Standards for Computer Systems Security:
An Interoperability Analysis of SDNS SP3 and ISO NLSP

W. Douglas Maughan
E-mail: wdmaugh@tycho.ncsc.mil

Department of Defense

Abstract

In the Open Systems Interconnection (OSI) communications framework, standards are being proposed for cryptographic-based security protocols that will provide security services to the user. Many of these security protocols provide almost identical security services and are being pursued in groups that include ANSI, IEEE, IETF, and NATO. This paper examines two of the current security protocols defined for the Network Layer of the OSI communications stack that are being proposed for use by Department of Defense and commercial networks and the issue of interoperability between these two protocols.

1 Introduction

This paper provides a technical analysis of interoperability at the protocol level of the current Network Layer security protocols, which have been developed for the provision of security services in an OSI protocol stack. The two protocols that are examined in this paper are the Secure Data Network Systems (SDNS) Security Protocol 3 (SP3) [1] and the International Standardization Organization (ISO) Network Layer Security Protocol (NLSP) [2]. This analysis has been done solely on the Protocol Data Unit (PDU) formats of these protocols and outlines the differences that exist. This analysis is based on the ISO NLSP Committee Draft (CD 11577). NLSP was advanced to a Draft International Standard (DIS) at the July 1992 meeting of ISO Sub-committee 6 (SC6).

1.1 Common Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CL</td>
<td>ConnectionLess</td>
</tr>
<tr>
<td>CLNP</td>
<td>ConnectionLess Network Protocol</td>
</tr>
<tr>
<td>CO</td>
<td>Connection Oriented</td>
</tr>
<tr>
<td>GOSIP</td>
<td>Government Open Systems Interconnection Profile</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>NLSP</td>
<td>Network Layer Security Protocol</td>
</tr>
<tr>
<td>NLSP-CL</td>
<td>NLSP ConnectionLess</td>
</tr>
<tr>
<td>NSAP</td>
<td>Network Service Access Point</td>
</tr>
<tr>
<td>NSDU</td>
<td>Network Service Data Unit</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>PDU</td>
<td>Protocol Data Unit</td>
</tr>
<tr>
<td>SA-ID</td>
<td>Security Association Identifier</td>
</tr>
<tr>
<td>SDNS</td>
<td>Secure Data Network Systems</td>
</tr>
<tr>
<td>SDTPDU</td>
<td>Secure Data Transfer Protocol Data Unit</td>
</tr>
<tr>
<td>SP3</td>
<td>Security Protocol 3</td>
</tr>
<tr>
<td>TLV</td>
<td>Type / Length / Value</td>
</tr>
</tbody>
</table>

2 Background

It is assumed that the reader is familiar with the ISO Open Systems Interconnection (OSI) Reference Model [3] and the layered communications architecture concept. The reader should also be knowledgeable of the work that is presented in ISO 7498-2, the Security Architecture for the OSI Reference Model [4]. The protocols discussed in this paper, SP3 and NLSP, provide the security services for the network layer that are discussed in ISO 7498-2.

2.1 Secure Data Network Systems (SDNS)

Security Protocol 3 (SP3)

The Secure Data Network Systems (SDNS) program was initiated in 1986 by the U.S. Government. It was a cooperative research program which involved several government agencies and twelve computer and communications corporations. The SDNS program designed and specified the standards for the next generation of secure network products providing cost effective, user friendly security features in secure communications components. The program concentrated on specifying a complete security architecture for the emerging OSI architecture. There are several pieces to the SDNS program, including Security Protocol 3 (SP3), Security Protocol 4 (SP4), Message Security Protocol (MSP), and Key Management Protocol (KMP).

