SCSI Stream Commands - 3: Working Group Minutes (T10/07-036r1)
Date: Jan 16, 2007
Time: 11:00 am - 7:00 pm
Location: Orlanda, FL

Agenda

1. Opening remarks and introductions [Peterson]

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

3. Approval of meeting minutes (06-494r0; 07-006r0) [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 Configurable EW (05-423r3) [Butt]

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

5.2 Security-related items

5.2.1 Using NIST AES Key-Wrap for Key Establishment (06-225r4) [Ball]

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

5.2.3 Using Public-Key Cryptography for Key Wrapping (06-389r4) [Avida]

5.2.4 Encryption KAD lengths, Nonces, and Resets (06-412r2) [Suhler]

5.2.5 Keyless Copy of Encrypted Data (06-462r1) [Butt]

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

6. New Business

6.1 General items

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

6.2 Security-related items

6.2.1 Encryption Error Behavior when usupported medium is loaded (07-005r0) [Butt]

6.2.2 Additional controls for keyless copy (07-016r0) [Entzel]

7. Liason reports

7.1 P1619.1 Status report [Ball]

8. Next Meeting Requirements (Memphis, TN)

9. Review of new action items

10. Adjournment

Attendance

SSC-3 Working Group Attendance Report - January 2007

Name	S	Organization
Mr. Noud Snelder	V	BDT
Mr. Robert Snively	P	Brocade Comm. Systems, Inc.
Mr. Gideon Avida	P	Decru
Mr. Robert H. Nixon	A	Emulex
Mr. Ralph O. Weber	P	ENDL Texas
Mr. Curtis Ballard	V	Hewlett Packard
Mr. Michael Banther	A	Hewlett Packard Co.
Mr. Kevin Butt	A	IBM Corp.
Mr. Robert Payne	P	Iomega Corp.
Mr. David Peterson	P	McDATA
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. Scott Painter	A#	Sun Microsystems, Inc.
Mr. Roger Cummings	P	Symantec
Mr. George Dake	V	SYMANTEC
Mr. Anders Liverud	AV	Tandberg Storage

22 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 thanked Symantec for hosting.

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

Paul Suhler, Quantum moved and Landon Noll, Neoscale seconded. Passed unanimously.

3. Approval of meeting minutes (06-494r0; 07-006r0) [Peterson]

Kevin Butt, IBM moved for approval and Paul Suhler, Quantum 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.

Carry-Over.

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

Done.

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

Done.

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

Done.

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

Done. 06-412r2.

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

Carry-Over

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

Done 06-389r4

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

Done.

5. Old business

5.1 General items

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

Defer.

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

Defer.

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

Discussed and feedback received. Kevin to Revise and post.

5.2 Security-related items

5.2.1 Using NIST AES Key-Wrap for Key Establishment (06-225r4) [Ball]

This is a method to get a key into the tape drive using ESP to encapsulate the key.

Dave Peterson does not like the term “command” in the Send Encrypted Command page. Matt suggested change is “Send Tape Data Encryption security protocol page”. Dave prefers “Send encapsulated page”. Almost the same as ESP except the padding has been removed.

Gideon asked if Matt had reviewed his questions and Matt said no.

Gideon and Kevin asked if this belongs in SSC-3 or if it better belongs in SPC-4 in the Security Protocol Out command. The answer from Matt is that it increases the logistics. The answer from Ralph is that it would greatly complicate the proposal.

Gideon mentioned that there are a lot of references in the proposal, some of which are no longer needed.

Michael Banther pointed out that the definitions do not match the definitions in Ralphs proposal to SPC.

Paul Entzel pointed out that there needs to be a definition for ICV.

Ralph mentioned that using 32 bit value in SAI definition will elicit a letter ballot comment from him.

David Black thinks SSC needs to make the SA more specific in SSC than SPC. Gideon thinks this is dangerous.

Ralph: The SA, SAI, and security association parameter definitions need to match those in 06-369 that are slated for SPC-4, and should reference SPC-4.

Went through the Acronyms and removed those that are no longer needed.

Reworded text to be more clear.

There was a discussion on what the proper behavior should be if the device receives a DS_SQN greater than that expected. RFC4303 was referenced to help the discussion.

Gideon is concerned about how an attacher can sit in the middle, swallow the commands and reply with a status. The answer is that this attack is not part of the threat model that is attempting to be protected against. Gideon says he does have a proposal to solve this in his encrypted write command.

