SNIA

STORAGE NETWORKING INDUSTRY ASSOCIATION

EDUCATION

Best Current Practices and Implementing the FC Security Protocol (FC-SP)

Larry Hofer, CISSP

Emulex

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.

© 2007 Storage Networking Industry Association. All Rights Reserved.

Abstract

Exploring FC-SP Best Current Practices Support and Planning for Implementation

The variety of environments in which Fibre Channel fabrics are deployed makes it difficult to rely on physical security. Different users may access storage subsystems over Fabrics that may span several sites. Security services are extremely important to prevent misconfigurations or access to data by non-authorized entities.

A new standard, the Fibre Channel Security Protocol (FC-SP) can improve fabric security, reduce the total cost of ownership (TCO) and improve availability. These benefits are the result of simplified management and mitigated threats, both accidental and malicious.

In this focused technical session, we develop an in-depth understanding of the new security architecture for Fibre Channel. Then, we identify key steps to help you implement the FC-SP framework and understand how it supports best current practices. Within this framework, a Fibre Channel device can verify the identity of another Fibre Channel device. A device may also use a shared secret and a key exchange protocol to establish security associations applied to Fibre Channel frames and information units. This framework also allows for the distribution of fabric-enforced policies within a Fibre Channel fabric. Some of these features are quickly becoming available.

Learning Objectives

–Understand underpinning concepts including device to device (hosts, disk, switches) authentication, data origin authentication, integrity, anti-replay protection, confidentiality, the role of IKEv2 protocol for Fibre Channel entities authentication and/or setup of security associations, and security policy distribution.

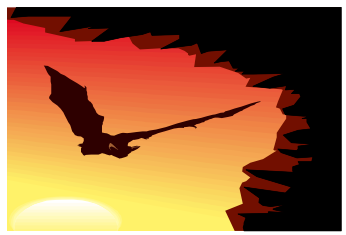
–Manage and establish secrets and security associations.

–Prepare to implement FC-SP functionality, including planning decisions, implementation process and changes in storage administrator practices in support of best of current practices.

© 2007 Storage Networking Industry Association. All Rights Reserved.

What we will explore

- Implementation Decisions, Planning, Process, Administrative Practices along the way
- Fibre Channel Security Protocols (FC-SP) Architecture
  - Authentication Infrastructure
    - Secret, certificate, or password based
  - Authentication
    - Device to device (hosts, disks, switches) authentication choices
      - Data origin authentication, integrity, anti-replay protection.
      - Managing secrets choices
  - Authorization (access control) choices
    - FC Fabric policies, FC-SP zoning
    - Summarizing Policies – N_Port verification of select policies
  - Security Associations (SA)
    - IKEv2 protocol for FC entities for authentication or SA setup
    - Managing and establishing associations
  - Cryptographic Integrity and Confidentiality choices



© 2007 Storage Networking Industry Association. All Rights Reserved.

What's in it for you?

- The Fibre Channel Security Protocols (FC-SP) :
  - Supports in-band authenticated and confidential management traffic
  - Supports creation of trusted fabrics and FC SAN infrastructure
  - Protects against certain operator errors or cable misconnections
  - Improved scalability promised in new zoning approach
  - Supports protecting data in-flight
  - Supports checking of network configuration for MF environments
- FC-SP supports best practices in SAN security
  - Authentication, Authorization, Integrity/Confidentiality
- Authentication should be used in storage networks.