This paper focuses only on SP3 and its variations, which extends to the connectionless network service, described in ISO 8348/AD1 [5], and the connectionless network protocol, described in ISO 8473 [6]. SP3 was designed with 4 variations, depending on the addressing...
mode in use. They are (1) SP3-N, which is used only from end-system to end-system, (2) SP3-A, which is similar to SP3-N but can be used for communications across both end-systems and intermediate systems, (3) SP3-I, which is similar to SP3-A but supports the use of CLNP headers, and (4) SP3-D, which is similar SP3-A but supports the use of DoD IP headers.

2.2 International Standardization Organization Network Layer Security Protocol (NLSP)

The Network Layer Security Protocol (NLSP) effort began in late 1989. At the ISO Sub-Committee 6 (SC6) meeting in January 1990, three contributions were introduced. These contributions were: (1) Security Protocol 3 (SP3), a connectionless protocol introduced by the U.S. from the SDNS program, (2) End-to-End Security Protocol (EESP), a connection oriented protocol introduced by the U.K., and (3) Security Protocol for X.25 (SPX), a connection oriented protocol for use with X.25 networks introduced by Northern Telecom. Since January 1990, SC6 has been refining the NLSP specification document so that it incorporates both modes of operation, connection oriented and connectionless, and is also suitable for use with intermediate systems as well as end-systems. The ISO SC6 work provides computer standards to achieve interoperability on an international level, without regard to national and commercial interests. The current version of the NLSP paper is Draft International Standard (DIS 11577). NLSP, as it is currently defined, has the functionality to work with both connectionless and connection oriented network protocols. Because SDNS SP3 is a connectionless protocol, this paper will focus only on the connectionless variant of NLSP to give the most precise interoperability analysis.

2.3 Comparison of Security Services

The ISO 7498-2 [4] document discusses the security architecture for the OSI Reference Model and establishes guidelines and constraints in order to provide secure communications within the framework of the Reference Model. It provides a general description of security services and related mechanisms and defines the positions with the OSI Reference Model where the security services and mechanisms may be provided. There are several security relevant definitions contained in 7498-2 and those applicable to this paper follow.

Access Control:
The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

Confidentiality:
The property that information is not disclosed to unauthorized individuals, entities, or processes.

Data Integrity:
The property that data has not been altered or destroyed in an unauthorized manner.

Security Service:
A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or data transfers.

Security Mechanism:
The method or technique utilized to provide the requested security service. Some mechanisms may be applicable to more than one security service.

Data Origin Authentication:
The corroboration that the source of data received is as claimed.

Peer Entity Authentication:
The corroboration that an entity in an association is the one claimed.

Traffic Flow Confidentiality:
A confidentiality service to protect against traffic analysis.

Connectionless Confidentiality:
This service provides for the confidentiality of all userdata in a single connectionless service data unit.

Connectionless Integrity:
This service provides for the integrity of a single connectionless service data unit and may take the form of determination of whether a received service data unit has been modified.

<table>
<thead>
<tr>
<th>Security Services</th>
<th>7498-2</th>
<th>NLSP</th>
<th>SP3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control Service</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Data Origin Authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Peer Entity Authentication</td>
<td>Yes</td>
<td>(Yes)</td>
<td></td>
</tr>
<tr>
<td>Connection Confidentiality</td>
<td>Yes</td>
<td>(Yes)</td>
<td></td>
</tr>
<tr>
<td>Connectionless Confidentiality</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Traffic Flow Confidentiality</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Connection Integrity without Recovery</td>
<td></td>
<td>(Yes)</td>
<td></td>
</tr>
<tr>
<td>Connectionless Integrity</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 1 Comparison of Security Services
Given the previous security relevant definitions, table 1 shows the security services that can be provided at the network layer, as defined by ISO 7498-2, and which of those security services are supported by NLSP and SP3.

NOTE: For NLSP, Connection Integrity without Recovery, Connection Confidentiality, and Peer Entity Authentication are services supported in a connection oriented environment. They have been included in table 1 to show some of the other functionality of NLSP, even though this paper is only concerned with connectionless network services.

