



Education

SCSI Security Nuts and Bolts

Ralph Weber, ENDL Texas

- The material contained in this tutorial is copyrighted by the SNIA.
 - Member companies and individuals may use this material in presentations and literature under the following conditions:
 - ◆ Any slide or slides used must be reproduced without modification
 - ◆ The SNIA must be acknowledged as source of any material used in the body of any document containing material from these presentations.
 - This presentation is a project of the SNIA Education Committee.
 - Neither the Author nor the Presenter is an attorney and nothing in this presentation is intended to be nor should be construed as legal advice or opinion. If you need legal advice or legal opinion please contact an attorney.
 - The information presented herein represents the Author's personal opinion and current understanding of the issues involved. The Author, the Presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.
- NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.**

➤ SCSI Security Nuts and Bolts

The SCSI Command Sets are the *lingua franca* of computer storage, the language by which computer systems and peripherals communicate to support the storage and retrieval of information - the lifeblood of any modern business. SCSI has evolved from origins in the early 1980s in *small* computers to support modern SANs that interconnect ten of thousands of peripherals and servers. The latest SCSI standards projects underway in INCITS Technical Committee T10 define the creation of Security Associations, methods of deriving keys & performing strong mutual authentication, per-command security controls supporting multiple levels of protection, support for security protocols defined separately by multiple other standards organizations, and the control and operation of new security features within storage peripherals themselves. This session will cover these new features in detail, and will highlight the new requirements that these features will place on the operation and management of future computer systems and their storage configurations.

- 50,000' View
 - ◆ History, Terms, Puzzle (some trees – some forest), etc.
- Management Concerns
- Nuts and Bolts
- Current Status

This History of **SCSI** (in one slide)

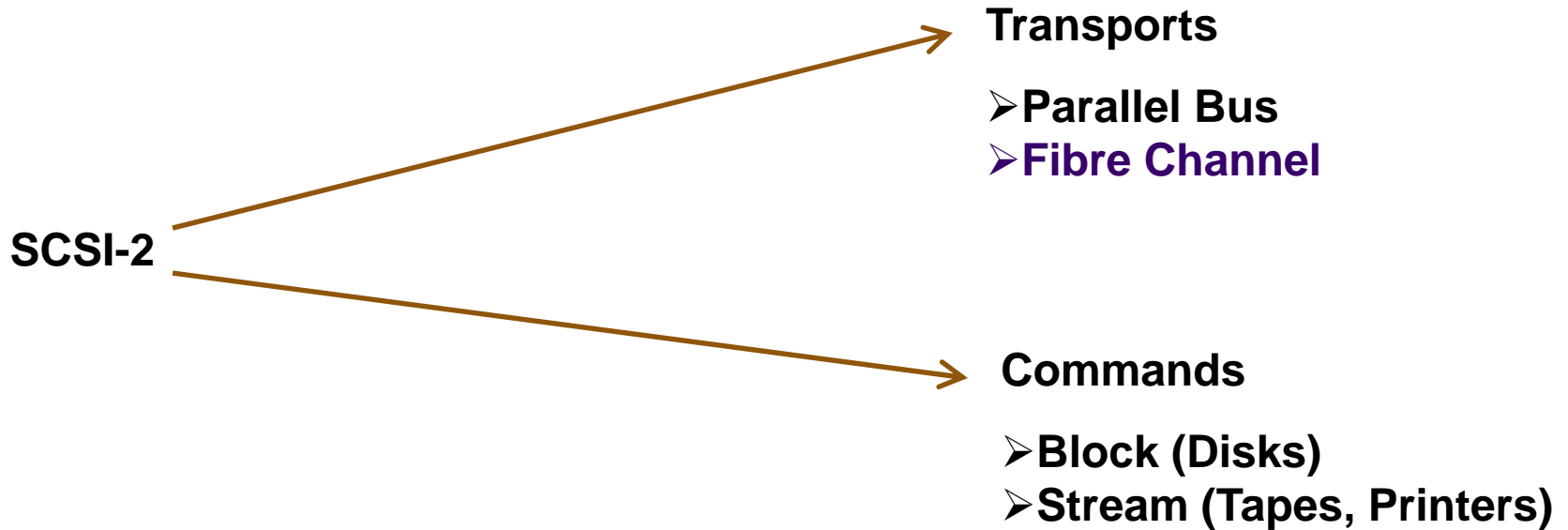
1980 — 1989

SCSI-2

- **Parallel Bus**
- **Disks**
- **Tapes**
- **...**

This History of **SCSI** (in one slide)

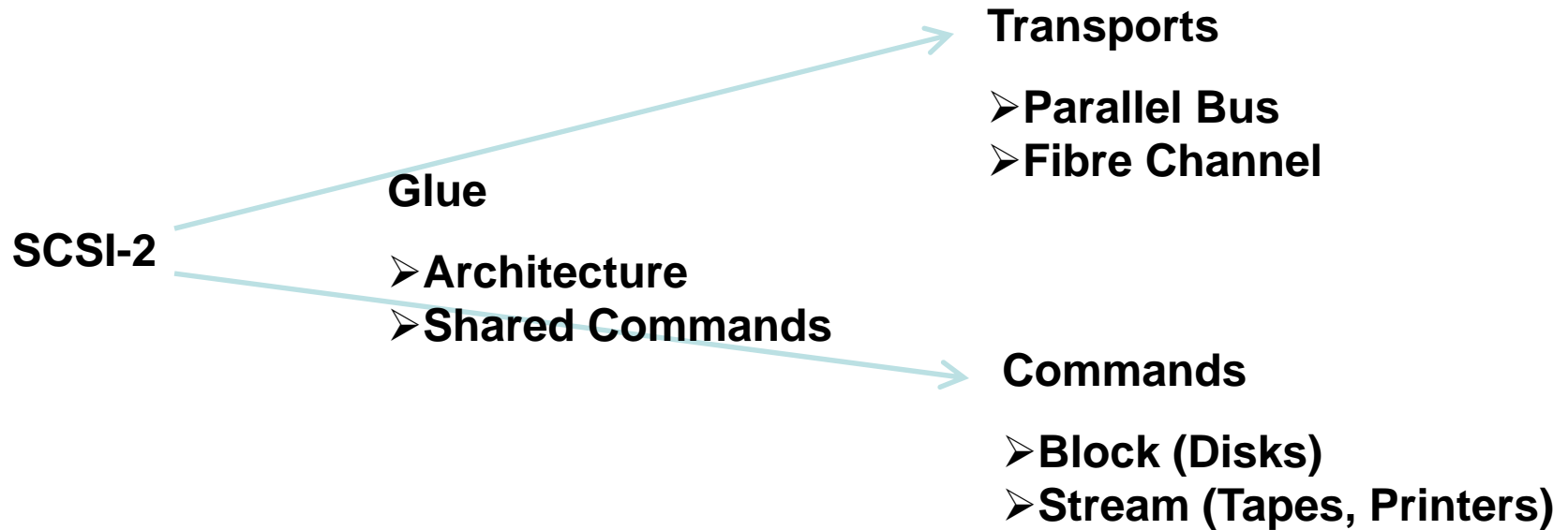
1980 — 1989 1990



This History of **SCSI** (in one slide)

1980 — 1989

1990



This History of SCSI (in one slide)

1980 — 1989

1990

Today

SCSI-2

- Architecture (SAM-x)
- Shared Commands (SPC-x)

➤ Transports

- SPI-x
- FCP-x
- SAS-x
- SBP-x (Firewire)
- ADT-x (robotics)
- iSCSI
- USB Bulk Transport

➤ Commands

- SBC-x/RBC (Disks)
- SSC-x (Tapes)
- SES-x (Enclosures)
- SMC-x (Media Changers)
- OSD-x (Object Storage)
- Optical Card Reader

Key:

- Developed by T10
(www.t10.org)
- Developed by T10
and other groups
- Developed exclusively
by other groups

Security Enforcement Points

➤ Transport Security

- ◆ Affects all commands and data
- ◆ Protection from
 - > Wire taps
 - > Hackers on the *network*
- ◆ **SCSI Transports**
 - > Fibre Channel
 - > iSCSI
 - > USB
 - > SAS

