
Education

# SCSI Security Nuts and Bolts

Ralph Weber, ENDL Texas

# SNIA Legal Notice

- 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.

# Abstract

## 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.

# Notice

- The authors are NOT attorneys, and nothing in this presentation is intended to be (and should not be) construed as legal advice or opinion. If you need legal advice or a legal opinion, please contact an attorney.
- The information presented herein represents the authors' personal opinions and understanding of the issues involved. The author, contributors, presenter, conference host, and SNIA **DO NOT** assume any responsibility or liability for damages arising out of any reliance on or use of this information.

# Agenda

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

# This History of SCSI (in one slide)

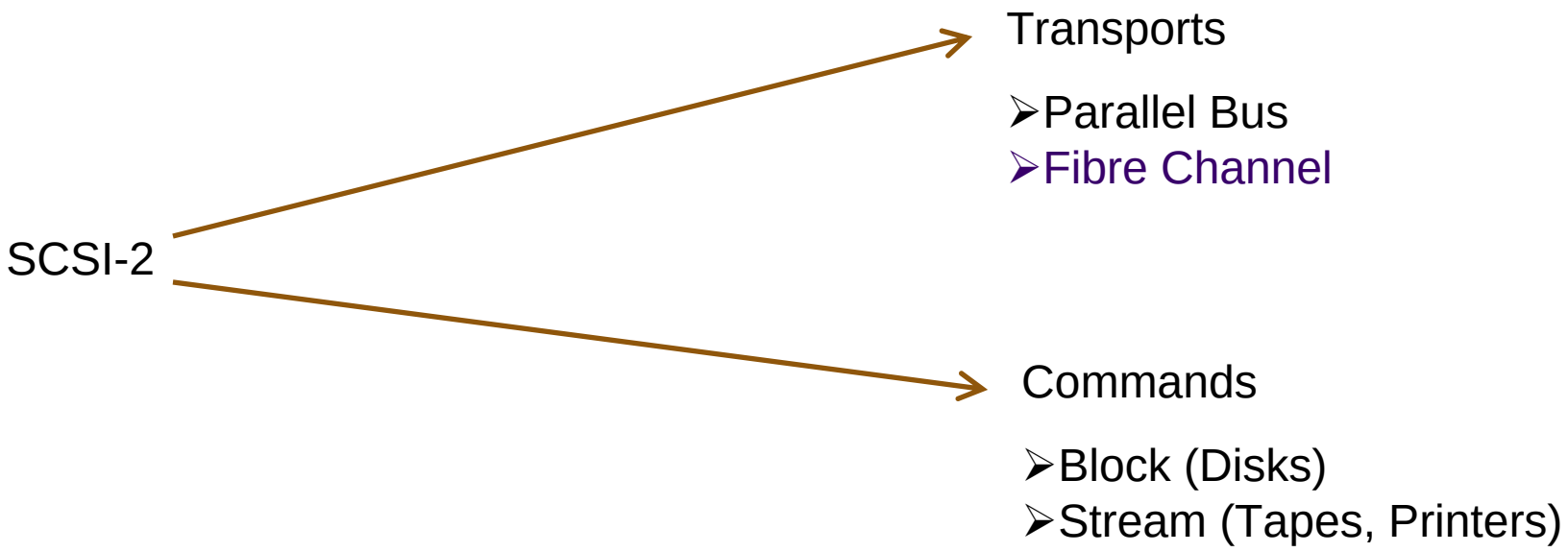
1980 — 1989

SCSI-2

- Parallel Bus
- Disks
- Tapes
- …

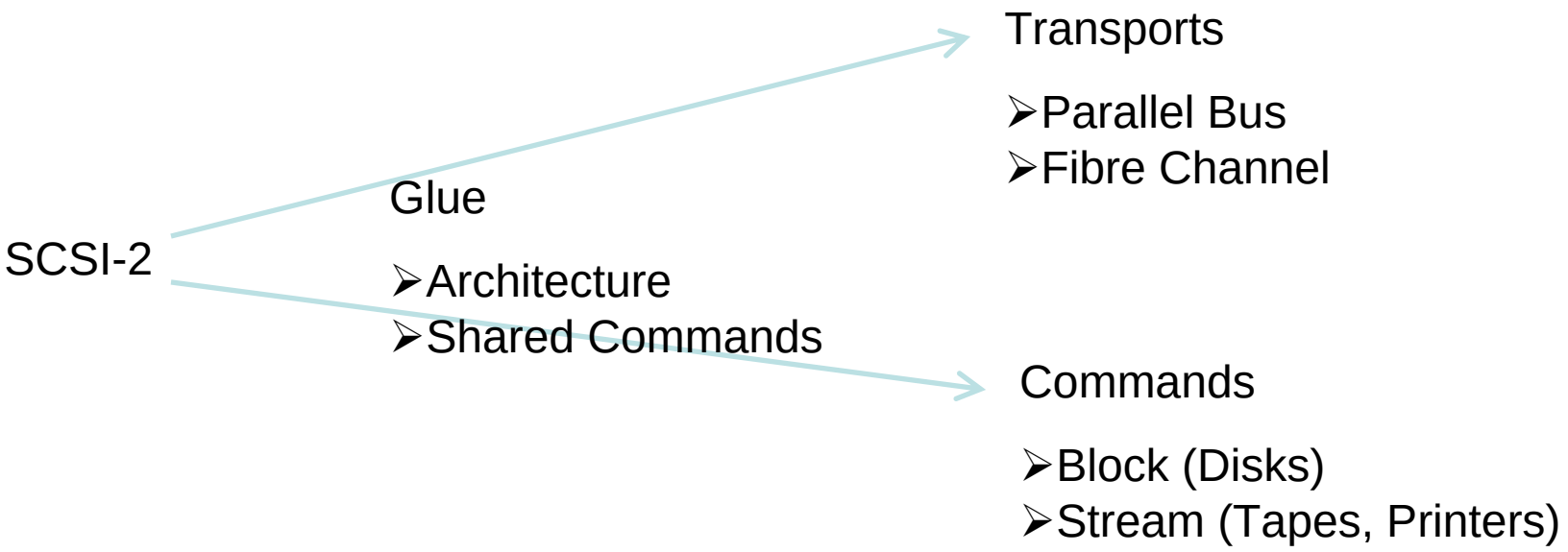
# This History of SCSI (in one slide)