3 Interoperability Issues

Data communication protocols define the rules, formats, procedures, and vocabulary for the exchange of information between two communicating entities. The purpose for describing a protocol is so that entities desiring communication can do so consistently and completely without restriction. A protocol provides the means for these communicating entities to interoperate. There are several elements to a protocol. They are (1) the services to be provided by the protocol, (2) the assumptions made about the environment, (3) the vocabulary of the messages used in the protocol, (4) the encoding formats of each message in the vocabulary, and (5) the procedure rules for handling the message exchanges.

Section 2.3 discusses the services provided by the protocols that are being examined. Some assumptions about the environment in which these protocols, NLSP and SP3, reside has also been mentioned, i.e. connectionless networks, in both end-systems and intermediate systems. The protocol vocabulary consists of the ordering of messages that will occur within the protocol. The protocols under analysis use a vocabulary of acknowledgments, negative acknowledgments, error reporting, and the standard ISO protocol vocabulary of request, indication, response, and confirm service primitives. The vocabulary for these protocols is discussed in greater detail in the respective protocol specification documents. The procedure rules specify the operations that must take place for correct transmission and receipt of information at each communicating entity. The procedure rules are not discussed in this paper, but the reader must understand that it is imperative these rules are consistent for both communicating entities in order for correct operation and interoperability to be achieved.

The analysis contained in the remainder of this paper discusses the encoding formats of the NLSP and SP3 protocols. Like the procedure rules, the encoding formats of protocols must be identical to ensure interoperability between the communicating entities. The analysis which has been done examines the encoding formats of the NLSP and SP3 protocols and points out those areas where the encoding formats are not compatible. The current trend in protocol design allows more flexibility in the placement of information within the protocol data unit (PDU). It is important to realize that this is possible because the procedure rules will gather the correct information from what is transmitted.

3.1 Clear Header Analysis

The Clear Header of a protocol data unit (PDU) is that portion which is not encrypted prior to transmission to the peer communicating entity. For SP3 and NLSP, the Clear Header contains an identifier to distinguish the PDU as a security PDU. There is also a field which provides an indirect mapping to the addresses of the communicating entities. This field is the SA-ID for NLSP and the Key-ID for SP3. It is understood that this portion of the PDU is "in the clear" and not encrypted, therefore, information that determines the actual identities of the communicating entities is not included in the Clear Header. Fields that are designated as having a variable length may be constrained by Length fields in the respective header. This is true for all occurrences mentioned throughout the remainder of this paper.

3.1.1 SP3 Clear Header

Figure 3-1 shows the format for the Clear Header of SP3. All fields are required and must appear in the order shown.

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length Indicator (LI)</td>
<td>Length: 1 octet</td>
</tr>
<tr>
<td>PDU Type Code (SE)</td>
<td>Length: 1 octet</td>
</tr>
<tr>
<td>KEY-ID</td>
<td>Length: variable</td>
</tr>
</tbody>
</table>

Figure 3-1 Format of SP3 Clear Header

- The Length Indicator (LI) field contains the length of the Clear Header in octets, excluding the length indicator field.
- The PDU Type Code or SE field indicates that the PDU is a security PDU and is represented by the value 72 (48 hex).
- The KEY-ID field contains the key identifier, which can be variable in length.
3.1.2 NLSP Clear Header

Figure 3-2 shows the format for the Clear Header of NLSP. All fields, except the Encipher Synchronization field, are required for NLSP-CL and must appear in the order shown.

### Table: Format of NLSP Clear Header

<table>
<thead>
<tr>
<th>Protocol ID</th>
<th>Length Indicator</th>
<th>PDU Type</th>
<th>SA-ID</th>
<th>Encipher Sync.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length: 1 octet</td>
<td>Length: 1 octet</td>
<td>Length: variable</td>
<td>Length: variable</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 3-2** Format of NLSP Clear Header

- The Protocol ID field contains the NLSP protocol identifier. The format for this identifier is defined in ISO TR9577.
- The Length Indicator field contains the length of the Clear Header in octets, excluding the length indicator field and the Protocol ID field.
- The PDU Type field indicates that the PDU is a Secure Data Transfer PDU (SDTPDU) and is represented by the value 0.
- The SA-ID field contains the Security Association identifier.
- The Encipherment Synchronization field is optional. It may be present depending on the encipherment algorithm identifier and associated attributes.

