SCSI Stream Commands - 3: Working Group Minutes – Draft (T10/06-244r0)
Date: January 10, 2006
Time: 10:00 am - 5:00 pm
Location: Hilton Head, SC

Agenda

1. Opening remarks and introductions [Peterson]

2. Approval of agenda (06-056r0) [Peterson]

3. Approval of meeting minutes (05-434r0) [Peterson]

4. Review of old action items [Butt]

5. Next meeting requirements (San Jose, CA)

6. Review of new action items

7. Adjournment

Attendance

SSC-3 Working Group Attendance Report - May 2006

Name	S	Organization
Mr. Noud Snelder	V	BDT
Mr. Robert Snively	P	Brocade Comm. Systems, Inc.
Mr. Gideon Avida	P	Decru
Mr. David Black	A	EMC Corp.
Mr. Ralph O. Weber	P	ENDL Texas
Mr. Walt Hubis	V	Engenio Information Tech.
Mr. Michael Banther	V	Hewlett Packard Co.
Mr. Kevin Butt	A	IBM Corp.
Mr. David Peterson	P	McDATA
Mr. Robert Lockhart	AV	NeoScale Systems Inc.
Mr. Landon Noll	AV	NeoScale Systems Inc.
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. Kjartan Nesbakken Haugen	AV	Tandberg Storage

```
18 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 NVIDIA for hosting and people introduced themselves.

2. Approval of agenda (06-241r0) [Peterson]

Dave Peterson made motion to approve agenda as modified. Erich Oeting seconded. Voting was unanimous.

3. Approval of meeting minutes (06-178r0, 06-162r0, 06-142r0) [Peterson]

Dave Peterson made a motion to approve the minutes. Gerry Houlder 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 Dave Peterson: Review initiator vs I_T nexus throughout document.

Carry-Over.

4.3 Michael Banther: Bring in proposal to improve handling of cleaning and firmware upgrade cartridges.
Carry-Over.

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

Carry-Over.

4.5 Michael Banther: proposal against the “Cleaning Required” parameter of Sequential Access Device log page to make it consistent with TapeAlert and ADC eventually

Closed. 06-235r0.

4.6 Michael Banther: revise and post 05-140r0

Carry-Over.

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

Carry-Over.

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

Carry-Over.

4.9 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.

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

Carry-Over.

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

Carry-Over.

4.12 Kevin Butt: revise and post Configurable EW (05-423r0)

Carry-Over.

4.13 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.

4.14 Dave Peterson: Create a proposed document for feedback to the ISV's.

Carry-Over.

4.15 Rod Wideman to revise and post SSC-3: Target Device Serial Number subpage (05-155r3)

Done.

4.16 Dave Peterson to incorporate SSC-3: Target Device Serial Number subpage (05-155r4) into SSC-3
Carry-Over.

4.17 Dwayne to revise and post The Requirement for More than One Decryption Key (06-051r4)

Done

4.18 Kevin Marks revise and post SSC-3: Device Statistics log page for SSC-3 and Tape Diagnostic Data log page (05-213r4) as modified.

Done.

4.19 Dave Peterson to incorporate SSC-3: Device Statistics log page for SSC-3 and Tape Diagnostic Data log page (05-213r5)

Done

5. Old business

5.1 SSC-3: Physical device model (05-049r2) [Suhler]

Defer

5.2 SSC-3: Vendor Feedback (05-351r2) [Group]

Defer

5.3 SSC-3: Add WORM VERSION field to Sequential Access Device Capabilities VPD page (05-391r0) [Banther]

Defer

5.4 SSC-3: Configurable EW (05-423r0) [Butt]

Defer

5.5 SSC-3: Secure Data Erase (06-120r2) [Butt]

Discussions revolved around the definitions of Vendor-specific Control Meta-data and Security Meta-Data. Also clarified and word-smithed the definitions of the METHOD field. A note was added to give an example to help understand the intent of the 10b value of the METHOD field. Discussions how to handle the LONG bit set to zero were also had.

Kevin Butt moved for inclusion into SSC-3. Ralph Weber seconded. Passed on 5:0:6 vote.

Action Item: Kevin Butt to revise and post SSC-3: Secure Data Erase (06-120r2).

Action Item: Dave Peterson to incorporate 06-120r3 into SSC-3.

6. New Business

6.1 SSC-3: Add Encrypted Write Command Proposal (06-207r0) [Avida]

Kevin Butt from IBM stated that IBM including TSM is opposed to a new command.

Also David Black stated that this would have to be a pass-thru command and pass-thru is slow and should not be used for primary data path. Roger Cummings from Veritas agreed.

Michael Banther suggested to bring back contingent allegiance and was argued against by David Black, Ralph Weber and Kevin Butt.

The problem trying to be solved is that data might get on media that is clear text instead of encrypted. Want to know for sure that nothing happens underneath the application.

A straw-poll was held for the question, “Are you in favor of the direction taken as specified in 06-207r0?” Result: 4:3:5

Suggestions were made to put it into the Explicit command set and take it out of the implicit command set.