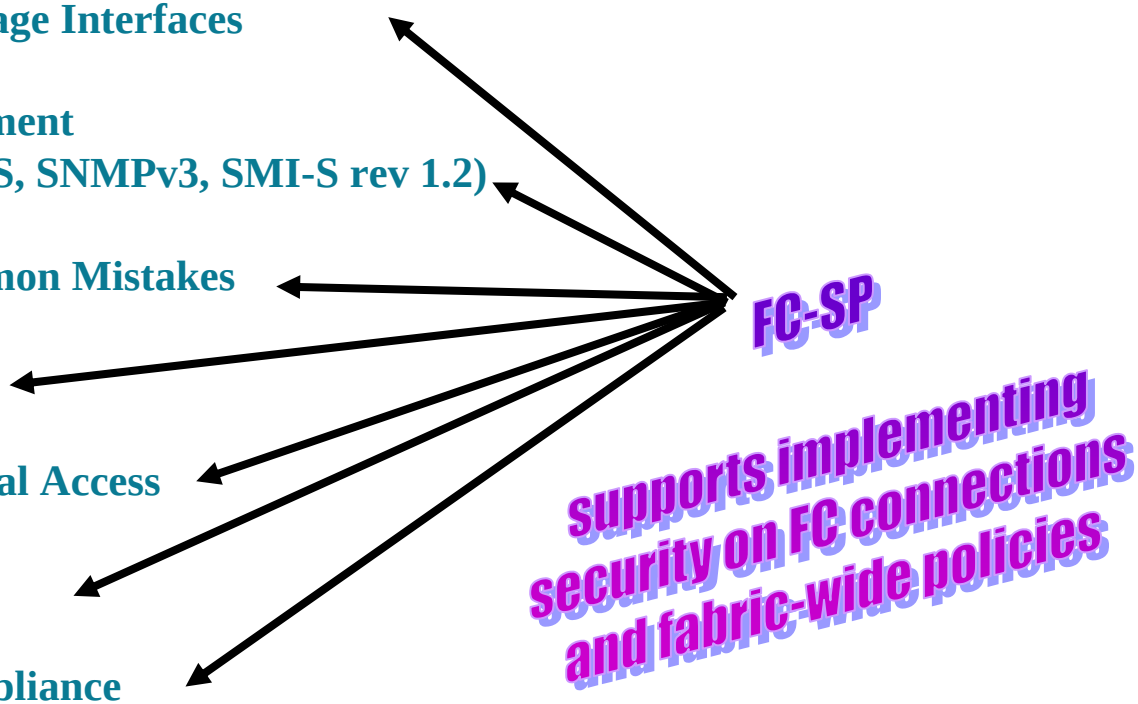
DEMAND (MANDATORY) AUTHENTICATION SUPPORT NOW!

© 2007 Storage Networking Industry Association. All Rights Reserved.