3.1.3 Clear Header Differences

There are four differences between the SP3 Clear Header and the NLSP Clear Header. They are as follows:

1) NLSP has a Protocol ID (PID) at the beginning of the Clear Header with a standard format defined by ISO Technical Report 9577 (TR9577). SP3 does not have this field at the beginning of the Clear Header in the PDU structure.

2) NLSP has a PDU Type value of "0" for the Secure Data Transfer PDU (SDTPDU). SP3 has a PDU Type value of 72 for the SP3 PDU.

3) NLSP has a field titled "SA-ID" with a variable length. SP3 has a field titled "Key-ID" with a variable length. The SA-ID of NLSP is based on a developing concept within ISO of security associations. Because these fields are variable length and the basis for the values are not necessarily compatible, it is highly unlikely that the NLSP SA-ID and the SP3 Key-ID will be the same.

4) NLSP has an encipherment synchronization field at the end of the Clear Header which may contain synchronization data for specific encipherment algorithms. SP3 does not have this field within the Clear Header.

3.1.4 Impact of Clear Header Differences

The impact of the differences between the NLSP and SP3 Clear Headers is that separate security devices, which implemented these two protocols as they are currently defined, would not interoperate. The example below in Figure 3-3 demonstrates these differences:

Given the following parameter values, the Clear Header formats are shown below.

- **NLSP**: Protocol ID of 20, SA-ID of 5 octets, and Encipherment Sync of 2 octets
- **SP3**: Key-ID of 5 octets

### Table: SP3 Clear Header Format

<table>
<thead>
<tr>
<th>Length Indicator</th>
<th>PDU Type Code (SE)</th>
<th>Key-ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value: 6</td>
<td>Value: 72</td>
<td>Value: 5 octets</td>
</tr>
</tbody>
</table>

The bit pattern would be:

00000110 01001000 (5 octets variable).

### Table: NLSP Clear Header Format

<table>
<thead>
<tr>
<th>Protocol ID</th>
<th>Length Indicator</th>
<th>PDU Type</th>
<th>SA-ID</th>
<th>Encipher Sync.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value: 20</td>
<td>Value: 8</td>
<td>Value: 0</td>
<td>Value: 5 octets</td>
<td>Value: 2 octets</td>
</tr>
</tbody>
</table>

The bit pattern would be:

00010100 00001000 00000000 (5 octets plus 2 octets variable).

**Figure 3-3** Example of SP3/ NLSP Clear Header PDU Differences

Upon examination of the example shown above in figure 3-3, the bit patterns that would be transmitted by the different protocols are not identical and, therefore, separate security devices implementing these protocols would not interoperate. As was discussed in section 3, the encoding formats must be identical in both communicating entities for interoperability.
3.2 Protected Header Analysis

The Protected Header of a protocol data unit (PDU) is that portion which is encrypted prior to transmission to the peer communicating entity. For SP3 and NLSP, the Protected Header contains an identifier to distinguish the initiator of transmission from the responder. The remainder of the Protected Header contains those fields that need to be encrypted for security reasons. Some of these fields include addresses, labels, sequence numbers, integrity check value, authentication information, and the actual userdata being transmitted. All of this information is enciphered using the encipherment function and the encipherment algorithm. A detailed discussion of how the encipherment function is implemented is beyond the scope of this paper.

3.2.1 NLSP Protected Header

Figure 3-4 shows the format for the Protected Header of NLSP. The Content Length, Content Type, and at least one Content Field are required and must appear in the order shown.