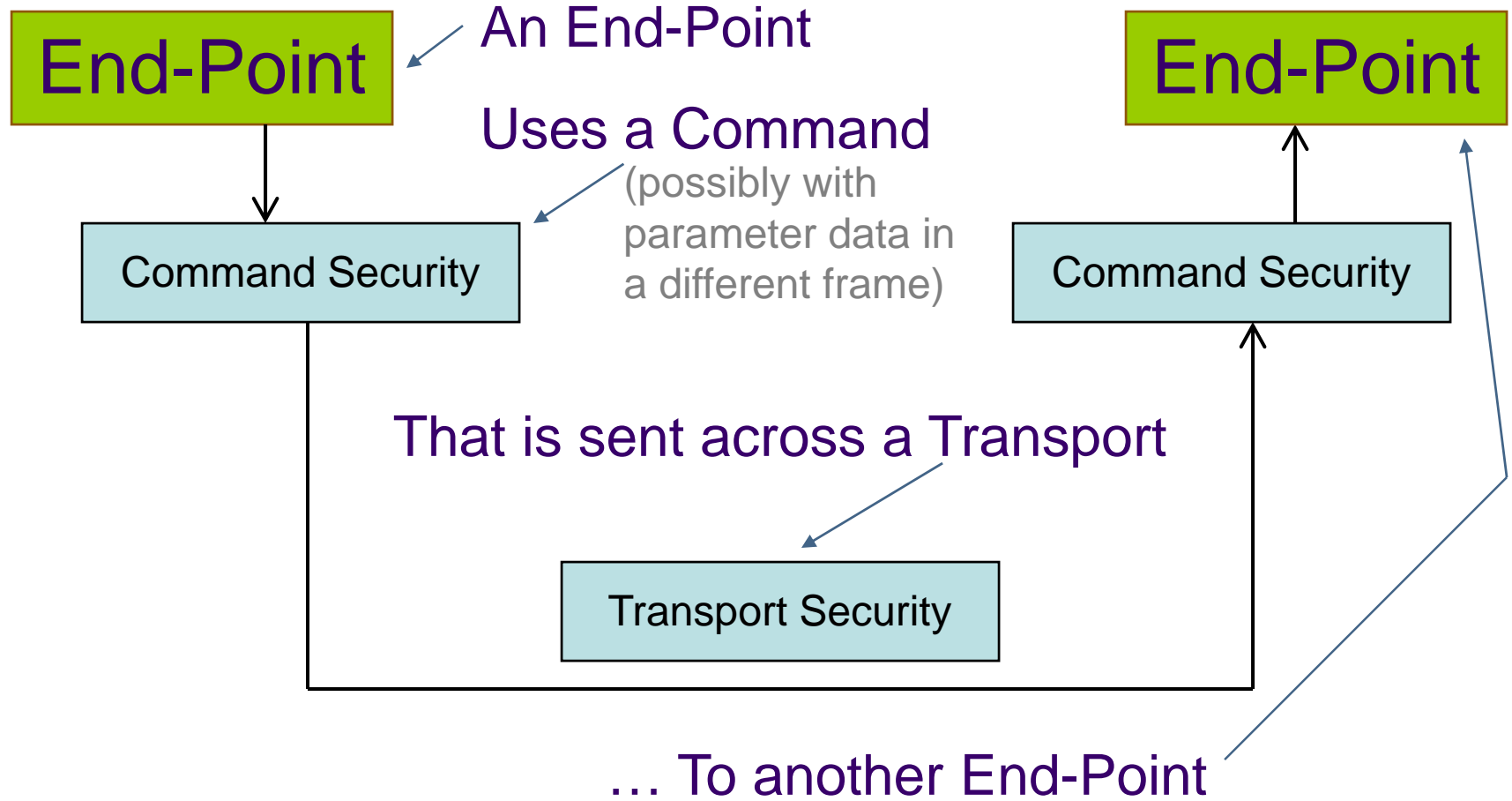


➤ Command Security

- ◆ Affects one command only
 - > Command data
 - > Not Command itself
 - > Not User data
- ◆ Protection from
 - > *Creative* software
 - > Hackers on the *network*

**Check out SNIA Tutorial:
Fibre Channel Technologies
Current and Future**

Ultimate Security *Enforcement Point* SNIA



End-Point Postscript

Note: Read-type parameter data has been ignored to keep things simple.

Warning: The definition of End-Point is fuzzy.

- HBA (Host Bus Adapter) builders see End-Point as the HBA.
- Applications see End-Point as their program.

Transport Level Security

- Authenticates Hardware (HBAs & Drive Ports)
- Hardware-based encryption
- Encrypts/Integrity Checks Whole Frames



**Check out SNIA Tutorial:
ABCs of Encryption**

- iSCSI
 - ◆ In-band Authentication (e.g. CHAP)
 - ◆ IKE — Authentication and Key Exchanges
 - ◆ IPsec — Encryption and Integrity Checking
 - ◆ MACSec — Ethernet Encryption and Integrity Checking
- Fibre Channel
 - ◆ FC-SP — Clones of IKE and IPsec all in one package

Command Level Security

- Authenticates Builder of the Command
 - ◆ Might authenticate the program image
- Software Based
- Encrypts/Integrity Checks Only Specific Data
 - ◆ Command Data
 - › Encrypt a Tape-Data-Encryption key
 - ◆ Variable Length CDB (Command Descriptor Block) bytes
 - ◆ **Not User Data** (as currently defined)
- See SPC-4 (SCSI Primary Commands) and other command standards

Security Toolbox

➤ Authentication

- ◆ Example: Driver's License Check

➤ Integrity Checking

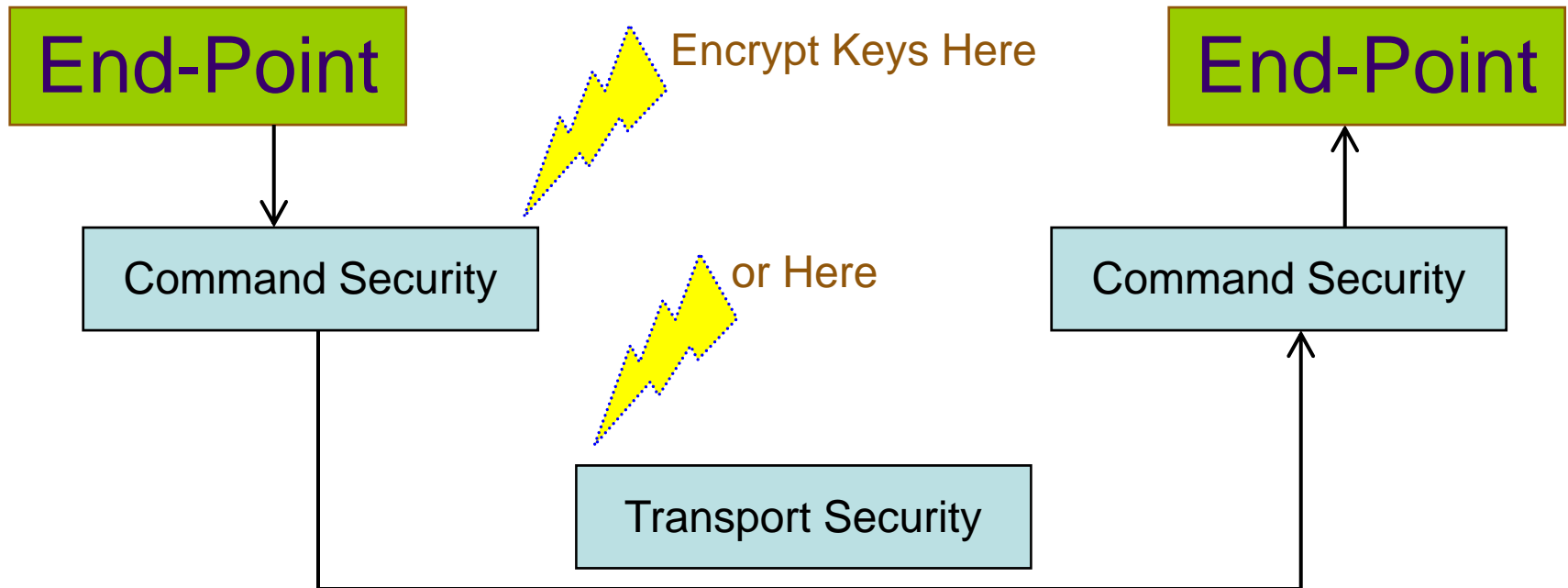
- ◆ Example: Is shipping box still intact?

➤ Encryption

- ◆ Example: Pig Latin

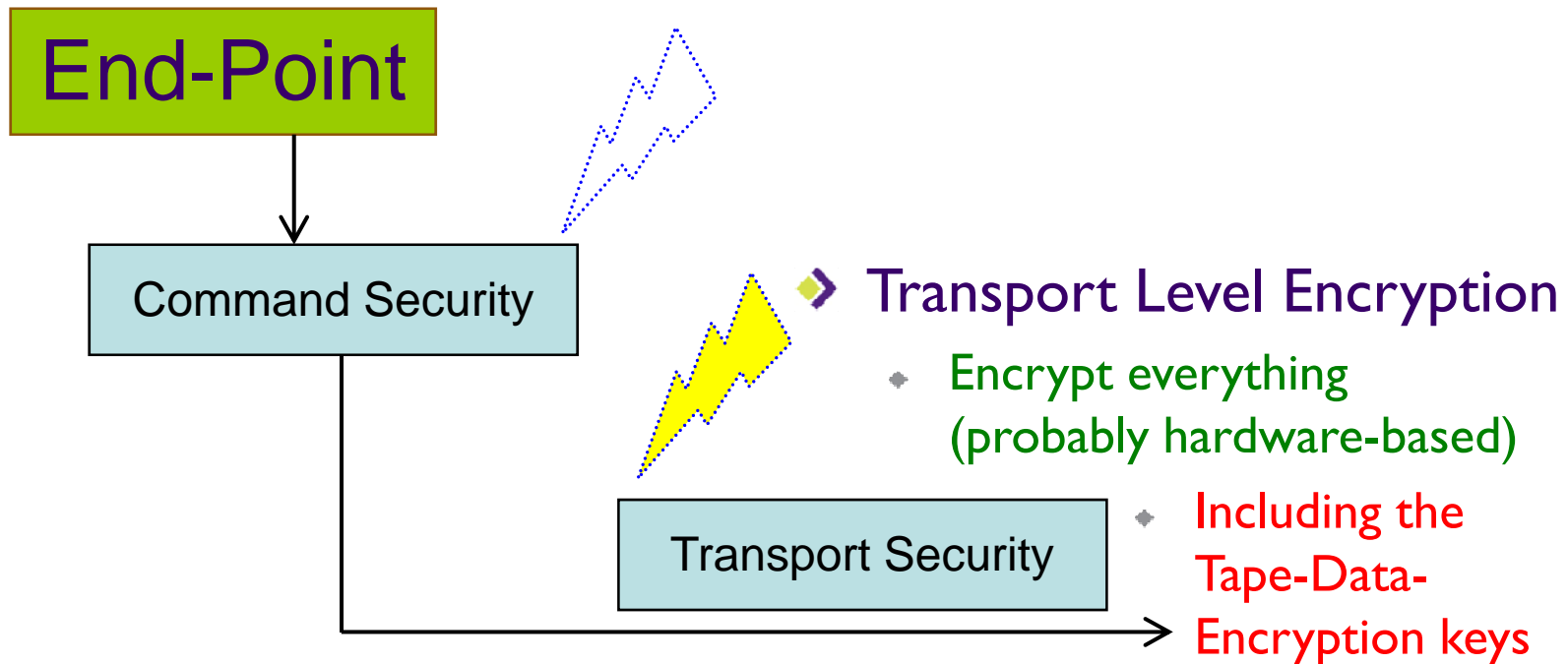
Security Jigsaw Puzzle

- Multiple ways to do the same thing
(using Tape-Data-Encryption keys as an example)



