To: INCITS Technical Committee T10
From: Kevin Butt
Date: July 2, 2007 8:58 am
Document: T10/07-290r0 — SSC-3: Protecting partially encrypted volumes

1. Revisions

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

2. Introduction

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.

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.

KEY:

~~Deleted Text~~

Added Text

Updates to added text

EDITOR’S NOTE: <Text>

Questions

3. Proposal

4.2.20 Data encryption

4.2.21 Data encryption overview

.

.

.

4.2.22 Accessing data on a volume containing encrypted data

A volume may contain 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 CEDD_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 E_SDEPR bit of the Device Configuration Extension mode page (see 8.3.8) being set to one.

If the E_SDEPR bit of the Device Configuration Extension mode page is set to one, a command received on an I_T nexus prior to receiving a Security Protocol Out command setting the data encryption parameters that will be used for that I_T nexus after the release of the resources used to save a set of data encryption parameters for that I_T nexus shall cause the device server to 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 and establish the logical position at the BOP side of the encrypted block if that command would cause:

a) a block to be read;

b) a block to be verified; or

c) at a beginning location that is not BOP:

  A) an erase of a logical object; or

  B) a write of a logical object; or

EDITOR’S NOTE: This effectively is a psuedo write protect for appends but not for an overwrite from BOP. At least until the SPOUT command.
Note that a logical object includes filemarks.

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							E_SDEPR
7	Reserved							
31								

.

.

.

The enable set data encryption parameters required (E_SDEPR) bit set to one indicates that the SDEPR bit of the Data Encryption Capabilities page shall be used. An E_SDEPR bit set to zero indicates that the SDEPR bit of the Data Encryption Capabilities page shall not be used.

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	Reserved		NONCE_C		Reserved		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					VCED	SDEPR	CEDD_C
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 contains encrypted data detection capable (CEDD_C) bit shall be set to one if the device server is capable of detecting that a volume contains encrypted data when the volume is mounted. The CEDD_C bit shall be set to zero if the device server is not capable of distinguishing that a volume contains encrypted data when the volume is mounted. If the capability of detecting that a volume contains encrypted data is format specific and a volume is mounted, the CEDD_C bit shall be set based on the current format of the medium. If no volume is mounted, the CEDD_C bit shall be set to one if the device server is capable of detecting that a volume contains encrypted data in any format that the device server supports.

If the E_SDEPR bit of the Device Configuration Extension mode page (see 8.3.8) is set to one, the set data encryption parameters required (SDEPR) bit shall be set to one for each I_T nexus after the release of the resources used to save a set of data encryption parameters. The SDEPR bit for an I_T nexus shall be set to zero when:

a) the data encryption scope for that I_T nexus is set to LOCAL;

b) the data encryption scope for any I_T nexus is set to ALL I_T NEXUS;

c) the device server successfully completes the processing of Set Data Encryption page with a scope value of ALL I_T NEXUS from that I_T nexus; or

d) the E_SDEPR bit of the Device Configuration Extension mode page is set to zero.

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.

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.

.

.

.