1980 — 1989 1990

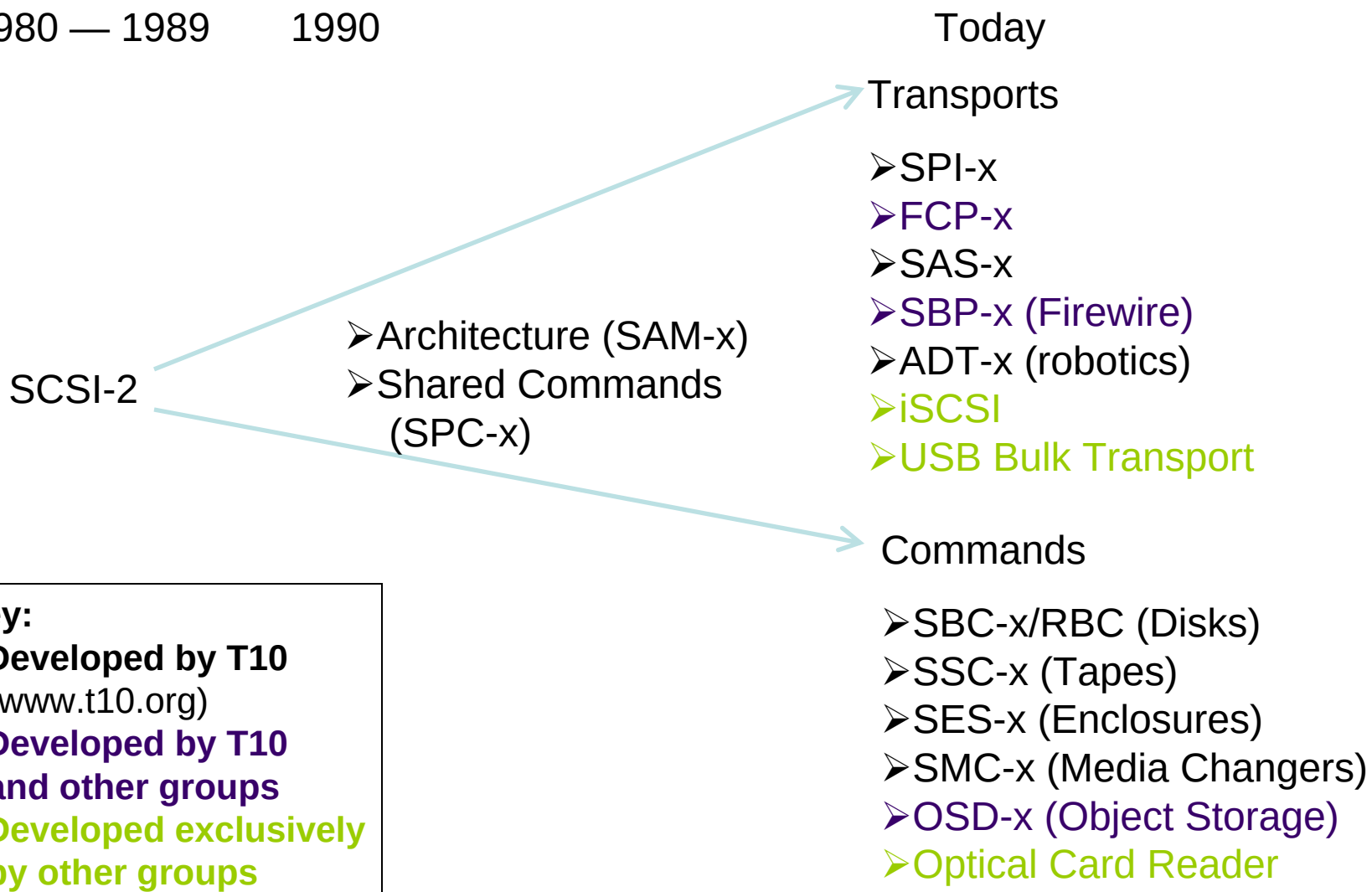


# This History of SCSI (in one slide)

1980 — 1989 1990



# This History of SCSI (in one slide)




**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
    - USB
    - SAS
    - Fibre Channel
    - iSCSI

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