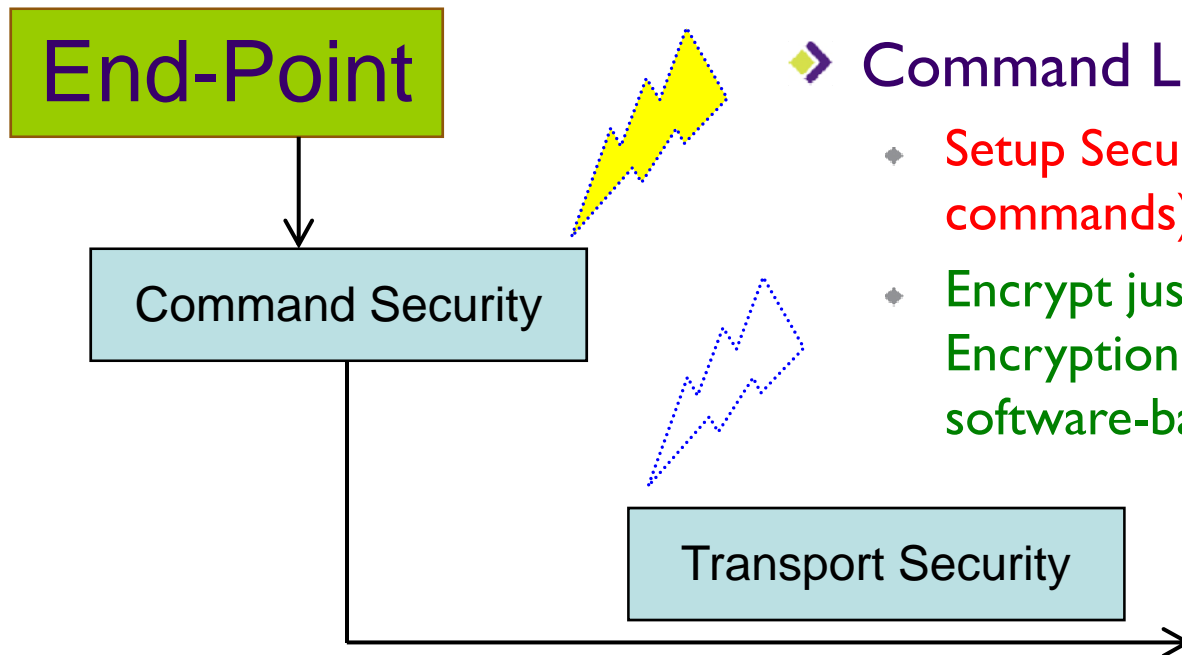
Security Jigsaw Puzzle

- Multiple ways to do the same thing
(using Tape-Data-Encryption keys as an example)



Security Jigsaw Puzzle

- Multiple ways to do the same thing
 (using Tape-Data-Encryption keys as an example)



- **Command Level Encryption**

- ◆ **Setup Security Association (extra commands)**
- ◆ **Encrypt just the Tape-Data-Encryption keys (probably software-based)**

Solving the Security Jigsaw Puzzle

- No Right (one size fits all) Answer
- Encrypting everything may be overkill
 - ◆ If (for example) the only family jewel on the link is the Tape-Data-Encryption key
- New Site-Specific Customization Opportunities
 - ◆ What to secure ... Where?
- Product Manufacturers Will Help
 - ◆ Promote standards
 - ◆ Suggest best product uses

- 50,000' View
- Management Concerns
 - ◆ Distributing Authentication Info
 - ◆ How to Authenticate
 - ◆ What to Authenticate
 - ◆ Where to Authenticate
- Nuts and Bolts
- Current Status

Distributing the Authentication Info

➤ **Security Job One is Always Authentication**

- ◆ Multiple Ways to Authenticate
- ◆ Multiple Things That Can Be Authenticated
- ◆ Multiple Places to Authenticate

➤ **Governmental Agencies May *Help* Make These Choices**



**Check out SNIA Tutorial:
Information Security
& IT Compliance**

Distributing the Authentication Info

- Multiple Ways to Authenticate Devices
 - ◆ Certificates (aka Public Key Infrastructure)
 - ◆ Shared Secrets (e.g., *passwords*)
- Multiple Things That Can Be Authenticated
 - ◆ Devices/Ports
 - ◆ Users
 - ◆ Programs
- Multiple Places to Check Authentication
 - ◆ In the End Devices
 - ◆ Central Security Server (e.g., RADIUS)

How to Authenticate

- Multiple Ways to Authenticate Devices
 - ◆ Certificates
 - ◆ Shared Secrets (aka *passwords*)

- Certificates Require a Public Key Infrastructure
 - ◆ Books have been written on this
 - ◆ Maybe you already have a PKI

- Shared Secrets Must Be Established
 - ◆ Centralized Password or Secret Management

What to Authenticate

- Multiple Things That Can Be Authenticated
 - ◆ Devices/Ports
 - ◆ Users
 - ◆ Programs

- Affects Where the Authentication Material Must be Distributed as well
 - ◆ Softer authentication *objects* might be harder to supply with an *authentication identity*

- Standardization for this is in its infancy
 - ◆ What your gut says is right may not be supported

Where to Authenticate

➤ Multiple Places to Authenticate

- ◆ In the End Devices
 - › More Management by Walking Around
- ◆ Central Security Server (e.g., RADIUS)
 - › More Lines-of-Communication Concerns

➤ Well-Designed Security Features Always Give You This Choice

- 50,000' View
- Management Concerns
- **Nuts and Bolts**
 - ◆ Transport Security (not much new)
 - ◆ **Command Security (very interesting)**
- Current Status

Transport Security

- Authenticates Hardware (HBAs & Drive Ports)
- Hardware-based encryption
- Encrypts/Integrity Checks Whole Frames

Command Security

- **New** Commands
- **New** SAs (Security Associations) for Command Uses
- **New** Command-Parameter Data Encryption and/or Integrity Checking
- **New** Extensions to Commands
- **New** Capability-Based Security on Commands

Security Commands

- SECURITY PROTOCOL IN/OUT Command
 - ~225 protocol codes still available for T10 assignment
 - ◆ Five protocols already used by T10
 - ◆ IEEE 1667 *Host Authentication*
 - ◆ ATA Drive Locking
 - ◆ Six protocols assigned to the Trusted Computing Group (www.trustedcomputinggroup.org)
 - ◆ 16 Vendor Specific



**Check out SNIA Tutorial:
TCG Trusted Storage
Specification**

SECURITY PROTOCOL IN/OUT

- Very Flexible
 - ◆ See list of existing uses

- Mostly a Data-Transfer Shell
 - ◆ Contents Always More Interesting Than Vessel

- Widespread Tendency to Abbreviate
 - ◆ SPIN and SPOUT

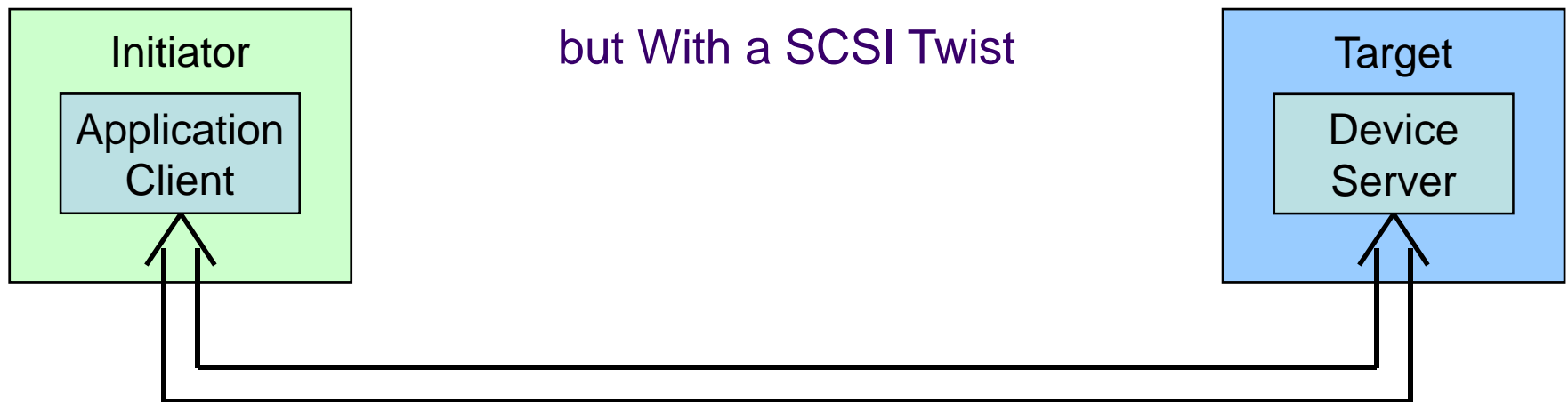
- One Use with Broad Implications is Command-Based SA Creation

