ENDL
TEXAS

Date: 13 March 2008
To: T10 Technical Committee
From: Ralph O. Weber
Subject: SPC-4 ESP-SCSI field alignments

Introduction

Concerns have been raised about the byte alignment of some of the ESP-SCSI data structures. This proposal attempts to address those problems.

Revision History

r0 Initial revision
r1 Changes requested by the March CAP working group.

Changes between r0 and r1 are indicated by change bars.

Unless otherwise indicated additions are shown in blue, deletions in ~~red strikethrough~~, and comments in green.

Proposed Changes in SPC-4 r13

5.13.7.3 ESP-SCSI data format before encryption and after decryption

Before data bytes are encrypted and after they are decrypted, they have the format shown in table 60.

Table 60 — ESP-SCSI data format before encryption and after decryption

Bit / Byte	7	6	5	4	3	2	1	0
0	UNENCRYPTED BYTES							
p-1								
p	PADDING BYTES							
j-1								
j	PAD LENGTH (j-p)							
j+1	MUST BE ZERO							

The UNENCRYPTED BYTES field contains the bytes that are to be protected via encryption or that have been decrypted.

Before encryption, the PADDING BYTES field contains zero to 255 bytes. The number of padding bytes is:

a) Defined by the encryption algorithm; or
b) The number needed to cause the length of all bytes prior to encryption (i.e., j+2) to be a whole multiple of the ~~cipher block size~~ alignment (see table 398 in 7.6.3.6.2) for the encryption algorithm being used.

18484 Preston Road, Suite 102 PMB 178, Dallas, TX 75252 214-912-1373 972-596-2775 Fx ENDL_TX@computer.org

The contents of the padding bytes are:

a) Defined by the encryption algorithm; or
b) If the encryption algorithm does not define the padding bytes contents, a series of one byte binary values starting at one and incrementing by one in each successive byte (i.e., 01h in the first padding byte, 02h in the second padding byte, etc.).

If the encryption algorithm does not place requirements on the contents of the padding bytes (i.e., option b) is in effect), then after decryption the contents of the padding bytes shall be verified to match the series of one byte binary values described in this subclause. If this verification is not successful in a device server, the command shall be terminated with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, the additional sense code set to INVALID FIELD IN PARAMETER LIST, the SKSV bit set to one, and SENSE KEY SPECIFIC field set to indicate the last byte in the encrypted data as defined in 4.5.2.4.2. If this verification is not successful in an application client, the decrypted data should be ignored.

The PAD LENGTH field contains the number of bytes in the PADDING BYTES field.

The MUST BE ZERO field contains zero. After decryption, the contents of the MUST BE ZERO field shall be verified to be zero. If this verification is not successful in a device server, the command shall be terminated with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, the additional sense code set to INVALID FIELD IN PARAMETER LIST, the SKSV bit set to one, and SENSE KEY SPECIFIC field set to indicate the last byte in the encrypted data as defined in 4.5.2.4.2. If this verification is not successful in an application client, the decrypted data should be ignored.

…

5.13.7.4 ESP-SCSI data-out buffer parameter list data descriptors

5.13.7.4.1 Overview

…

5.13.7.4.2 ESP-SCSI data-out buffer parameter lists including a descriptor length

…

5.13.7.4.3 ESP-SCSI data-out buffer parameter lists for externally specified descriptor length

…

Table 64 — ESP-SCSI data-out buffer parameter list descriptor without length and initialization vector

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
3				DS_SAI				(LSB)
4								
7				Reserved {{add 4 reserved bytes}}				
8	(MSB)							
15				DS_SQN				(LSB)
16								
i-1				ENCRYPTED OR AUTHENTICATED DATA				
i	(MSB)							
n				INTEGRITY CHECK VALUE				(LSB)

…

Table 65 — ESP-SCSI data-out buffer parameter list descriptor without length

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
3				DS_SAI				(LSB)
4								
7				Reserved {{add 4 reserved bytes}}				
8	(MSB)							
15				DS_SQN				(LSB)
16	(MSB)							
~~12+s-1~~ 16+s-1				INITIALIZATION VECTOR				(LSB)
~~12+s~~ 16+s								
i-1				ENCRYPTED OR AUTHENTICATED DATA				
i	(MSB)							
n				INTEGRITY CHECK VALUE				(LSB)