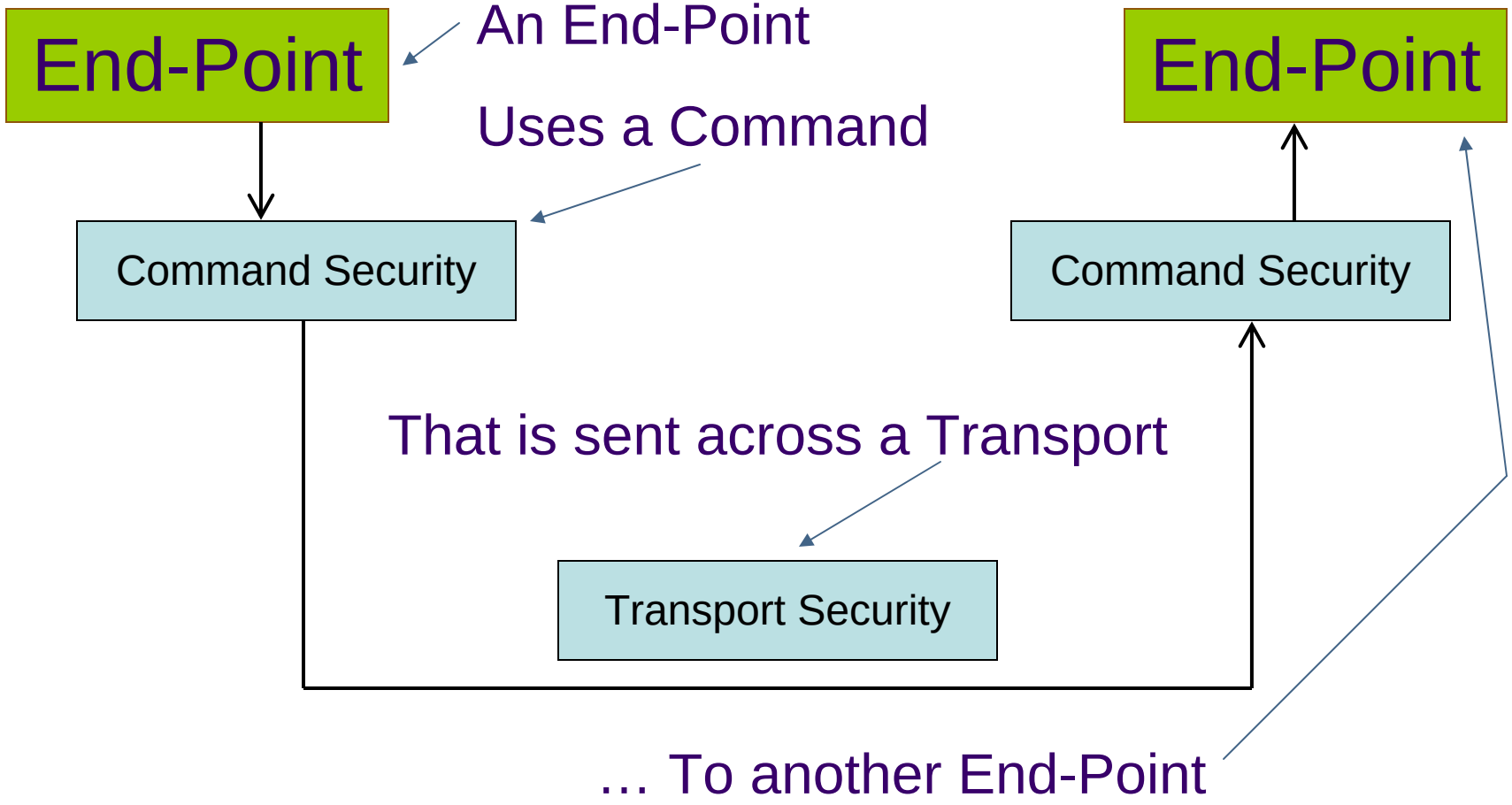
**Check out SNIA Tutorial:**

**Fibre Channel Technologies: Current and Future**

**Check out SNIA Tutorial:**

**IP Storage Protocols - iSCSI**

# Ultimate Security *Enforcement* Point



# End-Point Postscript

Warning: The definition of End-Point is fuzzy.