Command-Based SCSI SAs

Modeled on IKEv2 SAs

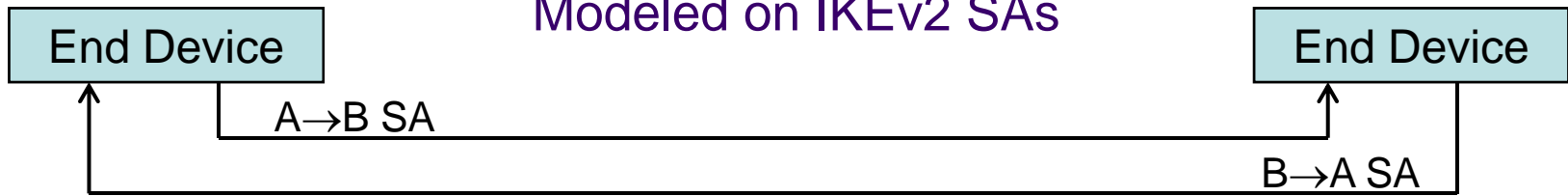


but With a SCSI Twist

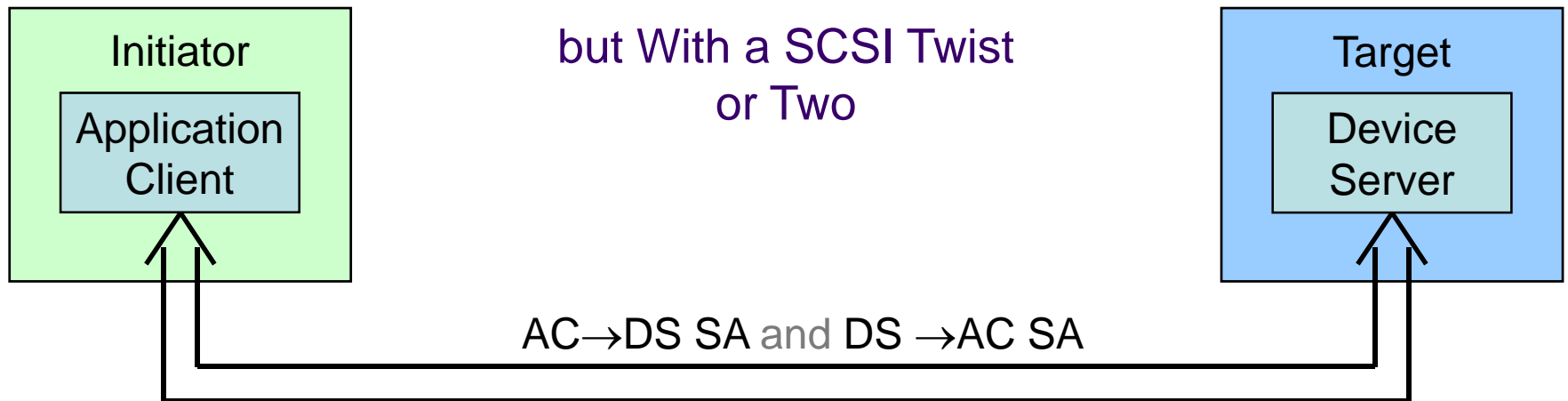


Command-Based SCSI SAs

Modeled on IKEv2 SAs

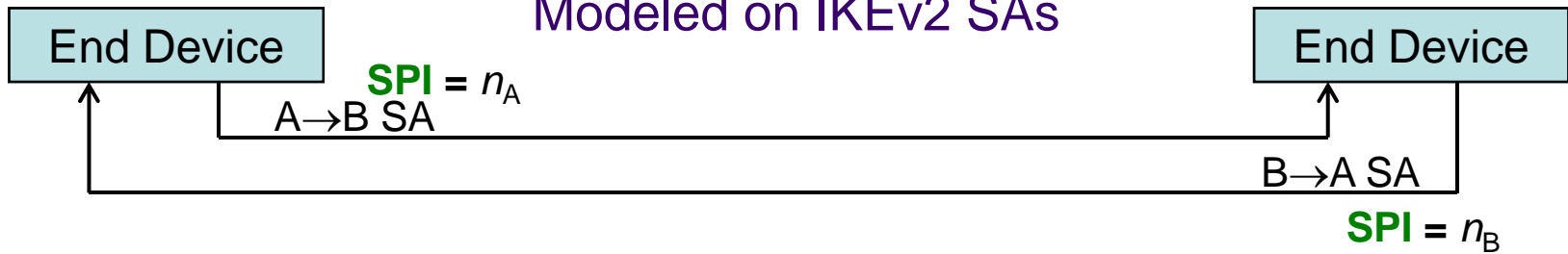


but With a SCSI Twist
or Two

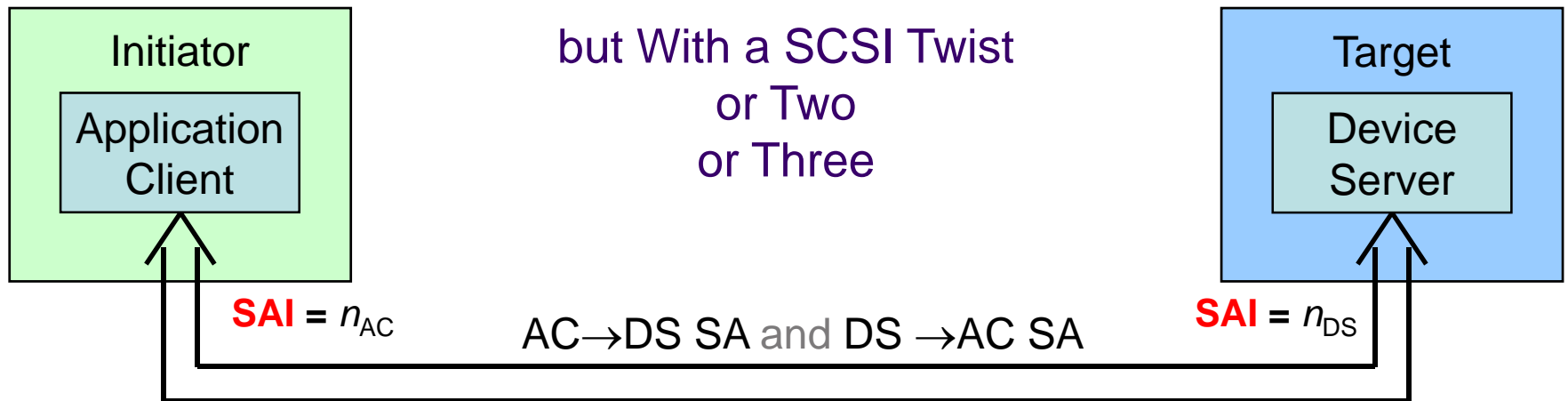


Command-Based SCSI SAs

Modeled on IKEv2 SAs



but With a SCSI Twist
 or Two
 or Three



Command-Based SCSI SAs

- Command-Based SAs are:
 - ◆ Created in response to Application Client Commands
 - ◆ Setup via a pair of SPIN/SPOUT Protocols
 - › Determine Supported Features (one command)
 - › Create the SA (two or four commands)
 - ◆ Not Qualified by I_T Nexus
 - › n_{DS} is unique throughout the Device Server (not qualified by n_{AC})
 - › Use Not Limited to One Initiator/Target Pair
 - › Initiators Can
 - Exchange SA Information Out-of-Band or
 - Use One SA Across Multiple Ports on a Target
 - › How useful this is remains to be seen

CDB History

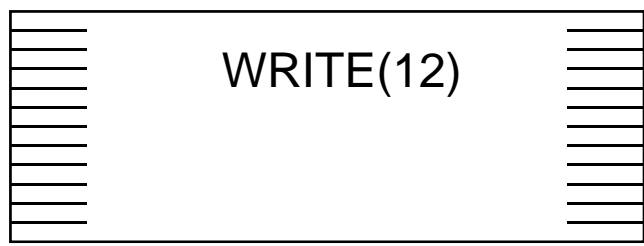
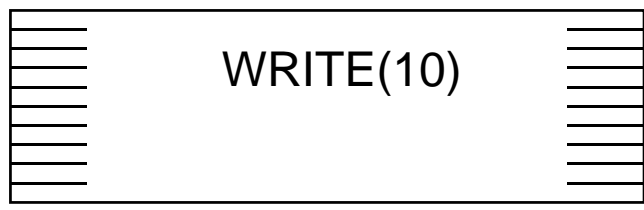
SCSI



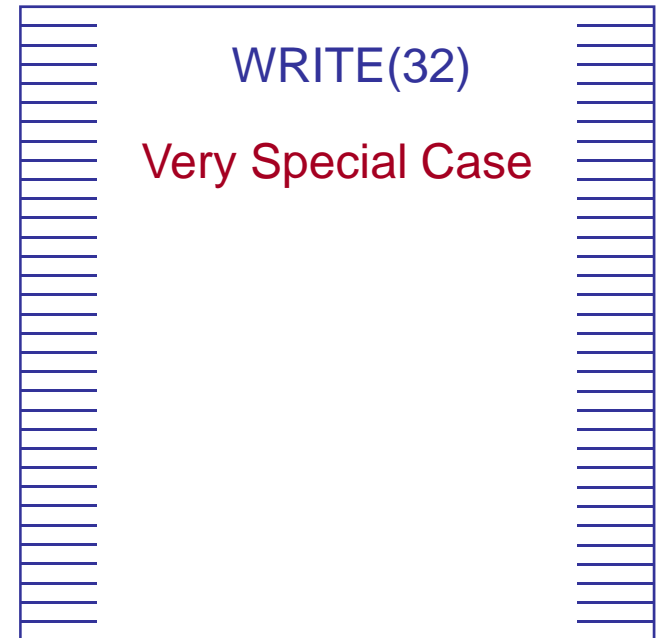
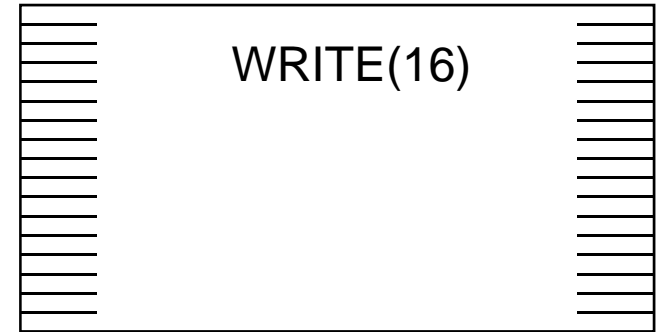
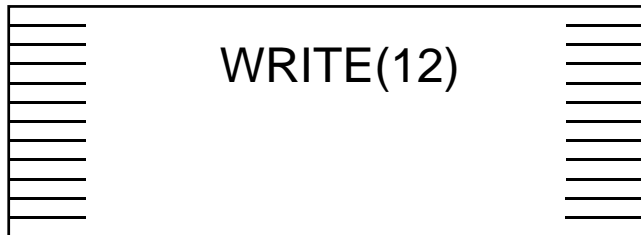
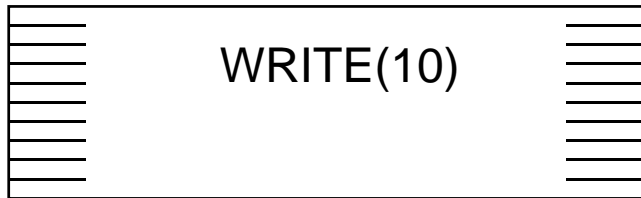
S = Small

