ENDL
TEXAS

Date: 5 March 2008
To: T10 Technical Committee
From: Ralph O. Weber
Subject: SPC-4 CbCS capability validation omissions

Introduction

Several CbCS capability validation tests appear to have been omitted from the applicable subclause. Since the changes are normative, this proposal seeks to remedy the problem.

Revision History

r0 Initial revision

Unless otherwise indicated additions are shown in blue, deletions in ~~red strikethrough~~, and comments in green.

Proposed Changes in SPC-4 r13

5.13.6.8.? CbCS Capability validation {{subclause numbers may be wrong}}

The enforcement manager (see 5.13.6.8.7) shall validate the CbCS capability descriptor (see 6.19.2.3) included in the CbCS extension descriptor (see 3.1.16). If the validation fails, the enforcement manager shall interact with the secure CDB processor (see 5.13.6.8.6) in a way that causes the command containing the CbCS extension descriptor to be terminated with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB.

The enforcement manager's validation of a CbCS capability descriptor shall fail if any of the following conditions occur:

a) The DESIGNATION TYPE field contains a value that table 182 defines as reserved (see 6.19.2.3);
b) The CBCS METHOD field contains a value that table 183 defines as reserved (see 6.19.2.3) or a vendor specific value that the enforcement manager does not support;
c) The INTEGRITY CHECK VALUE ALGORITHM field contains a value that is:
   A) Not one of those that table 61 (see 5.13.7) lists as being an integrity checking (i.e., AUTH) algorithm;
   B) Is AUTH_COMBINED; or
   C) Is a vendor specific value that the enforcement manager does not support;
d) The CAPABILITY EXPIRATION TIME field contains a non-zero value and the value in the CAPABILITY EXPIRATION TIME field is lower than the current time value (i.e., the current number of milliseconds passed since midnight, 1 January 1970 UT);
e) The enforcement manager is contained within the secure CDB processor, the DESIGNATION TYPE field value is set to 1h (i.e., logical unit designation descriptor), and the contents of the DESIGNATION DESCRIPTOR field in which a logical unit name (see SAM-4) is indicated does not match the addressed logical unit;
f) The enforcement manager is contained within the SCSI target device (i.e., addressed as a well-known logical unit), the DESIGNATION TYPE field value is set to 1h (i.e., logical unit designation descriptor), and the contents of the DESIGNATION DESCRIPTOR field in which a SCSI target device is indicated does not match the SCSI target device that contains the addressed well known logical unit;
g) The DESIGNATION TYPE field value is set to 2h (MAM attribute descriptor) and either of the following are true:
   A) The ATTRIBUTE IDENTIFIER field in the DESIGNATION DESCRIPTOR field contains any value other than 0401h (i.e., MEDIUM SERIAL NUMBER); or

18484 Preston Road, Suite 102 PMB 178, Dallas, TX 75252 214-912-1373 972-596-2775 Fx ENDL_TX@computer.org

B) The DESIGNATION DESCRIPTOR field contents do not match the MAM attribute of the volume residing in the addressed logical unit;

h) The POLICY ACCESS TAG field contains a non-zero value that does not match the Policy Access Tag attribute (see 5.13.6.8.9) of the addressed logical unit; or

i) The command in the CDB field of the extended CDB (see 4.3.4) that contains the CbCS extension descriptor is not permitted by the PERMISSIONS BIT MASK field (see 5.13.6.8.?).