To: INCITS Technical Committee T10
From: Kevin Butt
Date: August 15, 2007 11:10 am
Document: T10/07-290r2 — SSC-3: Protecting partially encrypted volumes

1. Revisions

07-290r0: Initial revision (June 22, 2007 10:30 am) using SSC-3r03c as base.

07-290r1: (August 10, 2007) Incorporated comments received from Paul Entzel and during the SSC-3 WG in July. Brought into synch with SSC-3r03d.

07-290r2: (August 15, 2007) Received feedback internal to IBM that this proposal does not meet the needs for which it was originally generated. Changed the proposal to more strongly enforce that once there is encryped data on the medium all new data must be encrypted.

2. Introduction

KEY:

~~Deleted Text~~

Added Text

Updates to added text

EDITOR'S NOTE: <Text>

Questions

IBM has had concerns raised by customers intending to use encryption about ensuring that a volume does not mix both encrypted data and unencrypted data. SSC-3 has made efforts to ensure that if a user wishes to mix encrypted data with unencrypted data the standard should allow it.

One method to alleviate the concern about having encrypted and unencrypted data on the same volume is to create a requirement that a volume must be entirely written unencrypted or entirely written encrypted. ~~However, this is counter to the current standard and counter to the stated desires of many on the committee. We do not suggest this method because we see it as too restrictive.~~ The approach this proposal will take is to provide a mode page to select which behavior the drive will employ. One behavior is the behavior of the current standard. The other behavior is once there is any encrypted data on the medium to only allow encrypted data be written from thenceforth.

~~An alternate and better method is to ensure that once a volume has encrypted data on it, that only application clients that understand encryption be allowed to append to that volume. This would alleviate concerns that legacy applications might corrupt volumes that are intended to be encrypted.~~

In practice, volumes are generally assigned to be members of a media pool that are assigned to a single application. If there are multiple applications in a shop, each application is assigned its own media pool so as to not contaminate or destroy data in use by a different application. This is a requirement since each ISV has different meta-data that is stores on each volume.

3. Proposal

4.2.20 Data encryption

4.2.21 Data encryption overview

.

.

.

4.2.22 Appending data to a volume containing encrypted data

A volume contains no encrypted blocks, all encrypted blocks, or a mixture of encrypted blocks and unencrypted blocks.

A device server that supports encryption should be capable of detecting when a mounted volume contains an encrypted block. The device server reports its capability of determining if a volume contains encrypted data through the VCED_C bit in the Data Encryption Algorithm descriptor (see 8.5.2.4). If the device server is capable of distinguishing if a mounted volume contains an encrypted block, it should support the the VCEDRE bit of the Device Configuration Extension mode page (see 8.3.8) being set to one.

If the VCED bit of the Data Encryption Status page is set to one and a command is received the device server shall terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to ENCRYPTION PARAMETERS NOT USEABLE if:

a) the VCEDRE bit of the Device Configuration Extension mode page is set to one;

b) the encryption mode of the set of data encryption parameters in use by the I_T nexus on which the command arrived is set to DISABLE;

c) the logical object identifier does not equal zero; and

d) the command is a:

   A) WRITE(6);

   B) WRITE(16);

   C) WRITE FILEMARKS(6);

   D) WRITE FILEMARKS(16);

   E) ERASE(6); or

   F) ERASE(16).

EDITOR'S NOTE: This does not require encryption or decryption to be enabled for read type commands - even if encrypted data is between the Logical Object Identifier and BOT.

EDITOR'S NOTE: Since VCED is not position aware, this requires that a write that may be attempted at a location prior to any encrypted data still requires encryption to be enabled.

EDITOR'S NOTE: This effectively is a psuedo write protect for appends but not for an overwrite from BOP.

4.2.23 Encrypting data on the medium

EDITOR'S NOTE: No changes other than new paragraph number

8.3.8 Device Configuration Extension mode page

The Device Configuration Extension mode page (see table 89), a subpage of the Device Configuration mode page (see 8.3.3), provides control of the SCSI features specific to sequential-access devices. If a device server supports the Device Configuration Extension mode page, the device server shall provide access to the mode page using the shared mode page policy (see SPC-4).

