following areas:

(a) Acceptable General Behavior

- ability to generate valid SE TPDUs
- ability to accept valid SE TPDUs
- ability to handle SE TPDUs in error
- ability to handle network failure

- ability to handle inopportune SE TPDUs

(b) SE TPDU Parameter Encoding/Decoding

- key identifier
- protected header flag
- label
- pad
- final sequence number
- integrity check value

(c) Specific Functions

- peer address verification
- reflection detection
- separation after decapsulation
- secure multiplexing
- security encapsulation
- security event reporting
- data encipherment
- integrity protection
- integrity sequence numbering
- pre-encapsulation concatenation
- padding
- explicit security labeling
- final sequence number checking

(d) Security Error Conditions

- improperly protected TPDU
- invalid key identifier
- invalid integrity check value
- invalid direction indicator
- improper label
- improper pad
- duplicate sequence number
- invalid peer address
- invalid final sequence number
- invalid destination address

(e) Protocol Error Conditions

- undefined parameter
- out-of-sequence parameter
- unexpected final sequence number

The test coverage areas give guidelines for test case development that need to be further specified and organized into test categories. The details of test specifications are left to the designer of abstract test scenarios for SP4.

5. SUMMARY

This paper explores the relationship between conformance assessment, interoperablity assessment and security evaluation of a typical lower layer security protocol, SP4. These categories of evaluation overlap somewhat with regard to the correctness of security functionality, but differ in their scope and objectives. The following points are made toward determining the role and method of SP4 conformance testing:

(a) Conformance testing, interoperability testing, and security evaluation are independent activities that may be applied at various times during the life cycle of a product.

(b) Conformance testing is a complementary and useful step toward the security evaluation of a product, since it may expose fundamental vulnerabilities.

(c) While the OSI conformance testing methodology is appropriate for evaluating the conformance of implementations to the SP4 standard, it is not a sufficient means to assess the trustworthiness of an implementation; a security evaluation is needed.

(d) Since the SP4 standard contains no assumptions about the trustworthiness of an implementation, implementors' groups are expected to develop security sub-profiles for generic applications of SP4 that may include sufficient information for a security evaluation to be conducted.

(e) A coordinated method for a single embedded layer is the appropriate method of testing for SP4, and the required test scenarios can be drawn directly from the SP4 PICS proforma.

(f) SP4 conformance testing can build upon existing Transport layer protocol test procedures, and be conducted in cooperation with established conformance testing bodies.

(g) Interoperability testing is a complementary follow-on step to the conformance testing and security evaluation of an SP4 implementation.

Several areas for further work are also evident from the discussion in this paper. They include the following:

(a) Construction of abstract test scenarios for SP4.

(b) Development of a security sub-profile for a target level of assurance.

(c) Realization of the CSE test method for SP4.

(d) Investigation of incorporating the OSI conformance testing methodology into the security evaluation process.

REFERENCES

[1] ISO IS 7498, Information Processing Systems - Open systems Interconnection - Basic Reference Model, 1984.

[2] ISO IS 7498/2, Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, 1988.

[3] Specification SDN.401, Secure Data Network Systems (SDNS) Security Protocol 4 (SP4), revision 1.3, National Security Agency, May 1989.

[4] D. Branstad and others, SP4: A Transport Encapsulation Security Protocol, Proceedings National Computer Security Conference, September 1987.

[5] R. Nelson, SDNS Services and Architecture, Proceedings National Computer Security Conference, September 1987.

[6] ISO/IEC IS 10736, International Standard - Open Systems Interconnection - Transport Layer Security Protocol, December, 1992.

[7] DoD 5200.28-STD, DoD Trusted Computer System Evaluation Criteria, August 1983.

[8] W. Jansen, Protocol Implementation Conformance Statement (PICS) Proforma for the SDNS Security Protocol at Layer 4 (SP4), NISTIR-4934, October 1992.

[9] ISO 9646, Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework, Parts 1-7, March 1991.

[10] Stable Implementation Agreements for Open System Interconnection Protocols, version 5, edition 1, Part 8: Message Handling Systems, NIST Special Publication 500-202, December 1991.

[11] Government Open Systems Interconnection Profile (GOSIP), Federal Information Processing Standard (FIPS) 146-1, National Technical Information Service, April 1991.

[12] J. Stephen Nightingale, GOSIP Conformance and Interoperation Testing and Registration, NISTIR-4594, March 1991.

[13] NCSC-TG-005, Trusted Network Interpretation, National Computer Security Center, version 1, July 1987.