SCSI Stream Commands - 3: Working Group Minutes – Draft (T10/06-106r0)
Date: February 17, 2006
Time: 10:00 pm - 12:00 pm MST
Location: Phone Conference

Agenda

1. Approval of Agenda

2. Review of old action items
2.1 Kevin write proposal to limit to one key
2.2 Kevin write text for External with verify
2.3 [David Black] ask ietf if they will be our registry for Encryption algorithm names

3. Business
3.1 SSC-3: Add commands to control data encryption (05-446r5) [Entzel]
3.2 SSC-3: Encrypt keys for transfer to device (06-103r1) [David L. Black]
3.3 The Requirement for More than One Decryption Key (06-051r4) [Edling]
3.4 Email about External w/Verify [Butt]

4. Next meeting requirements

5. Adjournment

Attendance

SSC-3 Working Group Attendance Report - January 2006

Name	S	Organization
-Mr. Gideon Avida	V	Decru
-Mr. Chris Williams	V	Hewlett Packard
-Mr. Kevin Butt	A	IBM Corp.
-Mr. David Peterson	AV	McDATA
-Mr. Paul Entzel	P	Quantum Corp.
-Dr. Paul Suhler	A	Quantum Corp.
-Dwane Edling		Sun
-Matt Ball		Quantum
-Greg Wheeless		Symantec
-David Black		EMC
-David Cuddihy		ATTO
-Gerry Houlder		Seagate

12 People Present

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

Results of Meeting

6. Business

6.1 SSC-3: Add commands to control data encryption (05-446r5) [Entzel]

1) Editors note on page 6 questioning requirement of “shall support at least one of”...

David Black is concerned that without a requirement there will be no interoperablility.

We agreed to change to “shall support on of the methods described by this standard”.

2) Editors note - support for any specific scope mandatory?

All I_T Nexus was agreed to be put as being mandatory.

3) Second Editors note pg 7. What scope should be dropped back to when encryption parameters released.

David Black is concerned about changing the scope on a failure behavior. The answer is that there is the Lock behavior and the UA’s.

4) Editors note bottom page 8. There are changes here that chagnes things and should be reviewed by all.

5) Section 4.2.19.6 has been added.

6) Discussion about RESERVATION GROUP and what it signifies. item b)1) of clause 4.2.19.8 was discussed in detail.

7) Paul has received model clause text from Chris Williams and will add in next version.

8) David Black talked to ietf and they are not willing to register items not useful for their protocol.

Discussions about how SSC-3 is not dynamic enough. But David Black says we need a registry otherwise we will not be interoperable. We need to talk to John Lohmeyer about a T10 registery. David Black agrees but would like to reuse the numbers used by ietf and use the private use numbers from ietf for the T10 assignments.

9) 8.5.2.6 is whole new page.

10) Editors note page 18. Nobody interested.

11) page 25&26 notes waiting for reply from Kevin.

12) Editors note pg 27. “Editor’s note: Chris Williams (HP) asks: “Are we specifying the format of the plaintext key“

Need format specified like MSB/LSB but the formats are different.

13) Editors note pg 27 - David Blacks proposal 06-103r1. We will talk about it in his proposal.

15) Editors note pg 28: T10 vendor identification with the key reference.

This has problems and needs to be fixed. This should be the Key Server identifier not necessarily the device server id. Discussion revolved around if the requiremnet should be included or not. Suggested to remove the requirement to check this T10 Vendor ID 8 bytes but leave in the definition.

16) Note pg 28. “EDITOR’S NOTE: I have received several comments that the AUTHENTICATED field value should be specified as 1 instead of zero. I felt that the field’s value adds no value at this point, but by specifying it as zero we have the flexibility to add meaning to other codes in the future. Is this reasonable?“

6.2 SSC-3: Encrypt keys for transfer to device (06-103r1) [David L. Black]

Greg Wheeless Symantec - (Greg sent me an email to ensure that his comments were reflected accurately in the minutes. I reviewed this text and believe it to accurately cover what he stated)

Point one: we want to distinguish between two distinct threats. Threat “A” is a backup tape that is lost in shipment, potentially ending up in the hands of an attacker. Threat “B” includes an attacker in the datacenter listening to backup traffic. Both threats are important, but threat A is more urgent. We don’t want to delay the standard to address threat B if that means that tape drives will ship with non-standard implementations to address threat A. We see the latter as the worse problem of the two. We have no objection to addressing threat B if that doesn’t cause a tape vendor to ship a non-standard product.

Point two: just a reminder of a basic security principle. Securing a communications channel is of dubious value if one doesn’t authenticate the endpoints. Establishing a secure channel directly to an attacker is, of course, not solving the problem. A solution for encrypted key exchange should provide for endpoint authentication. We see value in endpoint authentication even if we weren’t encrypting any data.

Point three: threat B can be addressed with existing technologies. If iSCSI or FC is chosen as the transport, IPsec or FC-SP may be used, providing not just encrypted key exchange but endpoint validation and in-flight encryption of the backup data. If we don’t address threat B in the first version of this standard we don’t prevent a solution that does address threat B using additional existing technologies.

Point four: customers certainly care about security, but they care greatly about regulatory compliance. We all expect that the federal government will in the future establish rules for encrypting backups, but at this point we can’t be sure what those rules will be. If our goal in addressing threat B is to insure we have a standard compatible with regulatory compliance, we can’t be certain that we’ll meet that requirement in the first version of our standard. It seems likely that we will need to update the T10 standard once regulatory standards for backup are known.

David Black: I can live with incorporating this into SSC-3 after 05-446 but it needs to be clearly stated the limitations of passing plain text keys.

David Black: encrypted keys need to be added before SSC-3 goes to Letter Ballot.

Discussion about how to get the secret into the drive for encrypting key exchange.

Suggestion to mention that Data and Key in flight is not protected but only the data at rest.

Suggested to add an editors note stating that encrypted keys is intended to be added. Dave Petereson agreed to add an Editors note stating that this is a work in progress.

6.3 The Requirement for More than One Decryption Key (06-051r4) [Edling]

6.4 Email about External w/Verify [Butt]

7. Next meeting requirements

March T10 Meeting Cycle in Hilton Head.

8. Review of new action items

9. Adjournment

Call ended at 12:03 MST.