TABLE 89. Device Configuration Extension mode page

Byte	Bit							
	7	6	5	4	3	2	1	0
0	PS	SPF (1b)	PAGE CODE (10h)					
1	SUBPAGE CODE (01h)							
2	(MSB)	PAGE LENGTH (1Ch)						
3								(LSB)
4	Reserved				TARPF	TASER	TARPC	TAPLSD
5	Reserved				SHORT ERASE MODE			
6	Reserved							VCEDRE
7	Reserved							
31								

.

.

.

The volume containing encrypted data requires encryption (VCEDRE) bit set to one indicates that when the VCED bit of the Data Encryption Status page is set to one, the device server shall require that any logical blocks written to the medium are encrypted (see 4.2.22). An VCEDRE bit set to zero indicates that device server does not use the VCED bit of the Data Encryption Status page to determine if encryption is required for writing logical blocks.

8.5.2.4 Data Encryption Capabilities page

.

.

.

TABLE 99. Data Encryption Algorithm descriptor

Byte	Bit							
	7	6	5	4	3	2	1	0
0	ALGORITHM INDEX							
1	Reserved							
2	(MSB)	DESCRIPTOR LENGTH (20)						
3								(LSB)
4	AVFMV	SDK_C	MAC_C	DED_C	DECRYPT_C		ENCRYPT_C	
5	AVFCLP		NONCE_C		Reserved	VCED_C	UKADF	AKADF
6	(MSB)	MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED DATA BYTES						
7								(LSB)
8	(MSB)	MAXIMUM AUTHENTICATED KEY-ASSOCIATED DATA BYTES						
9								(LSB)
10	(MSB)	KEY SIZE						
11								(LSB)
12	Reserved				RDMC_C			EARM
13	(MSB)	Reserved						
19								(LSB)
20	(MSB)	SECURITY ALGORITHM CODE						
23								(LSB)

.

.

.

The A-KAD Fixed (AKADF) bit shall be set to one if the device server requires the length of A-KAD in the parameter data for a SECURITY PROTOCOL OUT command to equal the value in the MAXIMUM AUTHENTICATED KEY-ASSOCIATED BYTES field. If the AKADF bit is set to one, then the MAXIMUM AUTHENTICATED KEY-ASSOCIATED BYTES field shall contain a non-zero value. If the AKADF bit is set to zero and the value in the MAXIMUM AUTHENTICATED KEY-ASSOCIATED BYTES field is non-zero, then the length of the A-KAD, if present in the parameter data for a SECURITY PROTOCOL OUT command, shall be a value between one and the value in the MAXIMUM AUTHENTICATED KEY-ASSOCIATED BYTES field.

The volume contains encrypted data capable (VCED_C) bit shall be set to one if the device server is capable of detecting that a volume contains data encrypted using this algorithm when the volume is mounted. The VCED_C bit shall be set to zero if the device server is not capable of distinguishing that a volume contains data encrypted using this algorithm when the volume is mounted. If the capability of detecting that a volume contains data encrypted using this algorithm is format specific and a volume is mounted, the VCED_C bit shall be set based on the current format of the medium. If no volume is mounted, the VCED_C bit shall be set to one if for at least one algorithm that the device server supports the device server is capable of detecting that a volume contains data encrypted using that algorithm.

The MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED DATA BYTES field indicates the maximum size of the unauthenticated key-associated data (see 4.2.20.11) that the device server can support for this algorithm.

.

.

.

8.5.2.7 Data Encryption Status page

Table 107 specifies the format of the Data Encryption Status page.

