SCSI Stream Commands - 3: Working Group Minutes – Draft (T10/06-494r0)
Date: Nov 07, 2006
Time: 9:00 am - 5:00 pm
Location: Las Vegas, NV

Agenda

1. Opening remarks and introductions [Peterson]

2. Approval of agenda (06-482r0) [Peterson]

3. Approval of meeting minutes (06-429r0) [Peterson]

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 Add WORM VERSION field to Sequential Access Device Capabilities VPD page (05-391r0) [Banther]

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

5.1.4 Position after Self-Test (05-140r1) [Banther]

5.1.5 TapeAlert Delineation (06-138r2) [Butt]

5.2 Security-related items

5.2.1 Using NIST AES Key-Wrap for Key Establishment (06-225r3) [Ball]

5.2.2 Authentication Concerns for Encrypted Key Transfer (06-329r0) [Cummings]

5.2.3 Using Public-Key Cryptography for Key Wrapping (06-389r1) [Avida]

5.2.4 Security Association creation (06-492r1) [Black]

5.2.5 Encryption KAD lengths, Nonces, and Resets (06-412r1) [Suhler]

5.2.6 Keyless Copy of Encrypted Data (06-462r0) [Butt]

5.2.7 Add a random number page to the Tape Data Encryption protocol (06-453r0) [Entzel]

6. New Business

6.1 General items

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

6.2 Security-related items

6.2.1 Review of T10/06-389r1: Using Public-Key Cryptography for Key Wrapping (06-493r0) [Black]

6.2.2 Alternative method for keyless tape copy (06-502r0) [Entzel]

7. Liason reports

7.1 P1619.1 Status report (06-504r0)[Ball]

8. Next Meeting Requirements (Orlando)

9. Review of new action items

10. Adjournment

Attendance

SSC-3 Working Group Attendance Report - November 2006

Name	S	Organization
Mr. Robert Snively	P	Brocade Comm. Systems, Inc.
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. Walt Hubis	V	Engenio Information Tech.
Mr. Michael Banther	A	Hewlett Packard Co.
Mr. Christopher Williams	V	Hewlett Packard Co.
Mr. Eric Hibbard	V	Hitachi Data Systems
Mr. Glen Jaquette	V	IBM
Mr. Kevin Butt	A	IBM Corp.
Mr. David Peterson	P	McDATA
Mr. Larry Hofer	V	McDATA Corp
Mr. Landon Noll	AV	NeoScale Systems Inc.
Mr. Frederick Knight	A	Network Appliance
Mr. Craig W. Carlson	AV	QLogic Corp.
Mr. Matthew Ball	V	Quantum Corp.
Mr. Paul Entzel	P	Quantum Corp.
Dr. Paul Suhler	A	Quantum Corp.
Mr. Gerald Houlder	P	Seagate Technology
Mr. Erich Oetting	A#	Sun Microsystems, Inc.
Mr. Roger Cummings	P	Symantec
Mr. Anders Liverud	AV	Tandberg Storage

23 People Present

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

Results of Meeting

1. Opening remarks and introductions [Peterson]

Dave Peterson thanked Hitachi Global Storage Technology for hosting and people introduced themselves.

2. Approval of agenda (06-482r0) [Peterson]

The Agenda was modified to remove already closed items.

Dave Peterson made motion to approve agenda as modified. Michael Banther seconded. Voting was unanimous.

3. Approval of meeting minutes (06-429r0) [Peterson]

Dave Peterson made a motion to approve the minutes. Kevin Butt seconded. Voting was unanimous.

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.

Carry-Over

4.4 Kevin Butt: Bring proposal following direction related to clean behavior.

05-285r0. Done.

4.5 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.

4.6 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

4.7 Banther: Revise and post SSC-3 Add WORM VERSION field to Sequential Access Device Capabilities VPD page (05-391r0)

Closed. Proposal Withdrawen.

4.8 Kevin Butt: Provide associated text, inside the cleaning proposal for 2.1.1 of 05-351r2.

Closed

4.9 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

4.10 [Roger Cummings; David Black] Decide what to do about item 5.9 (06-329r0)

Carry-Over

4.11 [David Peterson] Incorporate "Remove IV fields from the Data Encryption Algorithm descriptor (06-391r0)" into SSC-3

Cosed.

4.12 [Paul Entzel] Revise and post "Modifications to Tape Data Encryption (06-385r0)"

Closed.

4.13 [Dave Peterson] Incorporate "Modifications to Tape Data Encryption (06-385r0)" into SSC-3

Closed.

4.14 [Dave Peterson] Modify clause 4.2.19.2 of SSC-3r3a to add L per discussion item 6.6.

Closed.

4.15 [Kevin Butt] Query ISV's about UA vs No Sense in Configurable EW (05-423r1)

Closed.

4.16 [Kevin Butt] Revise and post Configurable EW (05-423r1)

Closed.

4.17 [Kevin Butt] Revise and post TapeAlert Delineation (06-138r1)

Closed.

5. Old business

5.1 General items

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

Defer.