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Length: 1 octet</td>
<td>Length: 1, 2, or 3 octets</td>
</tr>
</tbody>
</table>

Figure 3-4 Format of NLSP Protected Header

- The Content Length field contains the length of the Protected Header in octets, excluding the Content Length field. The maximum length of the Protected Header is 65,535 octets.
- The Content Type field consists of the following structure:
  - Bit 8 of the Content Type field contains the "Initiator to Responder" flag signifying the direction or origin of this PDU. If this bit has a value of 1, that indicates Initiator to Responder, and a value of 0 indicates Responder to Initiator.
  - The remaining 7 bits are encoded to identify the NLSP service primitives. NLSP-CL uses only the NLSP-UNITDATA request / indication service primitive, which has a value of 1.
- The Content Field contains a generic field format for data values to be placed within the Protected Contents of the NLSP SDTPDU. The format of the Content Field is known as TLV encoding, which stands for Type / Length / Value encoding. This format is shown below in Figure 3-5.

Figure 3-5 Format of Content Field Encoding

- The Content Field Type contains the encoding for the different types of data contained in the Protected Contents. Data items may include addresses, labels, key information, and userdata. Each data item has a reserved value, i.e. Label = C0, Calling NLSP Address = C2, Called NLSP Address = C3, etc.
- The Content Field Length contains the length of the Content Field Value in octets. The Content Field Length can be 1, 2, or 3 octets in length. If the length is 1 octet, the first bit is 0 and the remaining 7 bits define a value length up to 127 octets. If the length is 2 or 3 octets, the first octet specifies if there are 1 or 2 remaining octets. The remaining octets, 1 or 2, define a maximum value length of 255 or 65,535 octets, respectively.
- The Content Field Value contains the data for the specified Content Field Type. The formats of some expected Content Fields are given below in Figure 3-6. Each of the Content Fields has a Type field length of 1 octet, a Length field length of 1, 2, or 3 octets, and a variable Value field length depending on the Length field value (1, 2, or 3 octets).

NOTE: The only Content Field that differs from the standard format is the Label Content Field. It is listed first in Figure 3-6 and includes a Defining Authority field. The Defining Authority field has a variable length and the Content Length field includes the total length of the Defining Authority field and the Content Value field. Labels are defined and registered by organizations, such as ISO and CCITT. The Label field is used for access control purposes and will change as label standards and formats are standardized within the ISO community.
- The Integrity Check Value (ICV) is defined by the Integrity algorithm identifier contained in the attributes of a Security Association. The ICV has a variable length and is usually placed at the end of the Protected Header and Contents, but is not required to be in that position.
3.2.2 SP3 Protected Header Commonality

There are four different variations of the SP3 protocol depending on the addressing mode that is used. However, there is some commonality in the PDU formats of the different variations. The common features of the different variations is shown in figure 3-7. The Length Indicator (LI) and Flags field are required. Other fields are optional but must occur in the order shown, if used.

- The Length Indicator (LI) field contains the length of the Protected Header in octets, excluding the LI field. It has a maximum value of 254.
- The Flags field consists of the following structure:
  - Bit 1 of the Flags field contains the "Initiator to Responder" flag signifying the direction or origin of this PDU. If this bit has a value of 1, that indicates Initiator to Responder, and a value of 0 indicates Responder to Initiator.
  - The remaining 7 bits are reserved for future use.
- The Integrity Check Value (ICV) is defined by the Integrity algorithm identifier and attributes known between communicating SP3 entities. The ICV has a variable length and must be placed at the end of the Protected Header and Contents.

3.2.3 Analysis of NLSP and SP3-N

The SP3-N addressing mode is used only from end-system to end-system. An NSDU contains both protocol control information and actual data and is passed across layer boundaries in the OSI model. SP3-N encapsulates complete NSDU's, but does not include any addressing information in the encapsulated header. Addressing information from the transport layer is passed straight through to the underlying network on transmission and is passed straight through to the transport above from the network layer on reception.

