To: INCITS T10 Committee
From: Matt Ball, Quantum Corporation
Date: April 24, 2007
Subject: SSC-3: Key Entry using Encapsulating Security Payload (ESP)

Revision History

Revision 0 (T10/06-225r0):
Posted to the T10 web site on 4 May 2006.

Revision 1 (T10/06-225r1) 18 May 2006:
Changed SPI to SAI.
Added definition for 'encrypted information packet'.
Removed 'Secure Channel'.
Added mention of ANS X9.102 as a standard that could replace AES Key Wrap.
Within **Table Y1 – Set Data Encryption page**, moved the SAI (formerly SPI) and SEQUENCE NUMBER fields into the KEY field and left those as 'reserved' (as they were previously). Table Y1 is now unchanged.
Updated **Table Y9 – key field contents with key format field set to 02h** to include SAI and SEQUENCE NUMBER fields.
Minor edits.

Revision 2 (T10/06-225r2) 6 June 2006:
Moved the security association parameters into a table.
Created additional level 5 subclauses for describing the various key formats.
Added changes to the references section
Added clauses for these topics: Nonces and Key derivation functions
Changed the layout for the 'key reference' format
Changed key-wrap reference to RFC 3394 instead of "AES Key-Wrap (Draft)"
Added table for assigning an ID to the key derivation functions (KDF).
Numerous rewordings.

Revision 3 (T10/06-225r3) 27 June 2006:
Edits based on feedback from Michael Banther

Revision 4 (T10/06-225r4) 2 Jan 2007:
Changed from using AES-Key to IETF's ESP

Revision 5, 11 March 2007:
Changes based on January meeting

Revision 6, 24 April 2007:
Most of this text was moved to SPC-4 in 07-169 (ESP-SCSI). The only thing left is making a new key type that uses ESP-SCSI to wrap the key.

Related Documents

T10/07-169r0 “ESP-SCSI Security for Parameter Data”
T10/SSC-3 r3c "SCSI Stream Commands 3"
T10/06-369r8 (Ralph Weber, ENDL Texas) "Security Association Model for SPC-4"
T10/06-449r1 (Matt Ball and David Black) "SPC-4: Establishing a Security Association using IKEv2"
T11 FC-SP/06-157v2 "Fibre Channel Security Protocols (FC-SP)"
NIST FIPS 140-2 "Security Requirements for Cryptographic Modules"
NIST FIPS 140-2, Annex D "Approved Key Establishment Techniques"
NIST FIPS 140-2 IG "Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program"
IEEE 802.11i "Amendment 6: Medium Access Control (MAC) Security Enhancements"
IETF RFC 4303 "IP Encapsulating Security Payload (ESP)"
IETF RFC 4306 “Internet Key Exchange (IKEv2) Protocol”

General

NOTE – This proposal assumes the incorporation of 06-449r4 and 07-169r0 (or later) into SPC-4.

The purpose of this proposal is to provide a way for the application client to pass an encrypted key to the device server (note: this is different from passing an *encryption* key; the goal is to encrypt the encryption key). This feature has some of the following benefits:

- It is possible to hide the encryption key from an eavesdropper. Generally, the encryption key is more valuable than the data, so it is important to keep this information safe.
- To comply with NIST FIPS 140-2, it is necessary to encrypt the key before passing it to the device server. Currently, there is no method in SSC-3 to provide a FIPS-compliant solution.
- By using a security association, it is possible to enter several keys using fast symmetric-key encryption (as compared to slow public-key operations). The only cost is an up-front cost to perform a Diffie-Hellman operation to establish a shared secret.

To comply with FIPS 140-2, it is necessary to enter a key into a cryptographic module (device server) using an Approved encryption algorithm. By using ESP-SCSI (see SPC-4 with 07-169), it is possible to fulfill this requirement.

Proposed Changes

Note: Some headings are used only to keep the numbering consistent. (Proposed changes are in **blue**)

1 Scope

2 Normative references

2.1 Normative references

2.2 Approved references

2.3 References under development

3 Definitions, acronyms, keywords, and conventions

3.1 Acronyms

4 General Concepts

5 Explicit address command descriptions for sequential-access devices

6 Implicit address command descriptions for sequential-access devices

7 Common command descriptions for sequential-access devices

8 Parameters for sequential-access devices

8.1 Diagnostic parameters

8.2 Log Parameters

8.3 Mode Parameters

8.4 Vital product data (VPD) parameters

8.5 Security protocol parameters

8.5.1 Security protocol overview

8.5.2 SECURITY PROTOCOL IN command specifying Tape Data Encryption security protocol

8.5.3 SECURITY PROTOCOL OUT command specifying Tape Data Encryption security protocol

8.5.3.1 SECURITY PROTOCOL OUT command specifying Tape Data Encryption security protocol overview

8.5.3.2 Set Data Encryption page

8.5.3.2.1 Set data encryption page format

Table 117 – KEY FORMAT field values

Code	Description	Reference
00h	The KEY field contains the key to be used to encrypt or decrypt data.	8.5.3.2.2
01h	The KEY field contains a vendor specific key reference	8.5.3.2.3
02h	The KEY field contains the key wrapped by the device server's public key	8.5.3.2.4
03h	The KEY field contains a key that is encrypted using ESP-SCSI	8.5.3.2.5
04h – BFh	Reserved	
C0h – FFh	Vendor specific	

8.5.3.2.2 Plaintext key format

8.5.3.2.3 Key reference format

8.5.3.2.4 Key wrapped by device server public key

8.5.3.2.5 Key encrypted using ESP-SCSI

If the KEY FORMAT field is set to 03h, then the KEY field shall contain an ESP-SCSI out w/o length descriptor (see SPC-4) that includes a key that has been encrypted. The KEY LENGTH field contains the length of the ESP-SCSI out w/o length descriptor.

If the USAGE_TYPE SA parameter in the SA associated with the value in the DS_SAI field in the ESP-SCSI out w/o length descriptor is not set to 0081h (i.e. Tape Data Encryption), then the device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to BAD USAGE TYPE SA PARAMETER.

[note: BAD USAGE TYPE SA PARAMETER is a new ASC]

[Discussion point: Should we require that the device server support a 256-bit SK for encryption. (Should we make P-521 Elliptic curve mandatory as well?) – this question came out of the Houston CAP security meeting]