CDB History

SCSI
↕
S = Small

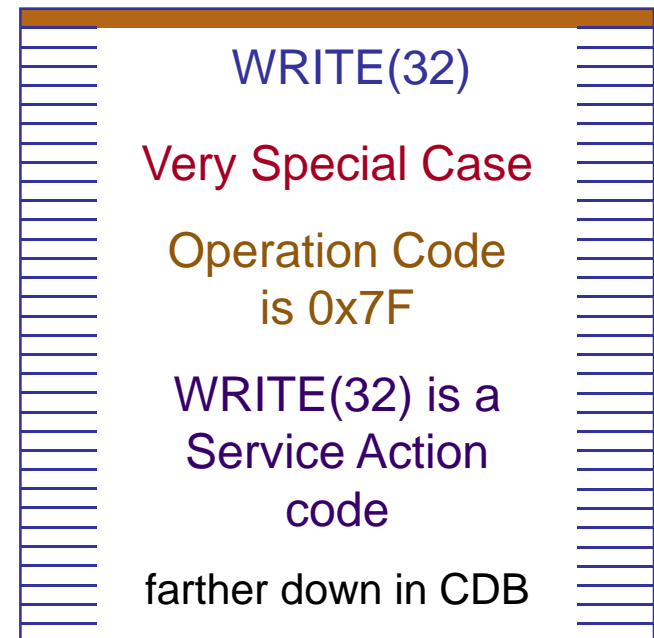


CDB History



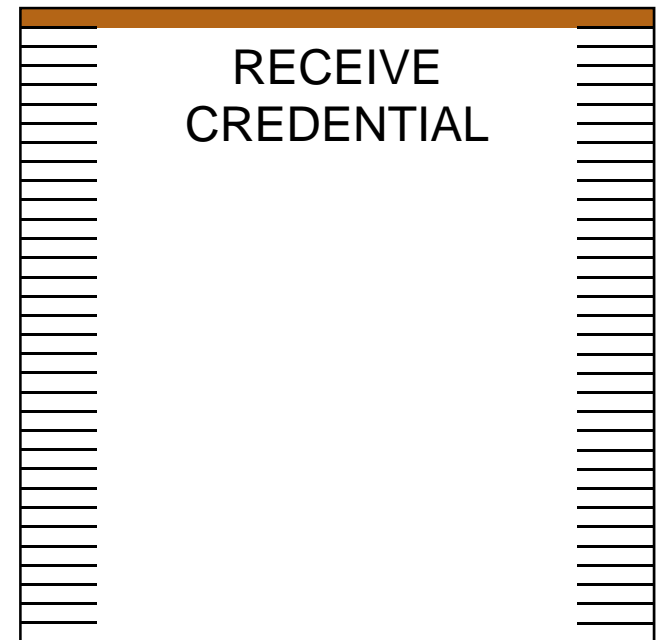
CDB History

- Operation Code 0x7F
 - ◆ **Means Variable Length CDB**
 - ◆ WRITE(32) bends the rules a little bit
 - ◆ Other Commands better fit the real rules

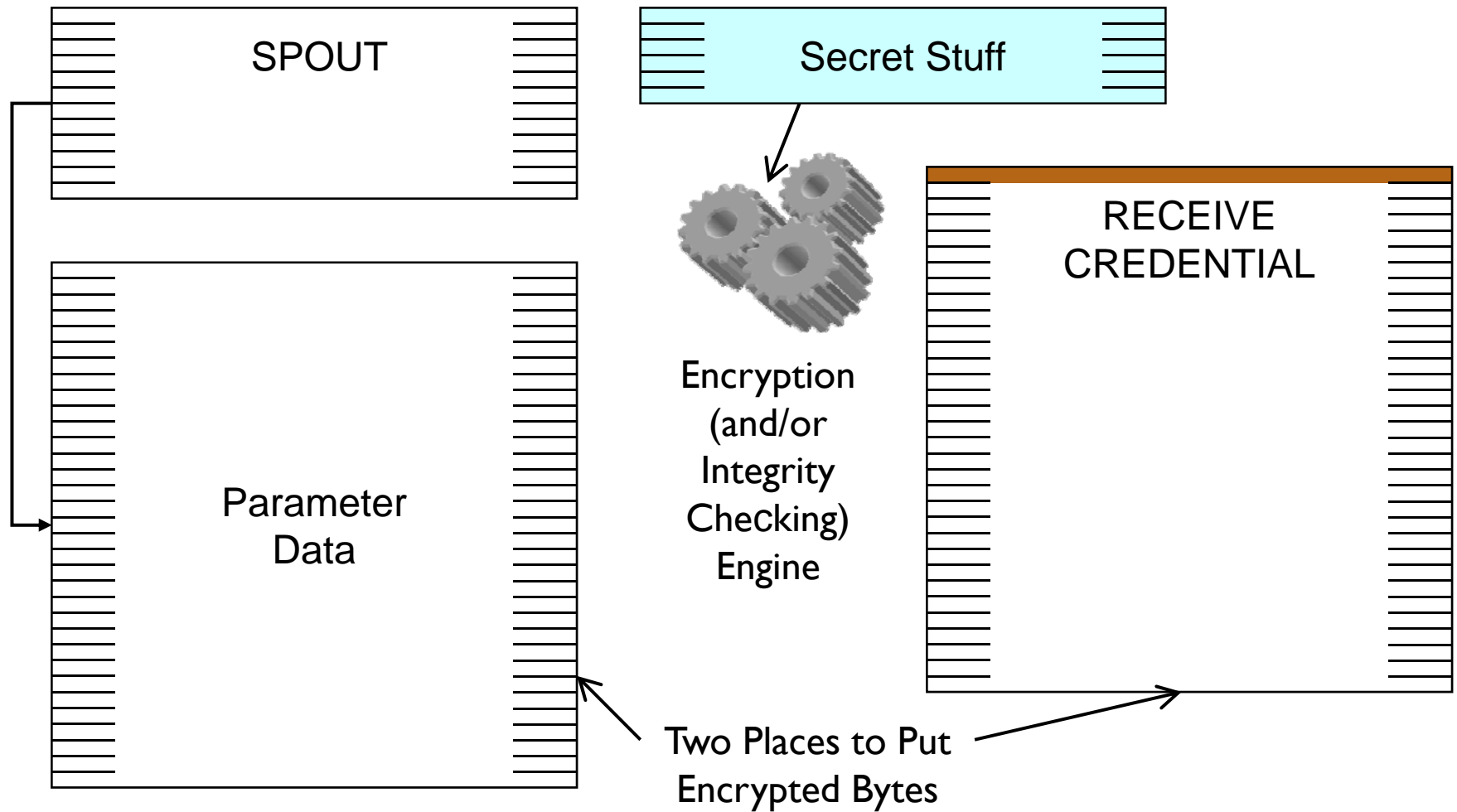


CDB History

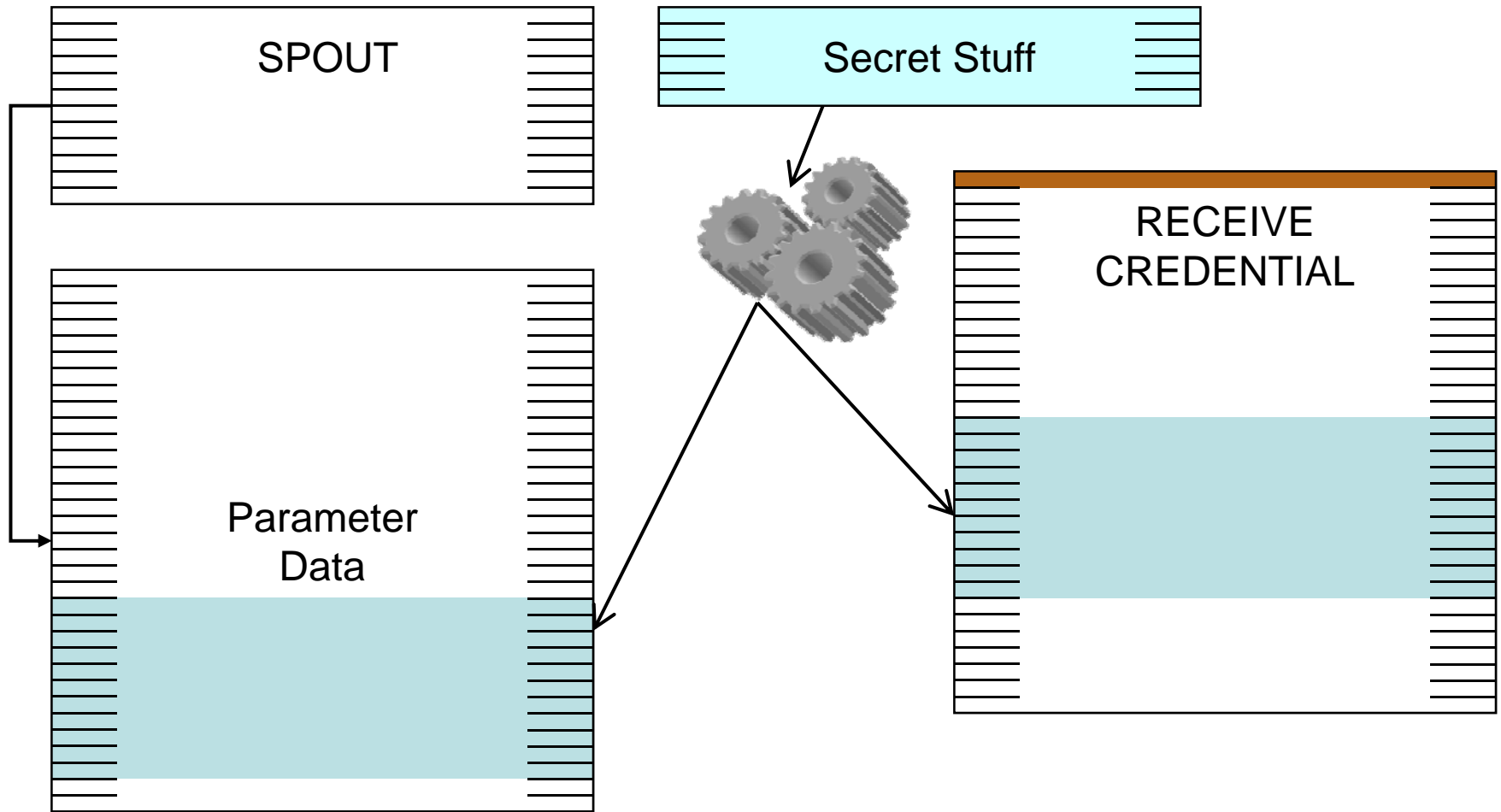
- Other commands fit better
- **RECEIVE CREDENTIAL**
 - ◆ A Capability-Based Command Security command
- **Operation Code 0x7F**
 - ◆ Means Variable Length CDB
 - ◆ Same as WRITE (32)
 - ◆ Service action is different
- **Big (larger than 16 bytes) CDB**