TABLE 107. Data Encryption Status page

Byte	Bit							
	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0020h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (n-3)				
3								(LSB)
4	I_T NEXUS SCOPE			Reserved		KEY SCOPE		
5	ENCRYPTION MODE							
6	DECRYPTION MODE							
7	ALGORITHM INDEX							
8	(MSB)			KEY INSTANCE COUNTER				
11								(LSB)
12	Reserved				VCED	CEEMS		RDMD
13				Reserved				
23								
24				KEY-ASSOCIATED DATA DESCRIPTORS LIST				
n								

The I_T NEXUS SCOPE field shall contain the value from the data encryption scope saved for the I_T nexus on which this command was received (see 4.2.20.7).

The KEY SCOPE field shall contain the value from the key scope in the saved data encryption parameters currently associated with the I_T nexus on which this command was received (see 4.2.20.8).

The ENCRYPTION MODE field shall contain the value from the encryption mode in the saved data encryption parameters currently associated with the I_T nexus on which this command was received (see 4.2.20.8).

The DECRYPTION MODE field shall contain the value from the decryption mode in the saved data encryption parameters currently associated with the I_T nexus on which this command was received (see 4.2.20.8).

The ALGORITHM INDEX field shall contain the value from the algorithm index in the saved data encryption parameters currently associated with the I_T nexus on which this command was received (see 4.2.20.8). If the ENCRYPTION MODE field and the DECRYPTION MODE field are both set to DISABLE, the value in the ALGORITHM INDEX field is undefined.

The KEY INSTANCE COUNTER field contains the value of the key instance counter (see 4.2.20.9) assigned to the key indicated by the KEY SCOPE field value.

The raw decryption mode disabled (RDMD) bit shall be set to one if the device server is configured to mark each encrypted record as disabled for raw read operations based on the RDMC_C value and the raw decryption mode disable parameter in the saved data encryption parameters currently associated with the I_T nexus on which the command was received (see 4.2.20.7).

The check external encryption mode status (CEEMS) field shall contain the value from the check external encryption mode parameter in the saved data encryption parameters currently associated with the I_T nexus on which the command was received (see 4.2.20.7).

If the ENCRYPTION MODE field and the DECRYPTION MODE field are both set to DISABLE, the KEY-ASSOCIATED DATA DESCRIPTORS LIST field shall not be included in the page.

The volume contains encrypted data (VCED) bit shall be set to one when a volume is loaded that contains encrypted data. The VCED bit shall be set to zero if the mounted volume does not contain any encrypted data. The VCED bit shall be set to zero if there is no mounted volume or if the device server is not capable of detecting if a mounted volume contains any encrypted data.

If either the ENCRYPTION MODE field or the DECRYPTION MODE field is set to a value other than DISABLE, the KEY-ASSOCIATED DATA DESCRIPTORS LIST field shall contain data security descriptors (see 8.5) describing attributes assigned to the key defined by the I_T NEXUS SCOPE and KEY SCOPE fields at the time the key was established in the device server. If more than one key associated descriptor is included, they shall be in order of increasing value of the DESCRIPTOR TYPE field. Descriptors shall be included as defined by the following paragraphs.

An unauthenticated key-associated data descriptor (see 8.5.4.3) shall be included if an unauthenticated key-associated data descriptor was included when the key was established in the device server. The AUTHENTICATED field is reserved. The KEY DESCRIPTOR field shall contain the U-KAD value associated with the key.

An authenticated key-associated data descriptor (see 8.5.4.4) shall be included if an authenticated key-associated data descriptor was included when the key was established in the device server. The AUTHENTICATED field is reserved. The KEY DESCRIPTOR field shall contain the A-KAD value associated with the key.

A nonce value descriptor (see 8.5.4.5) shall be included if a nonce value descriptor was included when the key was established in the device server. The AUTHENTICATED field is reserved. The KEY DESCRIPTOR field shall contain the nonce value associated with the key. A nonce value descriptor may be included if no nonce value descriptor was included when the key was established in the device server. In this case, the KEY DESCRIPTOR field shall be set to the nonce value established by the device server for use with the selected key.

A metadata key-associated data descriptor (see 8.5.4.6) shall be included if the metadata key-associated data descriptor was included when the data encryption parameters were established. The KEY DESCRIPTOR field shall contain the M-KAD value associated with the key.