3.2.3.1 SP3-N Protected Header

Figure 3-8 shows the format for the specific parts of the Protected Header of SP3-N. The Length Indicator (LI) and Flags fields are required, as stated in section 3.2.2, and all other fields are optional. If they are included, they must be in the order shown in figure 3-8.

3.2.3.2 NLSP / SP3-N Protected Header Differences

There are several differences between the NLSP Protected Header and the SP3-N Protected Header. They are as follows:

1) The Length Indicator is 2 octets in the NLSP Protected Header. It is only 1 octet in the SP3-N Protected Header.
2) The formats of the NLSP Content Type field and the SP3-N Flags field are different. The bit which represents the Initiator to Responder flag is located in a different place in each field. The remaining bits of the NLSP Content Type field are used to specify which service primitive is being transmitted. The remaining bits of the SP3-N Flags field are for future use.
3) The NLSP Label contains the following parameters:
   Type, Length, Defining Authority, and Value, as shown in Figure 3-6. The SP3-N Label field also contains these same parameters, however, there are three differences:
   A. The NLSP Length field can be 1, 2, or 3 Octets, whereas, the SP3-N Length field is only 1 octet.
   B. The NLSP Defining Authority field has a variable length, whereas, the SP3-N Defining Authority field is only 1 octet.
   C. The NLSP Defining Authority field will allow different Defining Authority formats and Label Contents based on the Defining Authority. SP3-N discusses only the Department of Defense (DoD) Defining Authority, which uses the Basic Security Option and Extended Security Option of the revised DoD Internet Protocol (IP) security options. It is unclear if SP3-N will allow for other Defining Authorities.

4) The NLSP Pad field is shown in Figure 3-6 and is similar to the SP3-N Pad field. The only difference is NLSP Padding Length can be 1, 2, or 3 octets, while SP3-N Padding Length is only 1 octet.

5) Although, little has been written about the ICV and the corresponding algorithm, it is assumed that the ICV's calculated for NLSP and SP3-N would be interoperable as long as the same algorithm was used. Given this assumption is true, a discussion about the use of algorithms, their identifiers, and attributes is needed, but is beyond the scope of this paper and will not be contained herein.

3.2.4 Analysis of NLSP and SP3-A

The SP3-A addressing mode can be used for both end-systems and intermediate systems. SP3-A encapsulates complete NSDU's, but includes any addressing information in the encapsulated header. These addresses are the source and destination NSAP addresses. If fragmentation is necessary before encapsulation, it is done. The fragments or complete PDU's are encapsulated. On receipt of fragmented PDU's, the data units are unencapsulated and then reassembled before transmission to a higher layer. SP3-I differs from SP3-A because it can handle PDU fragments as well as whole PDUs. SP3-I addressing is also different than SP3-A. NLSP is capable of handling PDU fragments, as well as whole PDUs, in both end-systems and intermediate systems, similar to SP3-I.

3.2.4.1 SP3-A Protected Header

Figure 3-9 shows the format for the specific parts of the Protected Header of SP3-A. The Length Indicator and Flags fields are required, as stated in section 3.2.2, and all other fields are optional. If they are included, they must be in the order shown in figure 3-9.

<table>
<thead>
<tr>
<th>Length Indicator</th>
<th>Flags</th>
<th>Label</th>
<th>Pad</th>
<th>Source NSAP</th>
<th>Dest. NSAP</th>
<th>ICV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length: 1 octet</td>
<td></td>
<td>Length: variable</td>
<td></td>
<td>Length: variable</td>
<td>Length: variable</td>
<td>Length: variable</td>
</tr>
</tbody>
</table>

Figure 3-9 Format of SP3-A Protected Header

3.2.4.2 NLSP / SP3-A Protected Header Differences

The Protected Header differences pointed out in Section 3.2.3.2 are also valid for the Protected Headers of NLSP and SP3-A.