Best Current Practices

SNIA
Storage Networking Industry Association
EDUCATION

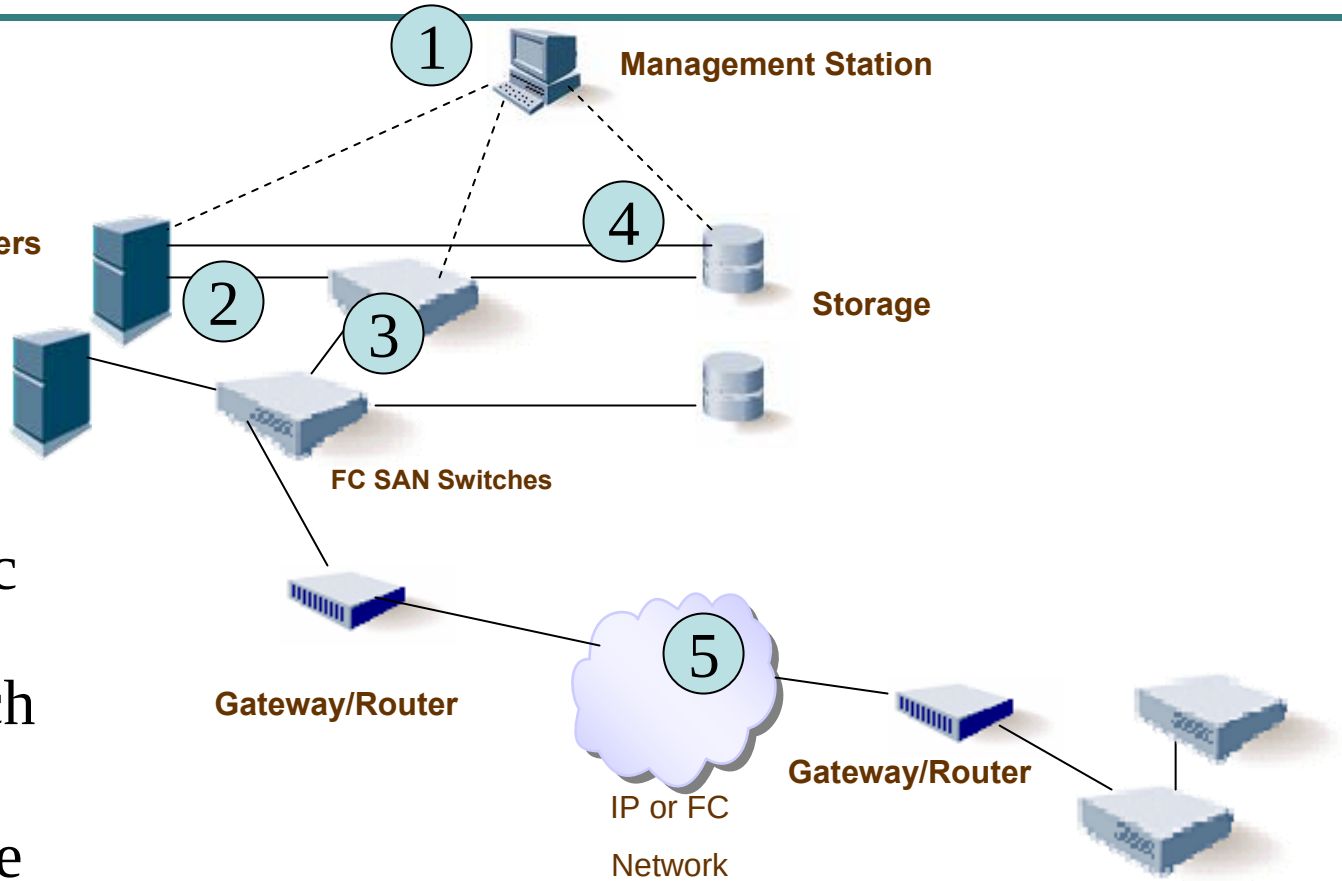
1. **Identify and Assess All Storage Interfaces**
2. **Secure the Storage Management (e.g. FC Mgt, SSH, SSL/TLS, SNMPv3, SMI-S rev 1.2)**
3. **Avoid Failures Due to Common Mistakes**
4. **Create Risk Domains**
5. **Monitor and Control Physical Access**
6. **Protect Externalized Data**
7. **Address Data Security Compliance**
8. **Understand the Exposures**
9. **Implement Appropriate Service Continuity**
10. **Utilize Event Logging**



Source: Introduction to Storage Security, A SNIA Security White Paper, October, 2005.

© 2007 Storage Networking Industry Association. All Rights Reserved.

1 Identify Interfaces



Threat Sources:

1. Management
2. Traffic to Fabric
3. Switch to Switch
4. Device to Device
5. IP or FC Network Connections

© 2007 Storage Networking Industry Association. All Rights Reserved.

Secure the interfaces

- FC Management interfaces (see ☑ 2)
- FC Distance connections (see ☑ 6)
- FC Outside the data center connections (see ☑ 6)
- FC Inside the data center connections

Decreasing Risk ?

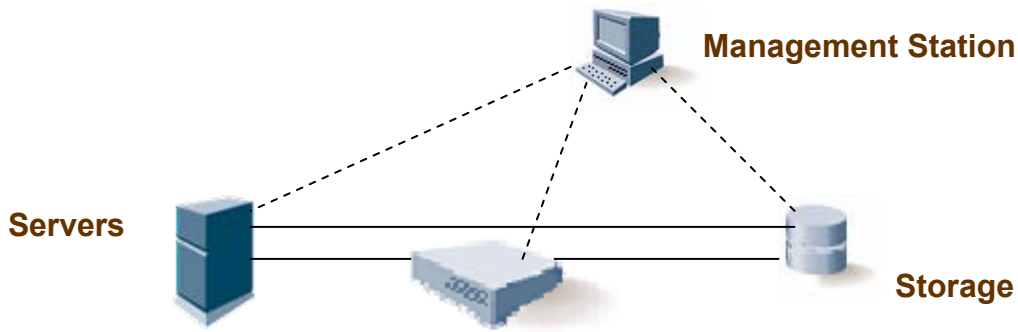
Implementation Tip: Always secure the management interfaces and enable access controls and authentication at a minimum. FC-SP authentication is being supported by most vendors first!

© 2007 Storage Networking Industry Association. All Rights Reserved.

