SSC-3 Working Group Agenda (07-126r0)
Date: March 13, 2007
Time: 11:00am-7pm
Location: Memphis, TN

Agenda

1. Opening remarks and introductions

2. Approval of agenda

3. Approval of meeting minutes (07-036r0, 07-070r0)

4. Review of old action items [Butt]

5. Old business

5.1 General items

5.1.1 Vendor Feedback (05-351r1) [Group]

5.1.2 Configurable EW (05-423r3) [Butt]

5.1.3 TapeAlert Delineation (06-138r3) [Butt]

5.2 Security-related items

5.2.1 Using NIST AES Key-Wrap for Key Establishment (06-225r5) [Ball]

5.2.2 Keyless Copy of Encrypted Data (06-462r4) [Butt]

5.2.3 Encryption Error Behavior when unsupported medium is loaded (07-005r1) [Butt]

5.2.4 Additional controls for keyless copy (07-016r1) [Entzel]

6. New Business

6.1 General items

6.1.1 Cleaning Model (05-285r0) [Butt]

6.1.2 Requested Recovery log page (07-046r1) [Banther]

6.2 Security-related items

7. Liaison reports

7.1 P1619 Status Report [Ball]

8. Project status

8.1 Next meeting requirements (Seattle, WA)

8.2 Target date for letter ballot - Nov 2007

9. Review of new action items

10. Adjournment

Attendance

SSC-3 Working Group Attendance Report - March 2007

Name	S	Organization
Mr. Noud Snelder	V	BDT
Mr. David Peterson	P	Brocade
Mr. Robert Snively	A	Brocade
Mr. Gideon Avida	P	Decru
Mr. David Black	A	EMC Corp.
Mr. Robert H. Nixon	A	Emulex
Mr. Ralph O. Weber	P	ENDL Texas
Mr. Curtis Ballard	V	Hewlett Packard Co.
Mr. Michael Banther	A	Hewlett Packard Co.
Mr. Christopher Williams	V	Hewlett Packard Co.
Mr. Kevin Butt	A	IBM Corp.
Mr. Landon Noll	AV	NeoScale Systems Inc.
Mr. Frederick Knight	A	Network Appliance
Mr. Matthew Ball	V	Quantum Corp.
Mr. Paul Entzel	P	Quantum Corp.
Dr. Paul Suhler	A	Quantum Corp.
Mr. Erich Oetting	P	Sun Microsystems, Inc.
Mr. Scott Painter	A#	Sun Microsystems, Inc.

18 People Present

Status Key:			
	P	-	Principal
	A,A#	-	Alternate
	AV	-	Advisory Member
	E	-	Emeritus
	L	-	Liaison
	V	-	Visitor

Results of Meeting

1. Opening remarks and introductions [Peterson]

Dave thanked SCSI Trade Association (STA) for hosting.

2. Approval of agenda (07-040r0) [Peterson]

Dave Petereson moved that the agenda as revised be approved. Paul Entzel seconded the motion. Passed unanimously.

3. Approval of meeting minutes (07-036r0; 07-070r0) [Peterson]

The date on the January minutes needs corrected. Dave Petereson moved for approval of 07-036r1 (07-036r0 as revised) and for approval of 07-070r0 and Erich Oetting seconded. Passed unanimously.

4. Review of old action items [Butt]

4.1 Dave Peterson: Bring in a White Paper on the value added with Explicit Command Set.

Carry-Over

4.2 Michael Banther: Bring in proposal to improve handling of cleaning and firmware upgrade cartridges.

Carry-Over

4.3 Michael Banther: Bring in proposal for Requested Recovery log page from ADC.

Completed by 07-046r1.

4.4 Kevin Butt: add cleaning bits from 05-213 to his proposal and find log page for them.

Kevin couldn’t find this. Dave said he would help look for this.

Carry-Over

4.5 Roger Cummings: produce a proposal to describe the events that shall activate and deactivate the cleaning related tape alert flags and to add a second flag for predictive failure of the medium.

Carry-Over

4.6 Micheal Banther: Create a proposal to add additional activation conditions to TapeAlert. See note in 05-154r3 to bring in new proposal for this additional info.

Carry-Over

4.7 Kevin Butt to revise and post Configurable EW (05-423r3)

Carry-Over

4.8 [Kevin Butt] Revise and post TapeAlert Delineation (06-138r2)

Completed by 06-138r3

4.9 [Matt Ball] to revise and post SSC-3: Key Entry using Encapsulating Security Payload (ESP) (06-225r4)

Carry-Over

4.10 [Gideon Avida] Revise and post Using Public-Key Cryptography for Key Wrapping (06-389r4)

Completed by 06-389r5

4.11 [Dave Peterson] Incorporate into SSC-3 Using Public-Key Cryptography for Key Wrapping (06-389r5)

Carry-Over

4.12 [Paul Suhler] Revise and post Encryption KAD lengths, Nonces, and Resets (06-412r2)

Completed by 06-412r3

4.13 [Dave Peterson] Incorpoarate into SSC-3 Encryption KAD lengths, Nonces, and Resets (06-412r3)

Completed in SSC-3r03c

5. Old business

5.1 General items

5.1.1 Vendor Feedback (05-351r1) [Group]

5.1.2 Configurable EW (05-423r3) [Butt]

Deferrred.

5.1.3 TapeAlert Delineation (06-138r3) [Butt]

Parameter codes must be returned in ascending order.

