Branstad, Dennis, Joy Dorman, Russell Housley, and James Randall. "SP4: A Transport Encapsulation Security Protocol." In *Tenth National Computer Security Conference Proceedings*, September 1987, pp 158-161.

SP4: A TRANSPORT ENCAPSULATION SECURITY PROTOCOL

Dennis Branstad, National Bureau of Standards
Joy Dorman, Digital Equipment Corporation
Russell Housley, Xerox Corporation
James Randall, International Business Machines Corporation

INTRODUCTION

The Secure Data Network System (SDNS) project is developing a security architecture within the Organization of International Standardization's (ISO) Open Systems Interconnection (OSI) computer network model[1]. The security architecture is designed to provide several security services to the user of an OSI network[2]. The architecture includes security protocols between peer entities of the OSI architecture. The SDNS architecture is designed to satisfy the security requirements of both classified and unclassified applications. The cryptographic algorithms used for data confidentiality, integrity and key distribution have been defined but are not discussed in this paper.

The SDNS project began during the summer of 1986, Phase I, completed in mid-1987, specified the security architecture. The SDNS architecture concentrates on the confidentiality, integrity, identification / authentication, and access control security services. Non-repudiation is of secondary interest. SDNS provides security services in four of the seven layers in the ISO model.

The application layer (layer 7) provides for application specific access to network services. SDNS examined the X.400 message handling system (electronic mail). SDNS secure electronic mail provides all four of the major security services and sender non-repudiation.

The physical layer (layer 1) provides a physical connection for the transmission of data by electrically encoding the data for a specific medium. The SDNS architecture provides for confidentiality at this layer. It is the only layer in the SDNS architecture which provides traffic flow confidentiality.

The network layer (layer 3) provides message routing and relaying between interconnected networks and end systems on the same network. The SDNS architecture provides all four of the major security services at this layer. Connectionless confidentiality and integrity are provided. Identification / authentication and access control are of the end systems. It is the only layer in the SDNS architecture which provides for encipherment at gateways to support "red" networks.

The transport layer (layer 4) provides reliable, transparent transfer of data between end systems. Again, SDNS provides all four of the major security services at this layer. This paper discusses these security services and protocol that implements them. The paper also outlines the requirements for key management.

The Security Protocol at Layer 4 (SP4) was developed by the SDNS Protocol Working Group. SP4 provides either connectionless or connection-oriented confidentiality depending on the cryptographic key granularity. Likewise, either connectionless or connection-oriented integrity may be selected. Peer entity authentication and access control are provided in conjunction with the key manager.

The following objectives were established in designing SP4:

- provide secure end-to-end reliable service independent of network technology
- provide confidentiality and integrity cryptographic protection continuously from one end system to another
- provide ease of implementation when red/black separation is required
- support both host-to-host keying and transport connection keying
- support many cryptographic algorithms
- support many different generic transport protocols
- minimize changes to existing transport services and protocols
- minimize the effort, cost and time required to achieve security certification for classified applications
- minimize the bandwidth of covert channels (i e , information paths that would allow unprotected data to exit from an end system)
- allow implementation within end systems with varying levels of trust

In order to satisfy the selected set of objectives, an encapsulation approach was taken . Transport encapsulation security was coined to denote that whatever the transport entity produced to send to a peer transport entity was encapsulated in a security envelope. This new envelope, called a Secure Encapsulated Transport Protocol Data Unit , could then be sent through any network. A simple format was defined and the required security transformations were specified.

KEY MANAGEMENT SUPPORT

The keys provided by the key manager are used by SP4 to provide confidentiality and integrity. Access control and authentication decisions are made before the key identifier is delivered to SP4. SP4 enforces these access control decisions by checking the labels on individual protocol data units (PDU).

Key Generation

SP4 was designed to be independent of encryption algorithm and method of key distribution. Either symmetric or asymmetric algorithms can be used.

SDNS uses SP4 with a symmetric key algorithm. SP4 depends on the key manager to establish and update traffic keys. The SDNS key manager uses public key cryptography to generate these traffic keys.

Key Granularity

One of three key granularities is selected when the key is established:

- Key per end system NSAP pair. One key protects all transport connections established between a pair of transport entities in two end systems.
- Key per end system NSAP pair and security label. As above with the addition that the protection extends to a single security level or range.
- Key per transport connection. One key will be used to protect each transport connection independently from all others. Transport connections are assumed to be single-level. Transport connection keying is required for connection-oriented integrity.

