SCSI Stream Commands - 3: Working Group Minutes – Draft (T10/06-093r0)
Date: February 8, 2006
Time: 1:00 pm - 3:00 pm MST
Location: Phone Conference

Agenda

1. Approval of Agenda

2. Review of old action items
2.1 Dwayne to make changes to 06-050r1 and send to Paul Entzel for inclusion into 05-446
2.2 Dwayne to make changes to 06-051r2 and post
2.3 Paul Entzel to rev and post 05-446r3
2.4 Kevin write proposal to limit to one key
2.5 Kevin write text for External with verify

3. Old Bussiness
3.1 SSC-3: Add commands to control data encryption (05-446r4 with comments) [Entzel]
3.2 The Requirement for More than One Decryption Key (06-051r2) [Edling]

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 Cresti                            Emulex


11 People Present
```

Status Key:

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

Results of Meeting

6. Old Bussiness

6.1 The Requirement for More than One Decryption Key (06-051r3) [Edling]

Description of Maximum Number of Decryption Keys needs word smithed and field length expanded to 4 bytes.

Chris WIlliams of HP objected to putting this into 05-446r4 if it will modify the base. Concern is about delaying 05-446r4. Will decide later.

6.2 SSC-3: Add commands to control data encryption (05-446r4 with comments) [Entzel]

Greg Wheeless asked why Hard Reset is not listed as event to lose keys. OK since key is lost with reservation lost with CKORL bit.

CKORL bit currently only applies to key with scope = Reservation Group. Do we want to make it apply to any reservation? Should add LOCAL scope. Valid for any scope was decided on.

David Black of EMC is concerned about not requiring the ability to distinguish between encrypted and unencrypted.

Chris Williams of HP argued vehemently against this.

Kevin Butt of IBM stated that this is levying requirements on the format layer and hence should not be a shall.

Paul Suhler Quantum: We are very much against making this a shall.

Paul Entzel Quantum wants to make the Exhaustive-Search section to describe only what you report if you detect an exhaustive search attack and lock out. Most agreed. Probably only the first and last paragraph from section.

David Black wants a strong should here in case somebody finds a set of weak keys that are unknown today. (i.e. discover a mathematical weakness in encryption algorithm). Retry limits or delays on numbers of retries. Greg Wheeless agreed.

4.2.19.5 comments about there being a requirement of supporting either method a or method b. Many people do not want this requirement and are very much opposed to it.

David Black kept on trying to get to adding a wrapped key.

Chris Williams wanted text on how to handle out of resources but others do not want the design specified. David Black explained how ipsec allows vpn gateways to drop keys becasue of resource limitations. We need to get back to this.

On page 6 comment from DAvid Black about why initiator port name is needed then need to add port name also.

Key Instance Counter s/b instead of Key Generation suggested by David Black.

Need a model clause for Authenticated Key-Assoc data. Chris Williams volunteered.

David Black EMC is concerned about how to make insecure options illegal by what the settings of the IV_* and NONCE reporting.

David Black is wanting information added to state that if string cipher is used that it shall not use the same key with the same string cipher. There was a lively discussion about rules for good encryption not belonging in this standard. Comments being that we are not security experts and that the algorithm being used is being reported to the application client and that should specify what is being done and if it is secure or not. No resolution was reached.

David Black said that we need a registry of some kind for algorithm names. Suggested using ietf registry.

Kevin Butt wants to discuss if a registry is even needed prior to attacking this issue.

Greg Wheeless Symantec believes that a registry is required.

David Black EMC says legato wants a registry.

David Black is willing to ask ietf if they will be our registry.

7. Next meeting requirements

Move conference call from 20th to 17th at 9am Pacific.

8. Review of new action items

8.1 [David Black] ask ietf if they will be our registry for Encryption algorithm names

9. Adjournment

Call ended at 3:03 MST.