Minutes May 2007 SSC-3 (07-238r1)
Date: May 08, 2007
Time: 11:00am-7pm
Location: Bellevue, WA

Agenda

1. Opening remarks and introductions

Dave Peterson thanked Microsoft for hosting.

Attendance

SSC-3 Working Group Attendance Report - May 2007

Name	S	Organization
Mr. David Peterson	P	Brocade
Mr. Gideon Avida	P	Decru
Mr. David Black	A	EMC Corp.
Mr. Robert H. Nixon	A	Emulex
Mr. Curtis Ballard	V	Hewlett Packard Co.
Mr. Kevin Butt	A	IBM Corp.
Mr. Robert Payne	P	Iomega Corp.
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. Roger Cummings	P	Symantec
Mr. Anders Liverud	AV	Tandberg Storage

14 People Present

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

2. Approval of agenda (07-230r0) [Peterson]

Dave Petereson moved that the agenda as revised be approved. Bob Nixon seconded the motion. Passed unanimously.

3. Approval of meeting minutes (07-133r0; 07-180r0) [Peterson]

Dave Peterson made a motion to approve the minutes. Kevin Butt seconded the motion. The motion 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 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. I need to call Dave.

Carry-Over

4.4 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

4.5 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

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

Complete

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

Complete

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

Complete

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

Complete

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

Complete

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

Complete

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

Carry-Over

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

Carry-Over

4.14 Dave Peterson to add Additional controls for keyless copy (07-016r2) into SSC-3

Carry-Over. This is pending approval of 06-462.

5. Old business

5.1 General items

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

Defer

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

Kevin presented his changes. Several changes were made. A request was made to query the ISV's about the desired behavior of the Read Position reporting of PEW.

AI: [Kevin Butt] Revise and post Configurable EW (05-423r3)

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

Defer

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

Defer

5.2 Security-related items

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

Matt covered changes. He pointed out that much of the content was moved to Ralph's proposal that is in CAP (07-169). Gideon Avida asked why he didn't wrap the entire page. Gideon was offered 06-225r5 so he can create an r6 if he wanted. He declined.

New discussion item about what happens when por.

Roger Cummings brought up that what Gideon was concerned about could be solved by setting an only if encrypted bit similar to the only if reserved bit. Daved Black pointed out that a man in the middle could flip that bit. This discussion ended with no resolution.

Edits were made. The answer to the question "Should we make P-512 Elliptic curve mandatory as well?" is no, there are alleged IP issues so we cannot.

There was discussion that the wrapping key strength in relation to the key strength. It was determined that there are different threat models and so we shoul dnot make a statement about it.

Matt Ball made a motion to include 06-225r7 (06-225r6 as modified) into SSC-3. David Black seconded the motion. The motion passed on an 8:1:0 vote

[Matt Ball] Revise and post Using NIST AES Key-Wrap for Key Establishment (06-225r5)

5.2.2 Keyless Copy of Encrypted Data (06-462r7) [Butt]

Kevin thanked the group for the feedback on the several revisions that he had posted between the meetings. He covered his changes and incorporated suggested modifications. Kevin asked if there was any reason he could not move the proposal as modified. Curtis Ballard indicated that he would invoke the two week rule. Then he requested a recess so he could check with others to see if he would or would not invoke the two week rule. Curtis recinded the 2 week rule.

Kevin Butt moved that Keyless Copy of Encrypted Data (06-462r7) as revised be included into SSC-3. Paul Suhler seconded the motion. The vote passed on a 5:0:3 vote.

[Kevin Butt] Revise and post Keyless Copy of Encrypted Data (06-462r7) as revised

[Dave Peterson] Incorporate Keyless Copy of Encrypted Data (06-462r8) into SSC-3

5.2.3 IKEv2 for CAP (06-449r4) [Black]

Remove from SSC-3 agenda. This is a CAP item.

5.2.4 Fix conflict between 06-412r3 and 07-016r2 (07-204r0) [Entzel]

Paul presented this and pointed out that Alternative 1 conflicted with another recently approved proposal. Alternative 2 is what should be done.

Paul Entzel moved that 07-204r0 as revised be accepted for inclusion into SSC-3. Curtis Ballard seconded the motion. Motion passed unanimously.

[Paul Entzel] Revise and post Fix conflict between 06-412r3 and 07-016r2 (07-204r0)

[Dave Peterson] Incorporate Fix conflict between 06-412r3 and 07-016r2 (07-204r1) into SSC-3

6. New Business

6.1 General items

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

Defer

6.2 Security-related items

No new security related items.

7. Liason reports

7.1 P1619.1 Status report (07-138r0) [Ball]

22 companies, 33 people were present for the IEEE P1619.3 meeting yesterday

8. Project Status

8.1 Next Meeting Requirements (Colorado Springs, CO)

Six to eight hours.

8.2 Last Technical Input - September 2007

8.3 Target date for letter ballot - November 2007

9. Review of new action items

9.1 [Kevin Butt] Revise and post Configurable EW (05-423r3)

9.2 [Matt Ball] Revise and post Using NIST AES Key-Wrap for Key Establishment (06-225r5)

9.3 [Dave Peterson] Incorporate Using NIST AES Key-Wrap for Key Establishment (06-225r6)

9.4 [Kevin Butt] Revise and post Keyless Copy of Encrypted Data (06-462r7) as revised

9.5 [Dave Peterson] Incorporate Keyless Copy of Encrypted Data (06-462r8) into SSC-3

9.6 [Paul Entzel] Revise and post Fix conflict between 06-412r3 and 07-016r2 (07-204r0)

9.7 [Dave Peterson] Incorporate Fix conflict between 06-412r3 and 07-016r2 (07-204r1) into SSC-3

10. Adjournment

Dave Peterson made a motion for adjournment at 4:04 pm PDT. Seconded by Erich Oetting.