2 Management Interfaces

Examples:

- FC Management Server – Authenticated In-band management can be protected using CT_Authentication and Confidentiality
  - *FC-GS-5 standard (INCITS 427-2007)*
- FC-SP defines IKEv2 for setting up the algorithms, traffic selectors, etc. (IKE = Internet Key Exchange)
- Secure any IP management interfaces, (outside the scope of FC-SP).



© 2007 Storage Networking Industry Association. All Rights Reserved.

3 Avoid Common Mistakes

Examples:

- Use authorization and authentication FC-SP features to avoid accidental misconnections
- Avoid zone merge complications
- Avoid accidents caused by mixed O/S (windows, linux)

Use connectivity/access controls to avoid “cabling” accidents. Example, zone merge won’t occur if authentication fails first (layers). Provide policies/procedures and use trained personnel with proper user roles/permissions.

© 2007 Storage Networking Industry Association. All Rights Reserved.

FC-SP Authentication

© 2007 Storage Networking Industry Association. All Rights Reserved.

FC-SP Authentication

Protocols

- *May negotiate what protocols to use*
  - *DH-CHAP – secrets*
    - ***required for FC-SP compliance***
    - *DH Null required – Diffie-Hellman (DH) is mainly for Security Associations after authentication*
  - *FCPAP – passwords*
  - *FCAP - certificates*

Interfaces

- Switch to Switch
- Device to Switch
- Device to Device

© 2007 Storage Networking Industry Association. All Rights Reserved.

CHAP (RFC 1994)

Challenge **H**andshake **A**uthentication **P**rotocol

- Originally used for Dial In User Authentication
- Used for user or device authentication
- Required for iSCSI standard
- A variation called Diffie Hellman CHAP (DH-CHAP) required by FC-SP Standard

© 2007 Storage Networking Industry Association. All Rights Reserved.

CHAP Protocol (RFC 1994)

B authenticates A

Server Port A

Switch B

Request Service

Generate random challenge (C*)
Choose Identifier (I*)

I, C

Compute Response
Hash (I | Shared Secret** | C)

Computes own hash
And compares

Success/Failure

*Must change every time
**Typically Password – major improvement is using random number!

FOR A TO AUTHENTICATE B, REPEAT THE PROCESS, USE NEW CHALLENGE

© 2007 Storage Networking Industry Association. All Rights Reserved.

Shared Secret Random # Brute Force Attack Times

Key Size (bits)	Time (1μs/test)	Time (1μs/10^6test)
32	35.8 mins	2.15 msec
40	64.8 days	550 msec
56	1140 years	10.0 hours
64	~500,000 years	107 days
128	5 x 10^{24} years	5 x 10^{18} years

© 2007 Storage Networking Industry Association. All Rights Reserved.

RADIUS Standard (RFC 2865)