5.1.2 Add WORM VERSION field to Sequential Access Device Capabilities VPD page (05-391r0) [Banther]

Withdraw. Remove from agenda.

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

Feedback was taken to make PEW into a zone.

AI: Kevin Butt to revise and post Configurable EW (05-423r3). May cover later if time available or in a conference call.

5.1.4 Position after Self-Test (05-140r1) [Banther]

Michael Banther made a motion to include 05-140r1 in SSC-3. Seconded by Erich Oetting. Motion passed unanimously.

AI: Dave Peterson to incorporate 05-140r1 into SSC-3. Remove this item from the agenda.

5.1.5 TapeAlert Delineation (06-138r2) [Butt]

Ran out of time

5.2 Security-related items

5.2.1 Using NIST AES Key-Wrap for Key Establishment (06-225r3) [Ball]

Defer

5.2.2 Authentication Concerns for Encrypted Key Transfer (06-329r0) [Cummings]

Defer

5.2.3 Using Public-Key Cryptography for Key Wrapping (06-389r1) [Avida]

Gideon presented the proposal. The intent is to protect the keys between the tape drive and the key manager. There is typically a weak link in between which is an open OS (e.g. Windows, Linux). So we need to protect the key from the backup server (i.e. midpoints).

There was a discussion of the threats this proposal is attempting to cover.

There was discussion about how this doesn't cover key replay.

David Black is concerned that there is no standard way to do setup enrollment.

Roger Cummings pointed out that maybe this should be named to clarify that this key is not for the media but for the drive.

A lot of discussion centered around the Key Format field.

Concerns about Recipient Id/Sender ID and how they are being used here vs. elsewhere.

David Black offered to review the proposal especially related to RSA with Gideon offline.

Dave Peterson to setup a Phone conference for Dec. 11 at 9:00am - 11:00am PST.

AI: Gideon revise and post Using Public-Key Cryptography for Key Wrapping (06-389r1)

5.2.4 Security Association creation (06-492r1) [Black]

This is how we are going to go about creating a security association. Moving to CAP meeting and will be covered there.

5.2.5 Encryption KAD lengths, Nonces, and Resets (06-412r1) [Suhler]

Bob Snively is concerned about KAD data not being specified and the tape generating the KAD itself. It was described that the tape drive doesn't create its own, but might pad a fixed length optional KAD.

Discussion was that it is preferred to have one method that is always use.

There was a suggestion to include a bit in the algorithm descriptor to specify if the KAD is padded.

AI:Paul Suhler to revise and post Encryption KAD lengths, Nonces, and Resets (06-412r1)

5.2.6 Keyless Copy of Encrypted Data (06-462r0) [Butt]

Chris Williams raised a concern about being able to rearrange or drop blocks using keyless copy.

Paul Entzel claimed that this proposal will break his implementation. He has some text about how it could be done differently. After much debate and expressed concern about needing to get this approved quickly, this item was pushed off to a phone conference.

5.2.7 Add a random number page to the Tape Data Encryption protocol (06-453r0) [Entzel]

Modifications to definitions to reference SPC-4 definitions. The question was asked how this was envisioned to be used. "A customer wants to use this for a key identifier.

Paul Entzel made a motion to include 06-453r0 as modified into SSC-3. Roger Cummings seconded. Motion passed 7:0:8.

Chris Williams was concerned about how this might open security holes if used too often to generate keys.

AI: Dave Peterson to include Add a random number page to the Tape Data Encryption protocol (06-453r0) as modified into SSC-3

6. New Business

6.1 General items

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

6.2 Security-related items

6.2.1 Review of T10/06-389r1: Using Public-Key Cryptography for Key Wrapping (06-493r0) [Black]

David will take this up with Gideon offline.

Withdraw from agenda.

6.2.2 Alternative method for keyless tape copy (06-502r0) [Entzel]

Paul showed this proposal as a concept. It is intended as an alternative to 5.2.6. Kevin Butt looked at this and thinks it might be feasible. He will review and a phone conference will be set up to resolve this keyless copy issues.

7. Liason reports

7.1 P1619.1 Status report (06-504r0)[Ball]

Can setup for Letter ballot by becoming member of IEEE-SA and requesting to be on letter ballot.

8. Next Meeting Requirements (Orlando)

Conference call on Dec 11. for Security.

Same time.Tuesday

9. Review of new action items

9.1 Dave Peterson to incorporate 05-140r1 into SSC-3

9.2 Dave Peterson to include Add a random number page to the Tape Data Encryption protocol (06-453r0) as modified into SSC-3

9.3 Paul Suhler to revise and post Encryption KAD lengths, Nonces, and Resets (06-412r1)

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

9.5 Gideon revise and post Using Public-Key Cryptography for Key Wrapping (06-389r1)

9.6 Kevin Butt to revise and post Keyless Copy of Encrypted Data (06-462r0)

10. Adjournment

Dave Peterson made a motion for adjournment at 4:15 pm PST. Seconded by Kevin Butt.