A SP4 transport entity may simultaneously support any or all of these key granularities. Security options are associated with each key identifier; this technique permits traffic to be protected to varying levels.

Security Option Association

When one of the transport entity pair keying alternatives is selected, the following attributes may be associated a key identifier:

- Encryption algorithm
- Confidentiality (encrypt or not)
- Message Authentication Code (MAC) length (including none)
- Security label in each protocol data unit (or not)
- Set or range of security levels which may be transmitted under the key

If transport connection keying is selected, the following attributes may be associated with a key identifier:

- Encryption algorithm
- Confidentiality (encrypt or not)
- Message Authentication Code (MAC) length (including none)
- Security label in each protocol data unit (or not)
- Connection truncation protection (or not)

PROTOCOL AND DATA FORMAT

SP4 povides many security services. This section further defines these services and discusses how each is provided. SP4 relies on the key manager and generic transport services; the dependencies will be highlighted.

Protocol Data Unit Format

Figure 1 illustrates the format of the protocol data unit (PDU) used in SP4. The SE PDU is formed by computing the message authentication code (MAC)[3] and then performing encryption.

Four heading fields are transmitted in the clear. The first field is the Length Indicator (LI); it simply points to the beginning of the encrypted information. Second is the type field; SP4 PDUs always have SE for their type. Next is the key identifier (KEY-ID). The key identifier names the key; including a name permits different connections to be cryptographically separated on the network. Finally, the Initial Vector (sometimes called the MI) appears. The recipient uses the Initial Vector to initialize the decryptor; this value permits the PDUs to be decrypted even if they arrive out of order

The encrypted header also contains four fileds The Security label, Final Sequence Numbers (FSN), and Pad are optional; only those which are needed are included. The LI points to the beginning of the user data. The security label indicates the sensitivity of the data contained in the PDU. The FSN gives the final transport sequence number sent and the final transport sequence number received. The FSN is included in the closing PDUs of the transport connection. Pad is used when the encryption algorithm requires the PDU to be a specific length.

Confidentiality

Confidentiality is the protection of information from disclosure to unauthorized individuals, entities, or processes. Connectionless confidentiality is the

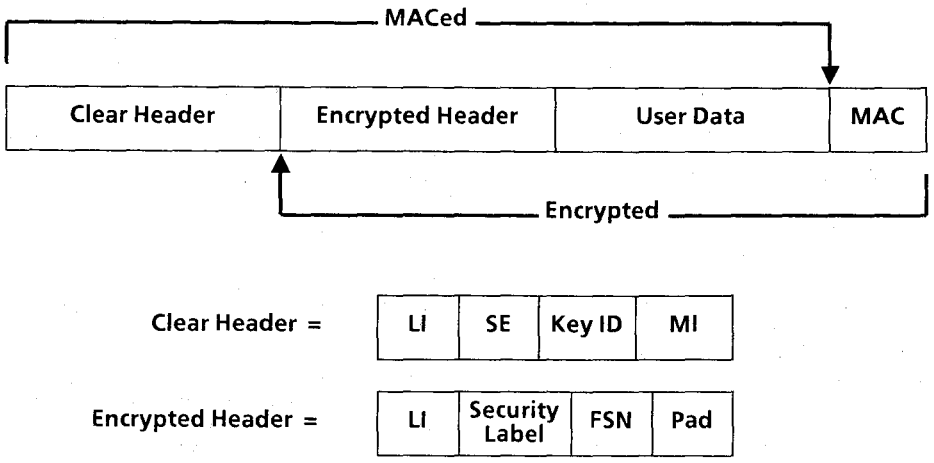

Figure 1. SE PDU Format

protection of a individual PDUs. Connection-oriented confidentiality is the protection of all PDUs in a transport connection.

SP4 supplies connection-oriented confidentiality when transport connection keying is used. Otherwise, connectionless confidentiality is provided.

Connectionless Integrity

Data integrity is the protection of data from alteration or destruction. Connectionless integrity provides protection against the modification of a individual PDUs.

SP4 provides connectionless integrity by appending a MAC to the PDU. The MAC algorithm uses the same key as the encryptor / decryptor, so an additional KEY-ID field is not required to support the MAC. The MAC is computed on the entire PDU, including the plaintext header. The MAC is computed before encryption and checked following decryption.