Remote **A**uthentication **D**ial **I**n **U**ser **S**ervice

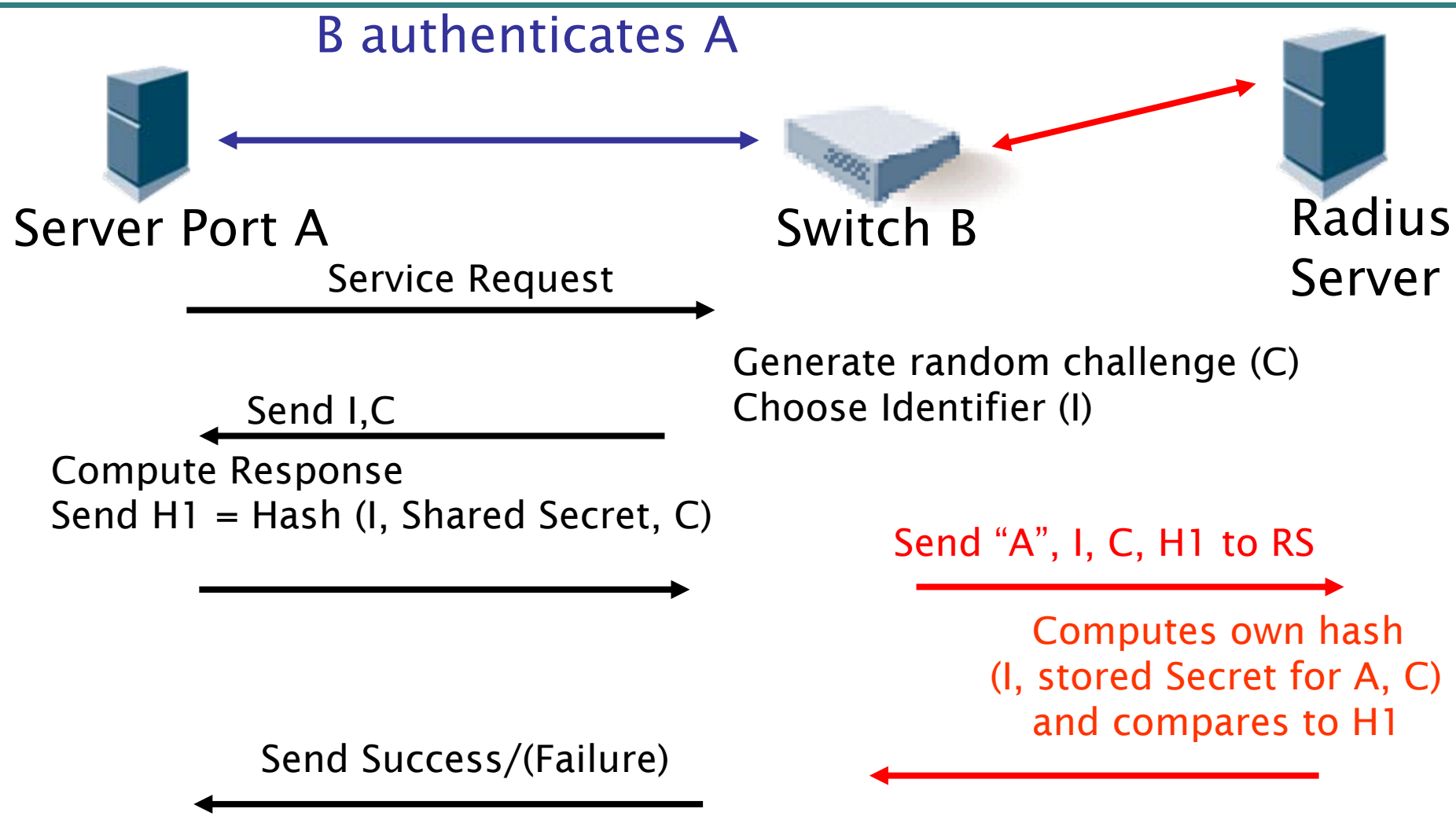
- Client/Server model
- Passwords never sent in clear text
- Messages are authenticated using a client/server shared secret (stops rogue RADIUS server from being used)

How it works:

- A Network Access Server operates as a client of RADIUS Server
- RADIUS Server receives user connection requests, authenticates the user, and returns the accept/reject
- RADIUS Server can act as proxy client to other RADIUS servers or other kinds of authentication servers
- RADIUS provides one-way authentication
  - Need to repeat authentication for the other party