3.2.5 Analysis of NLSP and SP3-I

The SP3-I addressing mode can be used for both end-systems and intermediate systems. SP3-I encapsulates complete NSDU's or fragments. The transmitting SP3-I constructs a CLNP Header for the entire NSDU. This CLNP Header includes the source and destination NSAP addresses. If fragmentation is necessary before encapsulation, it is done. The fragments or complete PDU's are encapsulated. On receipt of fragmented PDU's, the data units are unencapsulated and then reassembled before transmission to a higher layer.

SP3-I differs from SP3-A because it can handle PDU fragments as well as whole PDUs. SP3-I addressing is also different than SP3-A. NLSP is capable of handling PDU fragments, as well as whole PDUs, in both end-systems and intermediate systems, similar to SP3-I.

3.2.5.1 SP3-I Protected Header

Figure 3-10 shows the format for the specific parts of the Protected Header of SP3-I. The LI and Flags fields are required, as stated in section 3.2.2, and all other fields are optional. If they are included, they must be in the order shown in figure 3-10.

3.2.5.2 NLSP / SP3-I Protected Header Differences

There are several differences between NLSP and SP3-I. The differences pointed out in section 3.2.3.2 are also valid plus the following additional differences exist:

1) As shown in figure 3-6, the NLSP TLV format for the CLNP Header allows the length of the actual...
CLNP Header to be represented by a length of 1, 2, or 3 octets, while SP3-A only allows the CLNP Header to be represented by 1 octet in length. This means that the CLNP Header in the Protected Header of an NLSP SDTPDU could have a length up to 65,535 octets but the CLNP Header in the Protected Header of an SP3-A PDU could be only 127 octets.

<table>
<thead>
<tr>
<th>Length Indicator</th>
<th>Flags</th>
<th>Pad</th>
<th>CLNP HDR</th>
<th>ICV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length: 1 octet</td>
<td>Length: variable</td>
<td>Length: variable</td>
<td>Length: variable</td>
<td>Length: variable</td>
</tr>
</tbody>
</table>

**Figure 3-10 Format of SP3-I Protected Header**

3.2.6 Analysis of NLSP and SP3-D

The SP3-D addressing mode is identical to the SP3-I addressing mode, except that it uses the U.S. Government Department of Defense (DoD) Internet Protocol (IP) header format and protocol rules instead of the ISO CLNP format and protocol rules. NLSP does not support the use of DoD IP addressing.

3.2.6.1 SP3-D Protected Header

Figure 3-11 shows the format for the specific parts of the Protected Header of SP3-D. The LI and Flags fields are required, as stated in section 3.2.2, and all other fields are optional. If they are included, they must be in the order shown in figure 3-11.

<table>
<thead>
<tr>
<th>Length Indicator</th>
<th>Flags</th>
<th>Pad</th>
<th>IPHDR</th>
<th>ICV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length: 1 octet</td>
<td>Length: variable</td>
<td>Length: variable</td>
<td>Length: variable</td>
<td>Length: variable</td>
</tr>
</tbody>
</table>

**Figure 3-11 Format of SP3-D Protected Header**

3.2.6.2 NLSP / SP3-D Protected Header Differences

There are several differences between NLSP and SP3-D. The differences are pointed out in section 3.2.3.2 are also valid plus the following additional difference exists:

1) NLSP does not define a Content Field for encoding information for use with the DoD IP protocol but SP3-D does in the IPHDR field.

3.2.7 Impact of Protected Header Differences

The impact of the differences between the NLSP and SP3 Protected Headers is that separate security devices, which implement these two protocols as they are currently defined, would not be able to interpret the contents of the Protected Headers correctly. This means that they would not interoperate because the encoding formats and procedure rules are different for each protocol. The Protected Header formats are shown in figure 3-12 to demonstrate the differences between the NLSP and SP3 Protected Headers.