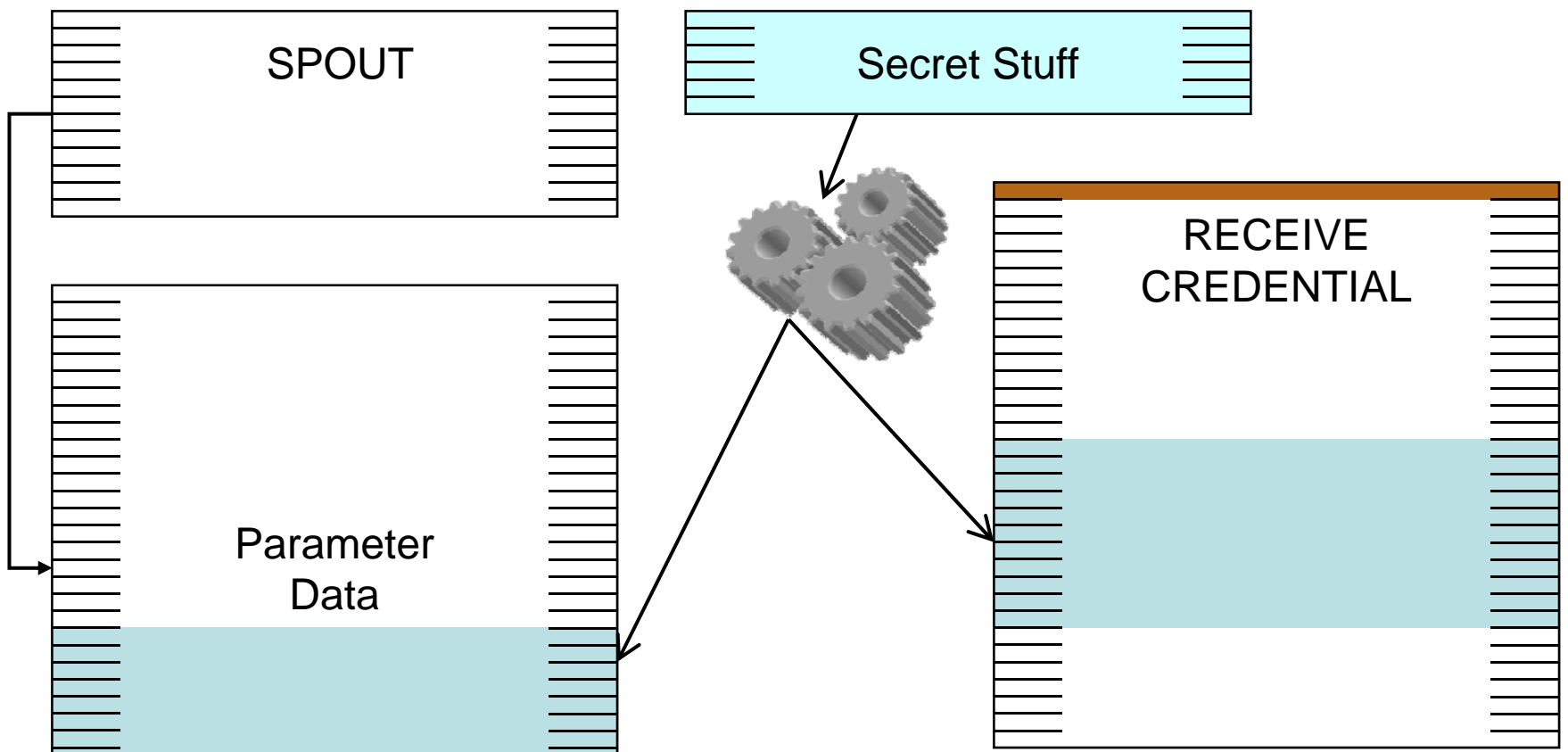
Command Data Encryption



Command Data Encryption



Command Data Encryption

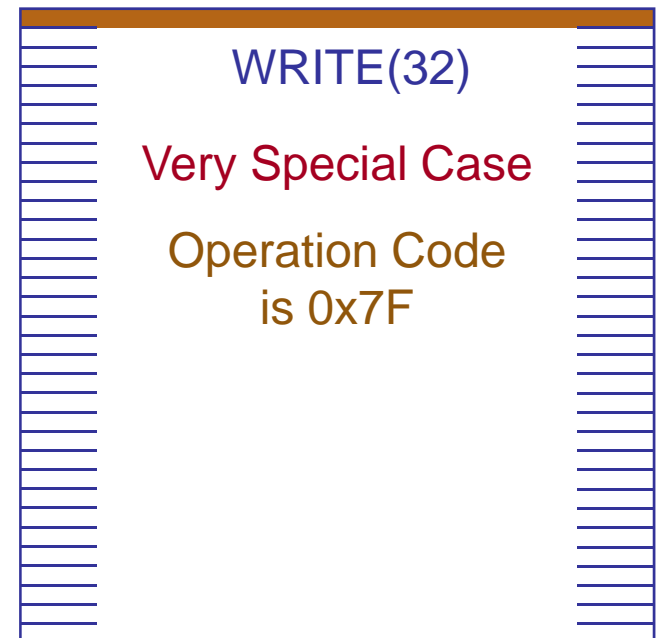
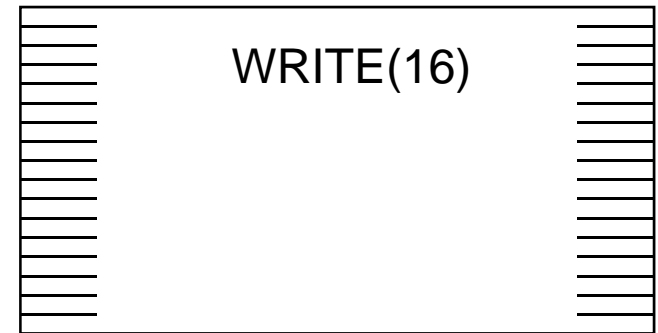
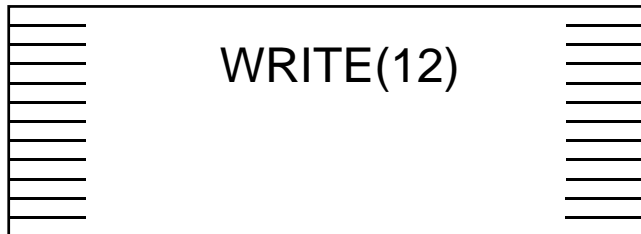
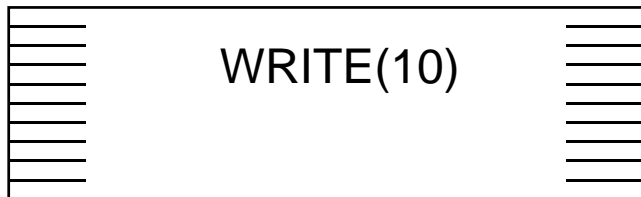


- Minimum Overhead is 16 Bytes
- Parameter Data and Variable Length CDBs Are the Only Viable Uses

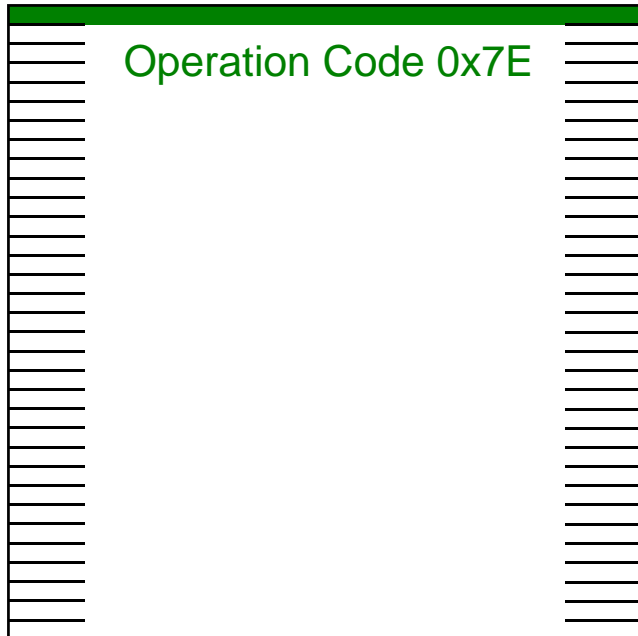
Command Data Encryption

- Define an SA to Specify
 - ◆ Type of Encryption
 - ◆ Type of Integrity Checking
- Use SA to *Protect* One or More Fields in Command-Related Parameter Data or CDB
 - ◆ Encrypt Some Parameter Data
 - ◆ Encrypt All Parameter Data
 - ◆ Encrypt Some CDB fields (**not all of CDB**)
- Ready-to-Use Tools in SPC-4
 - ◆ Used by:
 - > Tape-Data-Encryption Keys
 - > Capability-Based Command Security Credentials

CDB History (reprise)