6.2 SSC-3: Encrypt keys for transfer to device (06-103r2) [Black]

David Black: This is a discussion type document more than a proposal. I want to stear my proposal into an area that will be worth my time. The Goal is to defend against an eavesdropper and replay but not an active attacker.

Ralph Weber is attempting to get David to put the Diffie-Hellman portions into SPC.

Re-keying would end up going back up to SPC.

Roger Cummings: Rat hole embedded IKEv2 into google there are at least 7 libraries that claim support for this. It may be easier to use that.

David Black: the problem is that IKEv2 requires authentication.

There was a lengthy discussion on required entropy.

There was discussion about anouncement and what was the correct direction. Avida wants the anouncement to come from the host not the target.

David Black will go look at cutting down and adding some negotiation to this.

Discussion about how does the downgrade attack work?

Roger believes that the application will determine what to use when qulify support.

Straw Poll which one should we do:

1) 08: Target announces the rules.

2) 02: Host announces the rules.

3) 01: We need negotiation mechanism that is downgrade resistent.

4) 04: Abstain

David: There is anticipation that the secret generation can be rather expensive and may be done failry often. Diffie-Hellman reuse is a standard specified thing that is done. NIST doesn't like this. However, this reusing a well established network security protocol that has had all the security bugs hammered out.

Matt Black: We need to add in a re-keying functionality. But David and Ralph argue that is not secure and a new Diffie-Hellman exchange is required.

Avida wants eliptical curve added. If you want to deal with Government then you need this.

100 bits is way too small - 2^50 entropy.?

Someone says they do not want SHA-1 or AES_XCBC.

IPsec ESP (Encryption Security Protocol)

In terms of getting the wrapped key getting to the device. Given that Matt is taking AES Key forward should I take ESP forward? 1:1:10.

24 encryption operations for a 256bit key for AES.

David Black: I would guess that the firmware impact between AES and ESP is similar if you have a GCM hardware. If both are total software then AES is significantly smaller.

Landon: There needs to be a threat model and what threats are being addressed.

Michael Banther: Please have a discussion of the threat models before we dive into the details when you take this into CAP.

6.3 SSC-3: Using NIST AES key-Wrap for Key Establishment (06-225r0) [Ball]

This proposal assumes that a security association is already established.

Ralph Weber: I do not like SPI (security parameters index). Why not change P to A - association.

Michael Banther: I have an issue with the definition of secure channel. There is no channel defined in SCSI.

Is this security association between the application client task or the application client? It sounds like there is a fourth entity within the Logical Unit that has yet to be defined.

Discussions were about Security Associations to the Logical Unit from different ports. Are these the same or not? The LUN identifier should be the same no matter what port it is through. Do we have to create a separate SA down each port?

The only thing you need to have is the same shared secret between the application client and the device server. It does not matter across which port it passes.

Micheal Banther: We can remove “Secure Channel” and replace with a security association in most places.

Action Item: Matt Ball revise and post SSC-3: Using NIST AES key-Wrap for Key Establishment (06-225r0)

6.4 SSC-3: TapeAlert Delineation (06-138r0) [Butt]

Defer

6.5 SSC-3: Vendor-specific Service Actions for MAINTENANCE IN/OUT (06-223r0) [Banther]

6.6 SSC-3: Align clean notification names (06-235r0) [Banther]

6.7 Discussion of SSC-3 status [group]

When do we want to close out SSC-3? Paul Entzel: We should give a new schedule to John Lohmeyer. Nov 2007 to public review, May 2007 Letter Ballot. Last technical input Jan 2007.

6.8 Discussion of key integrity validation [Butt]

6.9 SSC-3 VPD page length fields [Peterson]

Page length field in manufacturer assigned serial number will use bytes 2 and 3 for length field.

7. Next Meeting Requirements (San Jose, CA)

Conference call Wed. May 31at 8:00 am - 10:00 Pacific.

Same time.Tuesday after FCP-4.

8. Review of new action items

8.1 Kevin Butt to revise and post SSC-3: Secure Data Erase (06-120r2).

8.2 Dave Peterson to incorporate 06-120r3 into SSC-3.

8.3 David Black to revise and post 06-141r0.

8.4 Action Item: Matt Ball revise and post SSC-3: Using NIST AES key-Wrap for Key Establishment (06-225r0)

9. Adjournment

Dave Petereson made a motion for adjournment at 6:40 pm central. Seconded by Kevin Butt.