Date: 27 June 2007
To: T10 Technical Committee
From: Ralph O. Weber (ENDL Texas) and George Penokie (IBM)
Subject: SPC-4: Command Security Model

Introduction

The May 24 CAP Security conference call identified several aspects of Command Security that should be viewed as common to the Capability-based Command Security (see 07-069) and SA-based Command Security (see 07-149) concepts. This proposal develops those ideas into a general model and then applies the model to each of the two techniques.

The intent is to define a model in which both techniques can coexist. It is also hoped that a common model will aid in the understanding of the security issues for Command Security in general and each of the techniques in specific.

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

5.13 Security Features

5.13.1 Security goals and threat model

…

5.13.x Command security

{{All of 5.13.x is new. No changes markings are provided until further notice.}}

5.13.x.1 Overview

SCSI command security defines a techniques for protecting against inadvertent or malicious misuse of SCSI commands to gain unauthorized access to logical units.

The following classes are used to specify SCSI command security:

a) Secure CDB Originator class;
b) Security Manager class;
c) Enforcement Manager class; and
d) Secure CDB Processor class.

The relationship between those classes varies depending on the implemented security technique.

5.13.x.2 Secure CDB Originator class

The Secure CDB Originator class is a kind of application client that originates SCSI commands to which it has attached a security extension (x.x.x.x) that allows an enforcement manager to determine if the SCSI command may be processed by the addressed logical unit.

The secure CDB originator interacts with the security manager to determine:

a) the types of the SCSI commands it is allowed to send to the Secure CDB processor; and
b) the content of the security extension to be attached to the SCSI commands.

5.13.x.3 Secure CDB Processor class

The Secure CDB Processor class is a kind of device server that processes SCSI commands that have an attached security extension, if an enforcement manager allows that type of SCSI command from the originating application client to be processed.

The secure CDB processor determines if a SCSI command is allowed to be processed by communicating the following information to the enforcement manager:

a) the CDB of the SCSI command to be processed; and
b) the security extension, if any, attached to the SCSI command to be processed.

5.13.x.4 Enforcement Manager class

The Enforcement Manger class is either contained within a:

a) device server (i.e., has the same LUN as the secure CDB processor); or
b) target device (i.e., has a LUN and all the properties of a device server).

The enforcement manager determines if the secure CDB processor is allowed to, or prohibited from, processing a SCSI command using security information received from the security manager.

5.13.x.5 Security Manager class

The Security Manager class is either a kind of:

a) application client collocated with a secure CDB originator that communicates security information to the enforcement manager using the SCSI domain's service delivery subsystem (see SAM-4);
b) device server collocated with a secure CDB processor that communicates security information to the secure CDB originator using the SCSI domain's service delivery subsystem (see SAM-4); or
c) SCSI device contained within a SCSI domain that communicates security information to the enforcement manager and to the secure CDB originator using the SCSI domain's service delivery subsystem (see SAM-4).

In addition to a device server, if any, and an application client, if any, the security manager includes a decision database and a decision database update management mechanism whose definition is outside the scope of this proposal.

{{If no proposal to define the decision database and/or decision database update management mechanism is being processed at the time this proposal is approved, change 'proposal' to 'standard' in the above sentence.}}

The security manager:

a) maintains SCSI command security information for the SCSI domain (e.g., authorization and authentication information);
b) delivers to the enforcement manger the security information required by the enforcement manager to determine if the secure CDB processor is allowed to, or prohibited from, processing a SCSI command; and
c) Responds to requests from authenticated secure CDB originators to send SCSI commands to a secure CDB processor as follows:

A) If the secure CDB originator only sends it's authentication, then the security manager responds with all the security information that is required to be attached to any CDB that is sent to the secure CDB processor; or
B) If the secure CDB originator sends it's authentication plus the security information to be attached to CDBs, then the security manager shall only accept the request if the secure CDB originator is allowed to send SCSI commands to the requested secure CDB processor.

5.13.x.6 Command security techniques

This standard defines the following techniques for implementing command security:

a) Capability-based command security (see 5.13.x.7); and
b) SA-based command security (see 5.13.x.8).

5.13.x.7 Capability-based command security technique

5.13.x.7.1 Overview

{{TBD}}

5.13.x.8 SA-based command security technique

5.13.x.8.1 Overview

{{TBD}}

5.13.x.9 Link security requirements

{{There will be a gigantic July snowball fight in Houston before I will proposed the contents of this subclause without suggestions from CAP or a subgroup thereof.}}

5.13.x.10 Command security CDB extensions

{{This subclause is referenced by at least 5.13.x.1 and is TBD.}}