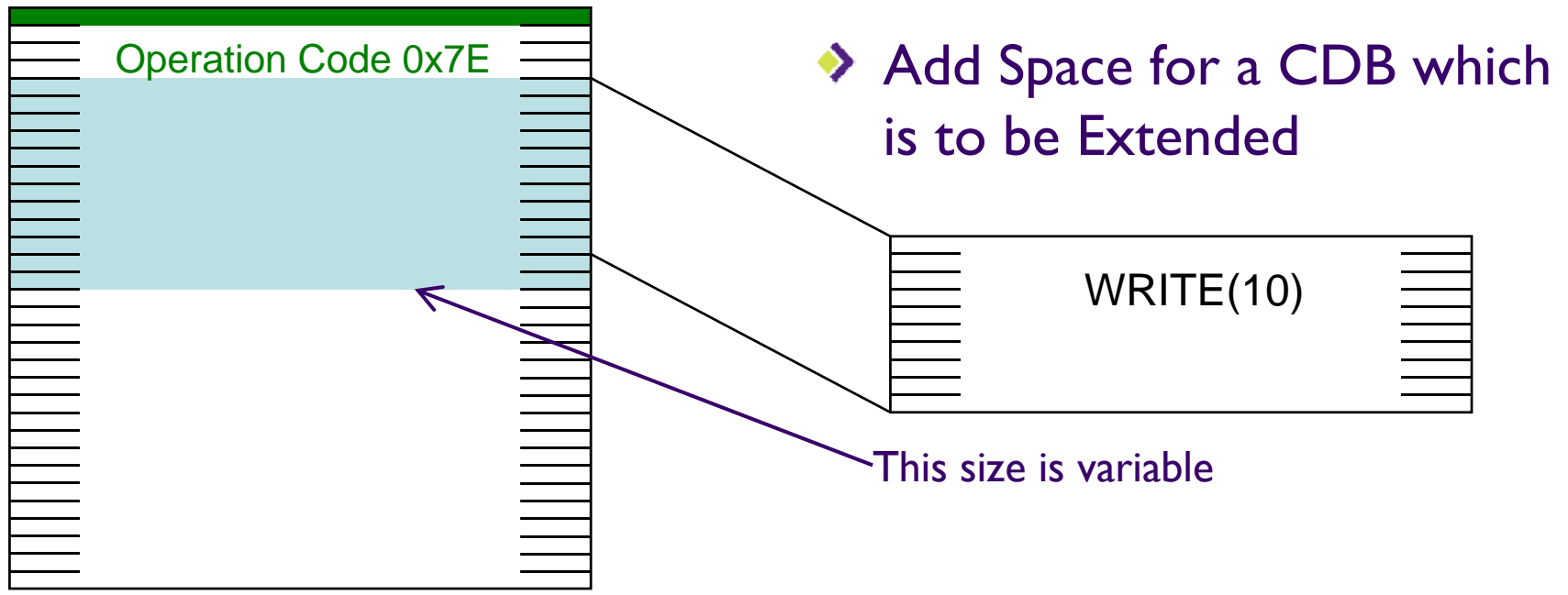


CDB Extensions

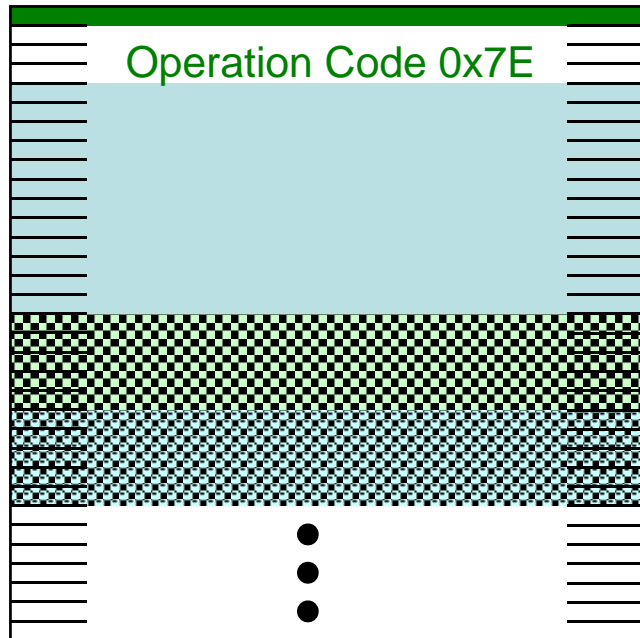


- Take the Variable Length CDB Concept
- Tweak the Operation Code
- Start to Build Something New

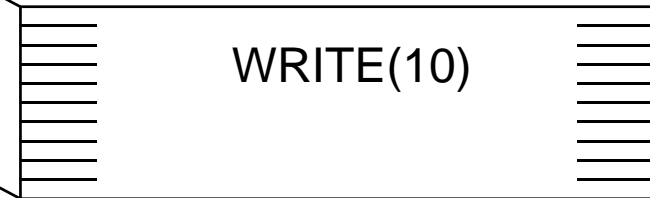
CDB Extensions



CDB Extensions



➤ Add Space for a CDB which is to be Extended

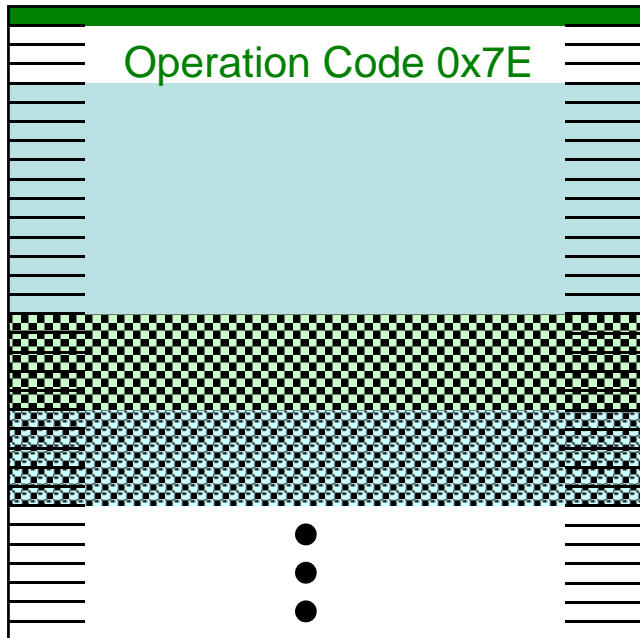


➤ Add One or More CDB Extensions

- ◆ Per-Command Quality of Service
- ◆ Per-Command Usage Classification
- ◆ Capability-Based Command Security
- ◆ ...

➤ Better Than 100's of New CDBs

CDB Extensions



➤ Add Space for a CDB which is to be Extended

➤ Add One or More CDB Extensions

- ◆ Per-Command Quality of Service
- ◆ Per-Command Usage Classification
- ◆ Capability-Based Command Security
- ◆ ...

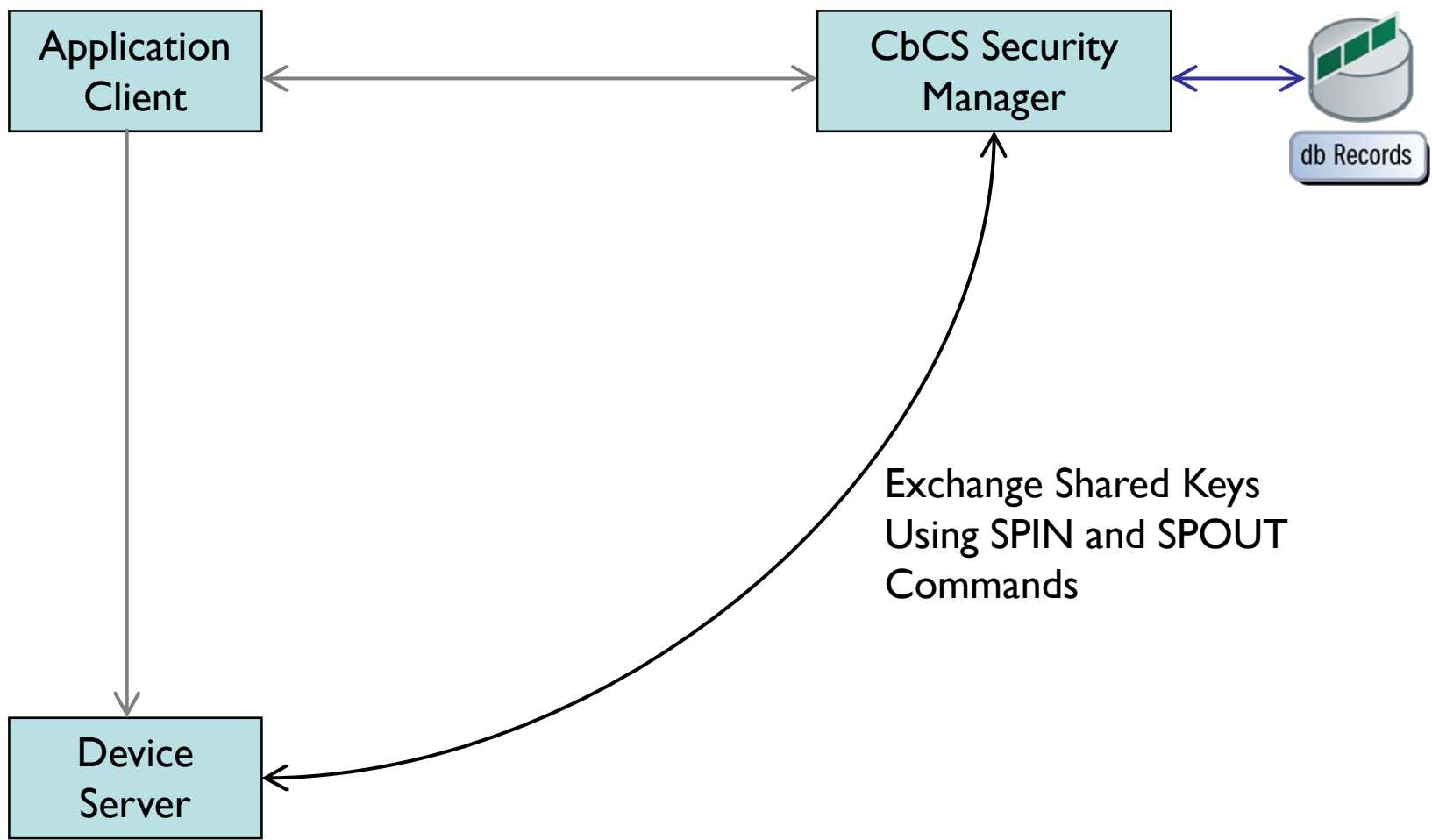
➤ Better Than 100's of New CDBs

There is a limit to this fun. No CDB can be bigger than 250 bytes.