Only parameters related to flags asserted shall be returned, but the flag clears when the tapealerts are returned. Need to word it in relation to condition is active/deactive.

Be clear about reading multiple times and what the clearing/non-clearing behavior is.

Make the format a descriptor list and add a code in byte 0 of each descriptor that indicates which descriptor it is. Make sure to specify there can only be one instance of each descriptor.

Remove vendor-specific from each descriptor since there is a vs descriptor.

The DEVICE COMPONENT CODE should be broken into a hierarchy of codes similar to ASC/ASCQ and use three levels of hierarchy with perhaps the third level being a text field or index to text field.

Kevin stated that the device severity code field is intended to replace the existing TapeAlert flags severity. Ralph reguested that spaces be added between values to allow for future expansion and to convert to a 3-column table. (i.e. Value, Severity, Description)

Michael Banther accepted an action to update 06-420r0 to match the device severity code definition table from 06-138r4.

Kevin agreed to revise and post.

5.2 Security-related items

5.2.1 Using NIST AES Key-Wrap for Key Establishment (06-225r5) [Ball]

Matt described his updates that will plug into Ralph Weber's security association proposal. ESP-SCSI which is a subset of ESP mapped onto SCSI.

Ralph Weber stated this proposal has material that belongs in SPC. Matt asked if he could do this is SSC WG before taking this to SPC. David Black wants to get this done in SSC-3

Matt Ball, David Black, and Ralph Weber are going to get together to do this.

5.2.2 Keyless Copy of Encrypted Data (06-462r4) [Butt]

Kevin presented his changes and agreed to revise and post.

5.2.3 Encryption Error Behavior when unsupported medium is loaded (07-005r1) [Butt]

Kevin covered the changes to his proposal. There was a very heated discussion on removing from the list of events that shall clear encryption parameters, item e) a volume is mounted that does not support data encryption using the algorithm specified by the algorithm index in the data encryption parameter. Kevin Butt, Gideon Avida, and Ralph Weber were on the side of removing it, or at least moving to a may list. Paul Entzel was on the side of keeping it since removing it would break his implementation. After a long heated debate is was agreed to move it and the vendor specific events into a may list. Paul raised a concern of this should be something that is configured and reported, but was eventually convinced that it was not necessary.

Kevin Butt moved that Encryption Error Behavior when unsupported medium is loaded (07-005r1) as modified be include in SSC-3 and Bob Nixon seconded. The motion passed on a vote of 4:0:6.

Kevin Butt has an action to revise and post Encryption Error Behavior when unsupported medium is loaded (07-005r1)

Dave Peterson has an action to incorporate Encryption Error Behavior when unsupported medium is loaded (07-005r2)

REMOVE FROM AGENDA

5.2.4 Additional controls for keyless copy (07-016r1) [Entzel]

Paul went through this proposal for the first time.

David Black this is morally equivalent to consenting adults in tape drives. Kevin Butt argued strongly that adding a knob to control if the drive allows raw read is the wrong thing to do. He lost his argument.

Kevin Butt argued that since RAW read is allowed today a value of zero better allow it.

Paul Entzel suggested that we just have two different algorthims, one that allows raw read and one that disallows raw read. After some discussion Ralph Weber said that it did not solve anything but is just Whipped Cream on road kill. the descision was made to put this info into a field to allow zero to refer to a vendor-specific default.

Ralph Weber said the RDME_C bit is described incorrectly. He reworded this so a value of zero “does not allow the application client to contol the use of raw....”

Time was called and the group moved on to other agenda items.

5.2.5 IKEv2 for CAP (06-449r2) [Black]

This was newly added during agenda modification.

6. New Business

6.1 General items

6.1.1 Cleaning Model (05-285r0) [Butt]

Deferred

6.1.2 Requested Recovery log page (07-046r1) [Banther]

Michael started describing this proposal as being brought over from ADC-2. Paul Entzel identified a problem with the Recover requested bit, tafc, and some other bits in the physical device that now will have a race condition with SSC and ADC both being able to clear the bits and starve the other device server. This needs to be addressed. Michael agreed to take that into consideration.

Table Y+3 Recovery Procedures was discussed. The discussion revolved around consistency with the comporable list in ADC. Paul Entzel wishes to make these two tables different and to have the device server ensure they do not interfere with each other.

Paul Entzel wants to keep the two tables as similar as possible. Discussion also revolved around if this should be supported if the drive is in a library. No change was made because of this discussion.

6.2 Security-related items

No new security related items.

7. Liason reports

7.1 P1619.1 Status report [Ball]

8. Project Status

8.1 Next Meeting Requirements (Memphis, TN)

Request same time for May 8.

Conference call on April 10 at 8:00 PDT - 10:00 PDT

8.2 Target date for letter ballot.

Nov 2007

9. Review of new action items

9.1 [Kevin Butt] revise and post Keyless Copy of Encrypted Data (06-462r4)

9.2 [Kevin Butt] has an action to revise and post Encryption Error Behavior when unsupported medium is loaded (07-005r1)

9.3 [Dave Peterson] has an action to incorporate Encryption Error Behavior when unsupported medium is loaded (07-005r2) into SSC-3

9.4 [Kevin Butt] revise and post TapeAlert Delineation (06-138r3)

9.5 [Michael Banther] accepted an action to update 06-420r0 to match the device severity code definition table from 06-138r4.

10. Adjournment

Dave Peterson made a motion for adjournment at 7:00 pm PST. Seconded by Bob Nixon.