…

5.13.7.5 ESP-SCSI data-in buffer parameter data descriptors

5.13.7.5.1 Overview

…

5.13.7.5.2 ESP-SCSI data-in buffer parameter data including a descriptor length

…

5.13.7.5.3 ESP-SCSI data-in buffer parameter data for externally specified descriptor length

…

Table 69 — ESP-SCSI data-in buffer parameter data descriptor without length and initialization vector

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)							
3				AC_SAI				(LSB)
4								
7				Reserved {{add 4 reserved bytes}}				
8	(MSB)							
15				AC_SQN				(LSB)
16								
i-1				ENCRYPTED OR AUTHENTICATED DATA				
i	(MSB)							
n				INTEGRITY CHECK VALUE				(LSB)

…

Table 70 — ESP-SCSI data-in buffer parameter data descriptor without length

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			AC_SAI				
3								(LSB)
4				Reserved {{add 4 reserved bytes}}				
7								
8	(MSB)			AC_SQN				
15								(LSB)
16	(MSB)			INITIALIZATION VECTOR				
~~12+s-1~~ 16+s-1								(LSB)
~~12+s~~ 16+s				ENCRYPTED OR AUTHENTICATED DATA				
i-1								
i	(MSB)			INTEGRITY CHECK VALUE				
n								(LSB)

…

7.6.3.5.10.2 Encrypted payload introduction

…

The PADDING BYTES field contains zero to 255 bytes. The number of padding bytes is:

a) Defined by the encryption algorithm; or
b) Any number of bytes that causes the length of all plaintext bytes (i.e., l+2) to be a whole multiple of the ~~cipher block size~~ alignment (see table 398 in 7.6.3.6.2) for the encryption algorithm being used.

…

7.6.3.6.2 Encryption algorithm (ENCR) IKEv2-SCSI cryptographic algorithm descriptor

…

Table 398 — ENCR ALGORITHM IDENTIFIER field

Code	Description	Salt [a] length (bytes)	IV [b] length (bytes)	Align-ment [x] (bytes)	Key length (bytes)	Support	Reference
8001 000Bh	ENCR_NULL [c]	n/a	0	4	0	Mandatory	
8001 000Ch	AES-CBC [c]	n/a	16	16	16	Optional	RFC 3602
					24	Prohibited	
					32	Optional	
8001 0010h	AES-CCM with a 16 byte MAC [d]	3	8	4	16	Optional	RFC 4309
					24	Prohibited	
					32	Optional	
8001 0014h	AES-GCM with a 16 byte MAC [d]	4	8	4	16	Optional	RFC 4106
					24	Prohibited	
					32	Optional	
8001 0400h – 8001 FFFFh	Vendor Specific						
0000 0000h – 0000 FFFFh	Restricted						IANA
All others	Reserved						

[a] See RFC 4106 and RFC 4309.

[b] Initialization Vector.

[x] The alignment required in the plaintext prior to encryption.

[c] If the INTEG cryptographic algorithm descriptor (see 7.6.3.6.4) in the same IKEv2-SCSI SA Cryptographic Algorithms payload or the same IKEv2-SCSI SAUT Cryptographic Algorithms payload as this ENCR cryptographic algorithm descriptor has the ALGORITHM IDENTIFIER field set to AUTH_COMBINED, then the error shall be processed as described in 7.6.3.8.3.

[d] If the INTEG cryptographic algorithm descriptor (see 7.6.3.6.4) in the same IKEv2-SCSI SA Cryptographic Algorithms payload or the same IKEv2-SCSI SAUT Cryptographic Algorithms payload as this ENCR cryptographic algorithm descriptor does not have the ALGORITHM IDENTIFIER field set to AUTH_COMBINED, then the error shall be processed as described in 7.6.3.8.3.

…

C.1 IKEv2 protocol details and variations for IKEv2-SCSI

…

y) The description of how combined mode algorithms are used in the Encrypted payload in this standard predates the definition of equivalent functionality in IETF standards. IETF standards omit the Integrity transform instead of using AUTH_COMBINED; ~~and~~

z) The command-response architecture of SCSI makes it difficult to protect the device server against denial of service attacks, and no such protection is defined by this standard. Protection against denial of service attacks against the application client is described in 7.6.3.8~~.~~; and

aa) IKEv2-SCSI requires Encrypted Payloads be padded to at least the 4 byte minimum alignment required by ESP-SCSI, whereas IKEv2 imposes no such requirement.