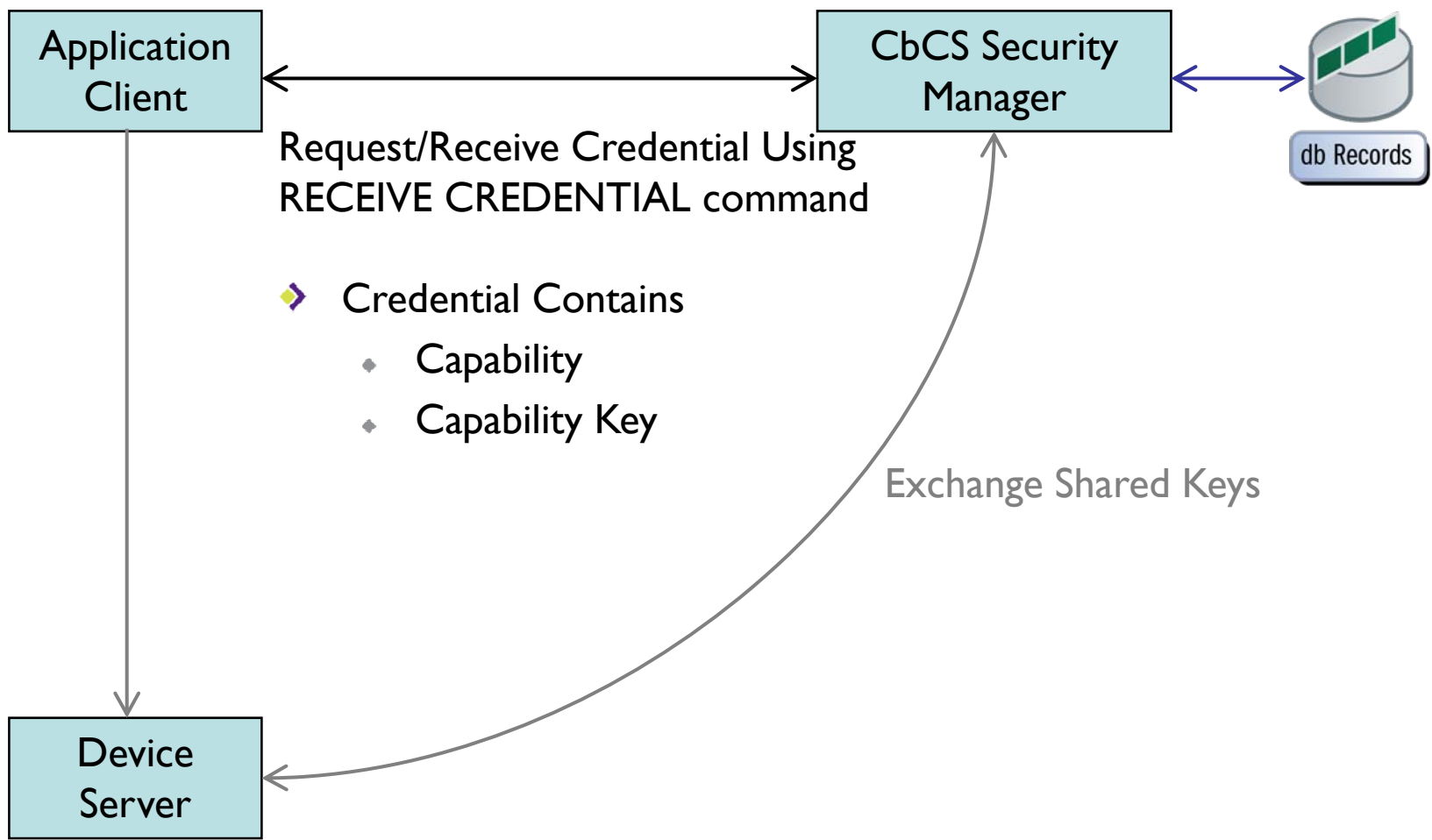
Capability-Based Command Security SNIA

- **Authenticate With Credential Server**
 - ◆ With SA, maybe other mechanism
- **Request Credential**
 - ◆ Encrypt Credential using above mentioned SA
- **Extend CDB by Adding Credential**
 - ◆ See CDB Extensions in previous slide
- **Manage Access to a Resource**
 - ◆ Defined for Disks, Tapes, and Media Changers

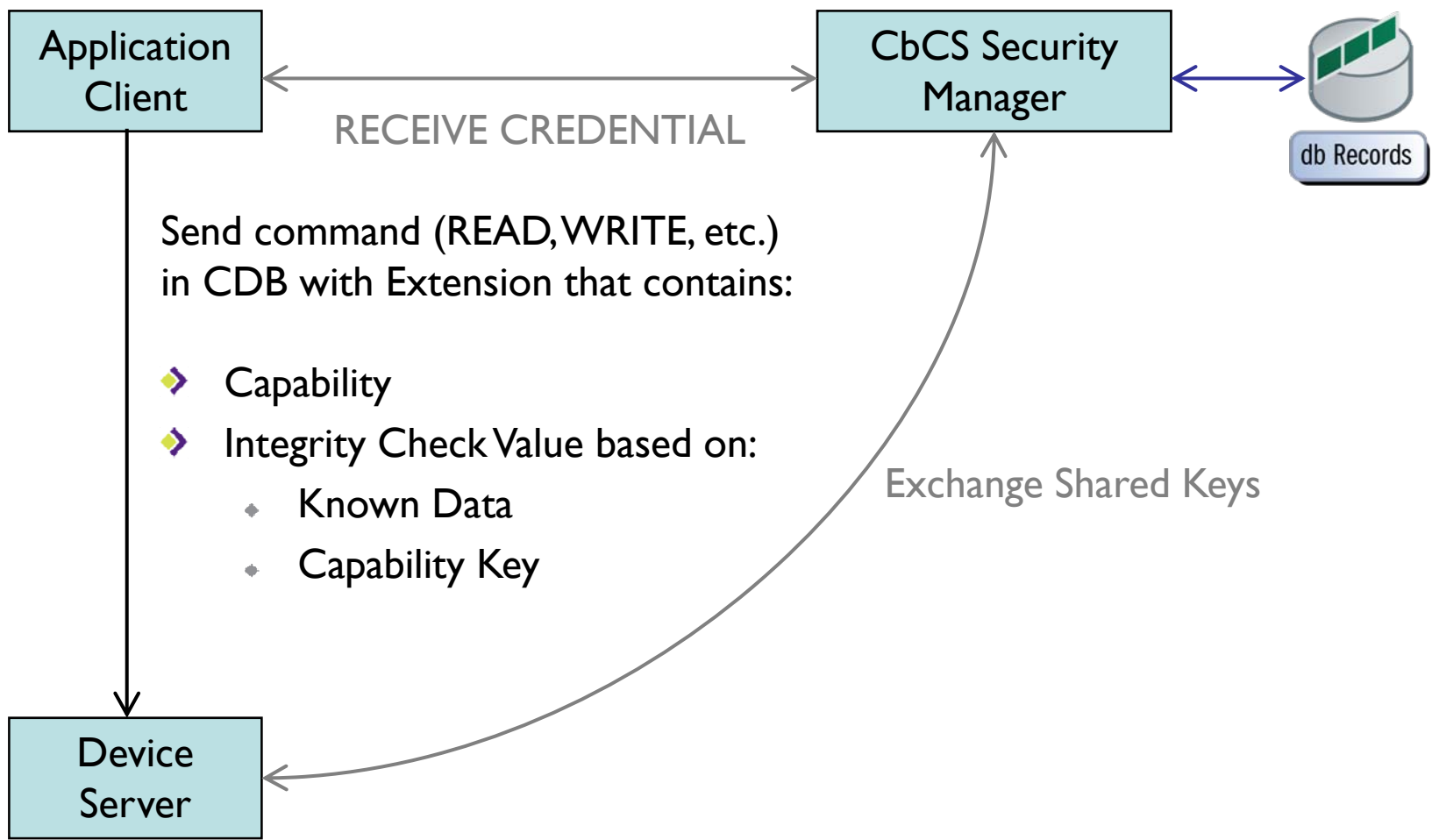
Capability-Based Command Security SNIA



Capability-Based Command Security SNIA



Capability-Based Command Security SNIA



Agenda

- 50,000' View
- Management Concerns
- Nuts and Bolts
- **Current Status**

Completed Tasks

- SPC-4 Working Draft ready with:
 - ◆ SA Creation
 - ◆ Capability-Based Command Security
 - ◆ <http://www.tl0.org/ftp/tl0/drafts/spc4/spc4r16.pdf>

- SSC-3 Working Draft in Letter Ballot with:
 - ◆ Tape Data Encryption Key Management based on SAs
 - ◆ <http://www.tl0.org/ftp/tl0/drafts/ssc3/ssc3r04a.pdf>

- SAT-2 Working Draft in Letter Ballot with:
 - ◆ ATA Drive Locking
 - ◆ <http://www.tl0.org/ftp/tl0/drafts/sat2/sat2r06.pdf>

Where Is All This Headed?

➤ The Sky's the Limit

- ◆ Reservations with Authenticated Access Restrictions
- ◆ Non-Capability Command Security
 - › Some people think Capability-Based Command Security is too complex
- ◆ Command level SAs seed Transport level SAs

➤ Work With Your Equipment Vendors to Request Features You Need

- Please send any questions or comments on this presentation to SNIA: tracksecurity@snia.org

**Many thanks to the following individuals
for their contributions to this tutorial.**

- SNIA Education Committee

**Roger Cummings
David Black
Eric Hibbard
Ralph Weber**