An assumption is made that the NLSP and SP3 entities are the Initiator. Given the following information, the Protected Header formats are shown below.

1) The Content Field of NLSP and the variations of SP3 are different, as outlined in section 3.2, but assume a length of 20 octets for each.

2) Assume that the ICV calculated would be the same as mentioned in section 3.2.3.2 and would have a length of 4 octets.

**Figure 3-12 Example of SP3/ NLSP Protected Header PDU Differences**

Upon examination of the example shown above in figure 3-12, the bit patterns that would be transmitted by the different protocols are not identical and, therefore, separate security devices implementing these protocols would not be able to interpret the contents of the Protected Header in the same manner, thus, interoperability would not be accomplished. As was discussed in section 3, the encoding formats must be identical in both communicating entities for interoperability to be achieved.
4 Conclusions

Based on the analysis presented in this paper, there are significant differences between the ISO NLSP and SDNS SP3 network security protocols. Even though one of the inputs to the ISO NLSP standard was the SDNS SP3 protocol, these differences are substantial enough that security devices running the NLSP and SP3 security protocols would not be interoperable. One of the reasons for the differences that have occurred is the international standardization process. Because NLSP is a combination of three separate protocols and is designed for use with both connectionless and connection-oriented networks, it went through several changes during the committee process of the ISO standards. This iterative process of standards definition resulted in the connectionless portion of the ISO NLSP protocol being non-interoperable with the original SDNS SP3 protocol that was submitted into the ISO SC6 committee.

There are significant differences, outlined in sections 3.1.3, 3.2.3.2, \(<\text{nlspsp3iphdiffs}>\), and 3.2.6.2, between the ISO NLSP and SDNS SP3 protocol formats. Some of these differences could be resolved through the use of protocol translators operating in a gateway-like manner. There are still other differences, i.e. NLSP SA-ID vs. SP3 Key-ID and associated key management issues, NLSP Clear Header Protocol ID vs. No Protocol ID for SP3, and CLNP Header length differences for NLSP and SP3-1 Protected Header, which cannot be resolved by using some form of translation between the two protocols. These irreconcilable differences must be considered in any attempts to make the ISO NLSP and SDNS SP3 protocols compatible.

The NLSP protocol is still undergoing design and development within the ISO community and is still somewhat of moving target. NLSP was designed to provide complete support for the security services outlined in ISO 7498-2, while SP3 does not provide all the required security services for the Network Layer. Additionally, NLSP provides support for connection-oriented communications (that was not examined in this paper). It is still very questionable within the ISO community whether SP3, in its current state, is satisfactory for connection-oriented communications.

The Government Open Systems Interconnection Profile (GOSIP) program being developed by the National Institute of Standards and Technology (NIST) is highly unlikely that compliance with both NLSP and SP3 will be allowed. Currently, NLSP is being touted as the Network Layer security protocol for inclusion in the GOSIP architecture. SP3, with its many variations, is still a valid security protocol for U. S. and DoD communications in a connectionless environment.

NLSP has also been adopted by the NATO Sub-Group 9 (SG/9) Ad Hoc Working Group on Security as the Network Layer protocol for the NATO OSI Security Architecture (NOSA). Because of the international standards process and the international nature of NATO, SP3 was not accepted as a security protocol for NATO.

5 Recommendations

There are many important components involved in obtaining interoperability between communicating computer systems. The introduction of security and the use of a security protocol is just one element of the entire communications architecture. Even though NLSP is still under development, it should be considered for future developments and procurements of network layer security products in order to be compliant with the proposed GOSIP architecture.

The problem of interoperability between ISO NLSP and SDNS SP3 still remains. Because of the momentum that NLSP has gained and the international nature of the ISO standardization process, it is highly unlikely that NLSP will be changed to meet the SP3 protocol formats. Therefore, if NLSP and SP3 are to be interoperable, consideration should be given to make changes to the SDNS SP3 protocol suite.

6 References