Connection-oriented Integrity

Connection-oriented integrity includes protection against modification, deletion, insertion, replay (of single PDUs and entire connections) and reflection.

Protection against modification is is provided as in connectionless integrity; the MAC provides this protection.

Protection against insertion is provided by the MAC and the sequence numbers of the generic transport layer. These sequence numbers are part of the encapsulated "user data".

Protection against deletion is provided by the same two facilities (MAC and transport layer sequence numbers) plus the final sequence numbers fields on the closing PDUs. The MAC and transport layer sequence numbers are sufficient to detect PDU deletions in the middle of connections. The ISO OSI Transport Protocol (TP)[4,5] is vulnerable to deletion of the end of a connection. SP4 includes the final sequence number received and sent on the closing PDUs to detect this truncation. Truncation is not prevented; it is detected.

Protection against PDU replay is obtained if the sequence numbers do not wrap around under the connection key. SP4 must obtain a new key from the key manager shouls the sequence number space be exhauseted.

SP4 must ensure that each transport connection is separately keyed. The key manager is responsible for performing a liveness check as part of key establishemnt. At connection release, SP4 must also notify the key manager to destroy the key.

Protection against reflection is provided if the KEY-ID for transmit and receipt are different. This is accomplished either by the use of different keys for the sender and the recipient or by different names for the same key.

Table 1 summarizes the division of responsibilities between generic transport, SP4 and the key manager to achieve connection-oriented integrity.

Access Control

Access control provides protection against unauthorized use of the resources accessible via OSI. Access control is provided by the key manager. In addition, SP4 provides support for access control via security label checking. SP4 discards any PDUs that arrive and decrypt but contain labels outside the range specified for use with the key identifier.

Peer Entity Authentication

Peer entity authentication is the verification that a peer entity in an association is the one claimed. This service can be provided both during the establishment of a connection and during the data transfer phase of a connection. SP4 does not provide peer entity authentication at connection establishment. This service is provided by the key manager.

Protection Against	Generic Transport	SP4	Key Manager
Modification	--	MAC	--
Deletion	Sequence numbers	MAC	--
Insertion	Sequence numbers	MAC & Final sequence numbers	--
PDU Replay	Sequence numbers	MAC & No wrap in sequence numbers	--
Connection Replay	--	--	Liveness test & Key per connection
Reflection	--	--	Different Key IDs in each direction

Table 1. Connection-orineted Integrity Division of Responsibilities

CONCLUSION

SP4 conforms to the OSI philosophy of putting desirable services in the lowest layer possible that can achieve the goals. The host-to-host nature of the transport layer, the encapsulation strategy, and the separation of the key management give SP4 security and flexibility. SP4 meets all of it's design objectives.

Since the transport layer is above the network layer, SP4 passes through routers and relays untouched. This host-to-host quality, along with encryption, fulfills the following design objectives:

- provide secure end-to-end reliable service independent of network technology
- provide confidentiality and integrity cryptographic protection continuously from one end system to another

The encapsulation strategy used in SP4 permits it to use any generic transport protocol including DOD's TCP and ISO's TP. Since the encapsulation is done as the last step in the transport layer, SP4 can be implemented within the host or within the network front end processor. When SP4 is implemented in a front end processor, the security boundary becomes obvious. The encapsulation technique reduces the covert channel bandwidth by filling all of the plaintext SP4 heading fields without influence from the user. Encapsulation fulfills the following design objectives:

- provide ease of implementation when red/black separation is required
- support many different generic transport protocols
- minimize changes to existing transport services and protocols
- minimize the effort, cost and time required to achieve security certification for classified applications
- minimize the bandwidth of covert channels (i.e., information paths that would allow unprotected data to exit from an end system)
- allow implementation within end systems with varying levels of trust

Separating the key management from the SP4 protocol fulfills the remaining two objectives:

- support both host-to-host keying and transport connection keying
- support many cryptographic algorithms

REFERENCES

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

[2] ISO 7498/2, Proposed Draft Addendum to ISO 7498 on Security Architecture.

[3] National Bureau of Standards, Data Encryption Standard, Federal Information Processing Standards Publication 46, 1977.

[4] ISO 8072, Information Processing Systems - Open Systems Interconnection - Transport Service Definition.

[5] ISO 8073, Information Processing Systems - Open Systems Interconnection - Transport Protocol Specification.