ENDL
TEXAS

Date: 18 November 2003
To: T10 Technical Committee & SNIA OSD TWG
From: Ralph O. Weber
Subject: OSD r09 Work List

Problem, Issue, or Work To Do	Resolution
Allow setting object logical length attribute to truncate the object.	In table 64, change "May Set" column to "Yes" for object logical length. Add the following to the definition of the object logical length attribute: "Setting the object logical length to a value that is smaller than the user object's logical length known to the OSD device shall cause the user object to be truncated to the specified length."
Identify zero Object Creation Time credentials to simplify validation.	In table 14, add one flag bit IGCRETM, 7 reserved bits, and 3 reserved bytes (4 bytes total, for alignment). IGCRETM == 1 means that the object creation time field in the credential is to be ignored (set to zero) when a capability is validated. Modify 4.6.4.4.4 to make use of the IGCRETM bit.
Move Object Creation Time from the Credential to the Capability.	**SNIA OSD TWG action required** Explain the purpose of this change and the effects on the Credential/Capability validation algorithm. It is not possible to edit the change into OSD r09 without understanding it.
Single Unique Object ID	Deferred to OSD-2
Attribute Access	Access allowed ONLY to attributes associated directly with the object being accessed (e.g., no accessing partition attributes as part of user object READ).
Persistence Model	Incorporate persistence_final.txt [04-005r0] in various clauses with edits appropriate to T10 standards wording.
Version Number	Incorporate the version number tag field in the Credential as described in Object Store Security Document rev 8. A marked copy of that document showing the concepts to be added is 03-279r2. Also define a version number tag attribute in the User Object Information attributes page.
Format issue (aka OSD as delivered from the factory)	Incorporate Rev08-Formatv02.doc [04-006r0] in various clauses with edits appropriate to T10 standards wording.

Problem, Issue, or Work To Do	Resolution
Current Command Attributes page	Define one Current Command attributes page, page number FFFF FFFEh, with the following attributes: • partition ID • object ID • object type • response integrity check value Define attribute page range F000 0000h to FFFF FFFEh for attribute pages that are associated with all objects (i.e., accessible in conjunction with any access to any object). Require the response integrity check value to contain 0 for security levels 0 and 1.
Combine LIST and LIST COLLECTION commands	Per 10/15/03 conference call, leave OSD r08 unchanged.
One CREATE XXX command per Credential	Modify as appropriate to require that each Credential used to allow a CREATE, CREATE AND WRITE, CREATE COLLECTION, or CREATE PARTITION command be invalidated subsequent to the completion of that command.
Task Management Functions	Prohibit support for task management functions when the security level is not zero. Add a PERFORM TASK MANAGEMENT command with a coded value for task management function. Add a permissions bit for the new command. Require all task management requests except ABORT TASK and QUERY TASK to be addressed to the root object.
Persistent Reservations	Modify the model to prohibit OSD devices from supporting Persistent Reservations when the security level is not zero. Indicate this in table 29 too.
Finish the removal of support for EXTENDED COPY	Remove the following commands from table 29 CHANGE ALIASES, RECEIVE COPY RESULTS, and REPORT ALIASES
Commands needing security protection	Modify table 29 to indicate that the following commands are prohibited with the security level is not zero: LOG SELECT, LOG SENSE, MODE SELECT(10), MODE SENSE(10), PREVENT ALLOW MEDIUM REMOVAL, READ BUFFER, RECEIVE DIAGNOSTIC RESULTS, START STOP UNIT, and WRITE BUFFER. Add a PERFORM SCSI COMMAND command that provides for delivery of the CDBs and parameter data for the above commands in concert with a Capability. Add a permissions bit for the new command. Require all of the new command to be addressed to the root object. Prohibit the use of the new command for delivery of any CDBs other than those listed.

Problem, Issue, or Work To Do	Resolution
REQUEST SENSE and TEST UNIT READY -- Owing to existing operating system implementations, these two commands cannot be prohibited when the security level is not zero. However, they have the ability to return/clear pending Unit Attention information that might be valuable to host software. Thus they might be viewed as security threats.	**SNIA OSD TWG action required** The degree of security threat must be evaluated. If the security threat is evaluated to be serious enough to require some remedy, then the nature of that remedy needs to be negotiated with T10 Unit Attention experts.
INQUIRY and REPORT LUNS -- Operating system device configuration software requires that these two commands be supported regardless of OSD security level. These commands do not clear pending Unit Attention conditions and so do not represent a known security threat.	No changes required. No SNIA OSD TWG action required, unless there are concerns about allowing these two commands regardless of OSD security level.
Does FORMAT OSD return a progress indication in sense data in the same why that the FORMAT commands for other device types do? Note: the answer affects one’s view of REQUEST SENESE which is the way such information is usually retrieved.	**SNIA OSD TWG action required** The need for or lack of need for a FORMAT OSD progress indication needs to be evaluated, and appropriate requirements defined.
Do Permissions Bits identify commands or functions? Different people reading OSD r08 get opposite views from the same text. So, some clarification is needed. The nature of the clarification depends on which view is adopted as the standard.	**SNIA OSD TWG action required** No consensus position has been observed regarding the commands or functions choice. If the functions position is taken, then changes along the lines shown in a reflector posting in the afternoon of 11/14 from Ralph Weber "re: Getting attributes" will need to be made. If the commands position is taken, then the Credential format will need to be modified to include explicit Get & Set Attributes controls.
Should the REPORT TARGET PORT GROUPS and SET TARGET PORT GROUPS commands be supported? This would allow Active/Standby OSD controller (aka asymmetric logical unit) implementations ala RAID controllers.	**SNIA OSD TWG action required** No consensus position has been observed regarding asymmetric logical unit support.
Man-in-the-middle DOS attacks	As just a command level standard, OSD is not designed to address all known security threats. Some threats are appropriately addressed by the SCSI transport protocol (e.g., data encryption) and thus are not covered by OSD. The DOS attacks raised as issues fall in to this category.
Attribute size hint (i.e., add an attribute that specifies the bytes of overhead associated with each attribute so that host software can calculate OSD space usage)	Host software should be relying on the OSD attributes and quotas to manage space usage. Attempting to mirror the calculations in host software is redundant and extremely error prone.
C.2 (General bibliography) is out of date	Subclause C.2 will be removed in OSD r09.

Problem, Issue, or Work To Do	Resolution
An OSD-specific sense data descriptor is required and should include the following: • partition ID • user object ID • object byte offset where error detected	**SNIA OSD TWG action required** Review/enhance this list.
Invalid CapKey effects on CHECK CONDITION responses.	**SNIA OSD TWG action required** The following 4.6.4.2.4 text needs to be revaluated and rewritten by OSD security experts to account for the fact that an application client that sends an invalid CapKey is guaranteed to observe an invalid response integrity check value: "If the validation fails, the application client should cease communications with the device server."
OSD System ID should have a format that matches that defined for the Device Identification VPD page, to provide compatibility with all SCSI transport protocols, especially iSCSI.	**SNIA OSD TWG action required** The issues raised by Rob Elliott in a 11/10/03 reflector posting need to be resolved, or they will become a Letter Ballot comment and T10 will resolve them at its pleasure.
Apply numerous editorial changes received since r08 published and editorial changes from the 11/7 T10 Editing Meeting	No SNIA OSD TWG action required.