Date: 14 August 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
r1 Revise based on 28 June 2007 conference call.
r2 Added in a new section that describes the relationship between Security Associations and Command Security.

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

Proposed Changes in SPC-4

2.5 IETF References

{{Insert the following in numerical order by RFC number.}}

RFC 2753, *A Framework for Policy-based Admission Control*

3.1 Definitions

{{Insert the following in alphabetical order by term.}}

3.1.e Enforcement Manager class: The command security (see 5.13.x) class that the Secure CDB Processor class (see 3.1.s) consults to determine if the processing of a command is permitted or prohibited. Equivalent to the Policy Enforcement Point in the policy model defined by RFC 2753 and similar policy-based authorization standards. See 5.13.x.4.

3.1.r Secure CDB Originator class: The command security (see 5.13.x) class application client that originates secure CDBs and performs any additional functions necessary to do so. See 5.13.x.2.

3.1.s Secure CDB Processor class: The command security (see 5.13.x) class device server that processes secure CDBs and performs any additional functions necessary to do so. See 5.13.x.3.

3.1.t Security Manager class: The command security (see 5.13.x) class that maintains information about which secure CDBs may be originated by which Secure CDB Originator class (see 3.1.r) application clients to which Secure CDB Processor class (see 3.1.s) device servers, responds to requests to allow the origination of secure CDBs from Secure CDB Originator class application clients, and updates secure CDB permissions and prohibi-

tions in appropriate Enforcement Manager class (see 3.1.e) members. Equivalent to the Policy Decision Point in the policy model defined by RFC 2753 and similar policy-based authorization standards. See 5.13.x.5.

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 Manager class is either contained within a:

a) device server (i.e., has the same LUN as the secure CDB processor); or
b) target device (e.g., has a W_LUN, or vendor specific presence in the SCSI target device).

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 contains a decision database and a decision database update management mechanism whose definition is outside the scope of this proposal and communicates with the Secure CDB Originator class (see 5.13.x.2) and the Enforcement Manager class (see 5.13.x.4) as shown in table x1.

{{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.}}

Table x1 — Security Manager class relationships

Security Manager location	Communications mechanism for …	
	Secure CDB Originator	Enforcement Manger
An application client located in the same SCSI device as the secure CDB originator	Outside the scope of this standard	Via the SCSI domain's service delivery subsystem (see SAM-4)
A device server located in the same SCSI device as the secure CDB processor	Via the SCSI domain's service delivery subsystem (see SAM-4)	Outside the scope of this standard
A SCSI device contained within the same SCSI domain as the secure CDB originator and the secure CDB processor [a]	Via the SCSI domain's service delivery subsystem (see SAM-4)	Via the SCSI domain's service delivery subsystem (see SAM-4)
Not a SCSI device, device server, or application client	Outside the scope of this standard	Outside the scope of this standard

[a] This SCSI device is required to contain an application client and a device server (i.e., to contain both a SCSI Initiator Port class (see SAM-4) and a SCSI Target Port class (see SAM-4)).

The security manager:

a) maintains SCSI command security information for the SCSI domain (e.g., authorization and authentication information);
b) delivers to the enforcement manager 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 sends its authentication and an authorization request, then the security manager responds with the authorization information necessary for the secure CDB originator to

generate security information to be attached to any authorized CDB that is sent to the secure CDB processor; or

B) If the secure CDB originator sends its authentication, an authorization request, and the security information to be attached to CDBs, then the security manager shall only accept the request if the secure CDB originator is authorized to send the requested SCSI commands to the requested secure CDB processor.

5.13.x.6 The relationship between SAs and Command Security

As defined by this standard, SAs provide the following forms of secure communications for command parameter data:

a) Cryptographic parameter data integrity provided by Message Authentication Code or Integrity Check Value; and
b) Confidentially provided by encryption of parameter data.

The SAs defined by this standard do not apply to data communicated in the CDBs sent from the secure CDB originator to the secure CDB processor. The function of securing CDBs is performed by the command security features described in 5.13.x. Command security and SAs features may be used in concert to protect both the CDB data and the parameter data.

Authorization information (see 5.13.x.5) includes associations between:

a) Permissions to use certain commands and command options; and
b) Secure CDB originator identities.

The secure CDB originator identity needs to be authenticated before authorized access is granted. SAs provide one mechanism for authenticating a secure CDB originator's identity. If SAs are used in this manner, every secure CDB originator is required to be authenticated using a unique SA.

{{N.B. Since secure CDB originators are application clients, all the vagaries of the SAM-4 application client definition apply equally to secure CDB originators.}}

Some command security techniques (e.g., the CbCS technique described in 5.13.x.8) need an established secure channel between a secure CDB originator and secure CDB processor. SAs provide one mechanism for establishing such secure channels.

5.13.x.7 Command security techniques

This standard defines the following techniques for implementing command security:

a) Capability-based command security (see 5.13.x.8); and
b) SA-based command security (see 5.13.x.9).

5.13.x.8 Capability-based command security technique

5.13.x.8.1 Overview

{{TBD}}

5.13.x.9 SA-based command security technique

5.13.x.9.1 Overview

{{TBD}}

5.13.x.10 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.11 Command security CDB extensions

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