Larry Hofer requested that we put in some text that specifies that this is for anti-replay. Ralph said that this probably belongs in his SA proposal against SPC-4.

Gideon thinks there needs to be a model clause, Pual Entzel does not. Michael Banther also wants a usage model somewhere for this. The conclusion is that there needs to be a model clause of why this would be used.

Rename 4.2.19 from “Data encryption” to “Encryption of data on the volume”.

Bob Nixon wants a list of attacks specified, not necessarily a complete threat model.

Kevin Butt: SQN needs to start at one.

Ralph Weber: are the sequencing rules general enough that they should be specified in SPC? The answer is yes, but nobody has come forward to write the proposal yet. So Matt should leave the language in place until somebody writes the proposal for the general definition for SPC.

This proposal is missing the CREATE_CHILD_SA information.

Michael Banther is uneasy with interoperability issues relying on lengths defined in other (non-T10) standards. We cannot use a reference to an unpublished standard that is non-T10.

ANSWER: Matt does not believe it is good to add the length field to the overhead. It will be stored as part of the state that SSC-3 or SPC-4 needs in order to use an SA (i..e part of the SA) to protect keys being transfered to a tape drive. This is missing and needs resolved.

Gideon and Kevin both believe that this effectively blocks this proposal until resolved.

RFC4106 should be referenced for GCM.

It needs to be spec’ed where you put what algorithm is being used.

Michael: Why is the IV being sent here? David: this is the IV for the entire page and not the other IV. Michael: please clarify what the IV is being used for (i.e. which encryption function).

The term “Encryption Algorithm” is used in 7.7.4.11.1 and is the encryption algorithm referenced in this table.

Michael would like a model clause or statement that says we are taking this page, encrypting it and sending it in this page.

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

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

Overtaken by events.

REMOVE FROM AGENDA

5.2.3 Using Public-Key Cryptography for Key Wrapping (06-389r4) [Avida]

Dave Peterson thinks 4.2.x.2 and 4.2.x.3 do not belong in the model clause but should be in an informative annex. What is different about this threat model vs. the one in SPC-4?

Gideon: The difference is that you have a key manager that is outside your data/media manager.

Dave Petereson would like to put these in an informative annex and see how much can be removed in favor of the SPC-4 threat model.

David Black suggested that would be a good idea.

Dave Peterson made the offer that if Gideon gives him the source he will put it into the format that the SSC-3 Editor (Dave Peterson) desires for SSC-3.

Edits were made to make the proposal into standardese.

David Black: There is now identity information in here but non interoperable format and not know how to use it. The identity is unspecified to format. (e.g. 8.5.4.8) But I just want to note it but not hold it up for it.

POTENTIAL PATENT ISSUE: There has been some comments in the past about the elliptic curve algorithm being in the public domain, but there is question about this being covered by a patent by certicom. You should have your legal department check about the Patent applicability.

Gideon Avida made a motion to incorporate 06-389r4 as modified into SSC-3. Landon Noll seconded the motion. The motion passed on a 4:0:10 vote.

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

AI: [Dave Peterson] Incorporate into SSC-3 Using Public-Key Cryptography for Key Wrapping (06-389r4)

REMOVE FROM AGENDA

5.2.4 Encryption KAD lengths, Nonces, and Resets (06-412r2) [Suhler]

Paul needs to specify behavior if UKADF or AKADF is zero.

Michael Banther asked for section 5.2 changes to be removed. That is, remove that a Logical Unit reset clears the encryption parameters.

Paul Suhler moved that Encryption KAD lengths, Nonces, and Resets (06-412r2) as modified be incorporated into SSC-3. Michael Banther seconded the motion. The passed unanimously.

5.2.5 Keyless Copy of Encrypted Data (06-462r1) [Butt]

Modifications made.

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

REMOVE FROM AGENDA

6. New Business

6.1 General items

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

6.2 Security-related items

6.2.1 Encryption Error Behavior when usupported medium is loaded (07-005r0) [Butt]

6.2.2 Additional controls for keyless copy (07-016r0) [Entzel]

7. Liason reports

7.1 P1619.1 Status report [Ball]

Elections are in process.

P1619.3 PAR proposal was presented.

8. Project Status

8.1 Next Meeting Requirements (Memphis, TN)

Request same time

February 14, 8:00-10:00 AM Pacific

8.2 Target date for letter ballot.

Nov 2007

9. Review of new action items

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

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

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

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

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

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

10. Adjournment

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