- HBA (Host Bus Adapter) builders see End-Point as the HBA

# End-Point Postscript

Warning: The definition of End-Point is fuzzy.

- HBA 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
  - 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 encryption
- Encrypts/Integrity Checks Only Specific Data
  - Command Data (as currently defined)
    - Encrypt a Tape-Data-Encryption key in transit from Host to Drive
  - Not User Data
- See SPC-4 (SCSI Primary Commands) and other command standards

# Security Toolbox

- Authentication
  - Example: Driver's License Check
- Integrity Checking
  - Example: Notarized Copy
- Encryption
  - Example: Pig Latin

# Security Jigsaw Puzzle

- Several ways to do the same thing
  (using Tape-Data-Encryption keys as an example)
- Transport Level Encryption
  - (Hardware) Encrypt everything
  - Including the Tape-Data-Encryption keys
- Command Level Encryption
  - Setup Security Association (extra commands)
  - (Software) Encrypt just the Tape-Data-Encryption keys

# 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

# Agenda

- 50,000' View
- Management Concerns
  - Distributing Authentication Info
  - How to Authenticate
  - What to Authenticate
  - Where to Authenticate
- Nuts and Bolts
- Loose Ends

# 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 and IT Compliance**

# Distributing the Authentication Info

- Multiple Ways to Authenticate Devices
  - Certificates (aka Public Key Infrastructure)
  - Shared Secrets (aka *passwords*)
- Multiple Things That Can Be Authenticated
  - Devices/Ports
  - Users
  - Programs
- Multiple Places to Authenticate
  - 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 too
  - 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

# Agenda

- 50,000' View
- Management Concerns
- Nuts and Bolts
  - Transport Security (not much new)
  - Command Security (very interesting)
- Loose Ends

# 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
    - SD Card TrustedFlash (www.sdcard.org)
    - Six protocols assigned to the Trusted Computing Group (www.trustedcomputinggroup.org)
    - 16 Vendor Specific

**Check out SNIA Tutorial:**

**TCG Trusted Storage Specifications**

# 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

# Command-Based SAs

- Setup via a Pair of SPIN/SPOUT Protocols
  - Determine Supported Features (one command)
  - Create the SA (two or four commands)
- Identified by Indices
  (but with differences from Transport SAs)
  - Two SAs per Creation Operation (In and Out)
    - Best fit for SCSI command structure
  - Index called SAI (Security Association Index)
    not SPI (Security Parameters Index)
    because SPI is the name of the Parallel Bus standard
  - Numerous differences in the details too

# Command-Based SAs

- SA Pair is Not Qualified by I_T Nexus
  - Use Not Limited to One Pair of SCSI Devices
  - Device Server Required to Assign a Unique SAI to Every SA It Creates
  - Hosts Can
    - Exchange SA Information Out-of-Band and
    - Use SAs Across Any Port
- How useful this will be is yet to be seen

# 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 Data
  - Encrypt Some Data
  - Encrypt All Data
- Ready-to-Use Tools in SPC-4
  - Used by:
    - Tape-Data-Encryption Keys
    - Capability-Based Command Security Credentials

# CDB Extensions

- General Mechanism for Adding Chunks of New Data to Every CDB (Command Data Block)
  - Better than defining hundreds of new CDBs
- Uses
  - Per-Command Quality of Service
  - Per-Command Usage Classification
  - Capability-Based Command Security Extensions
  - …

# Credential-Based Command Security

- Authenticate With Credential Server
  - Maybe 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

# Credential-Based Command Security

- Authenticate With Credential Server
  - Maybe 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
- Much Like Standard OSD (Object-based Storage Device) Security Feature

# Agenda

- 50,000' View
- Management Concerns
- Nuts and Bolts
- Loose Ends

# Where Is All This Headed?

- The Sky's the Limit
  - Reservations with Authenticated Access Restrictions
  - Non-Credential Command Security
    - Some people think Credential-Based Command Security is too complex
  - Command level SAs seed Transport level SAs

- Work With Your Equipment Vendors to Request Features You Need

# Q&A / Feedback

- 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**