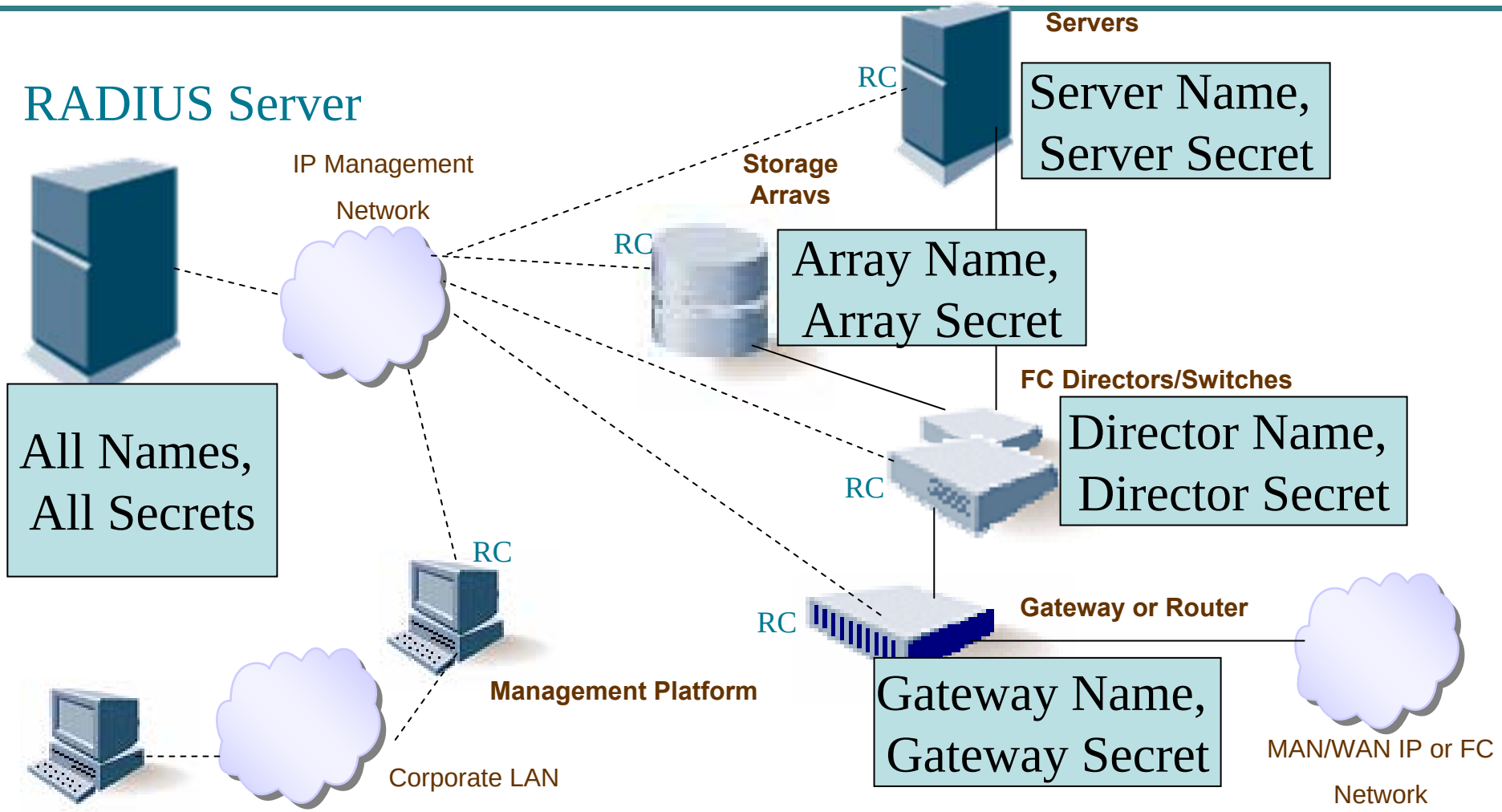
© 2007 Storage Networking Industry Association. All Rights Reserved.

CHAP with RADIUS



© 2007 Storage Networking Industry Association. All Rights Reserved.

Clients and Secrets



Note: It's ok, using RADIUS, to use a single secret to authenticate multiple entities .

© 2007 Storage Networking Industry Association. All Rights Reserved.

CHAP Attack Types and Protection Techniques

Spoofing

- Impersonation, session hijack, masquerade, WWN spoof
  - Prevented by separate secret in each direction

Sniffing

- Replay
  - prevented by random challenge each time
- Offline Dictionary lookup of passwords
  - Prevented by generated random number 128 bit secrets
  - Acceptance of secret from external source required also
- Challenge Reflection attack
  - Checking for same challenge as sent (bi-directional)
  - Or use of non-null DH (in FC-SP which we'll discuss later)

© 2007 Storage Networking Industry Association. All Rights Reserved.

FC-SP Authentication Implementation Checks

SNIA
Storage Networking Industry Association
EDUCATION

Review Notes:

- FC-SP requires DH-CHAP authentication – Available now.
- Doesn't require RADIUS
- RADIUS can be useful to centralize secret administration
- RADIUS requires an IP or IP over FC connection

Ask:

- What authentication infrastructure do I need to use?
- Do I want or need to use RADIUS?
- Does implementation support random number secrets/representations?
- What name rules must be used for setting up RADIUS?
- What secondary RADIUS features are supported?
- What facilities exist to help automate setup?
- Which HBAs/switches/devices support authentication?

Decide if you want to use RADIUS to centralize secrets. Some vendors offer alternatives.

© 2007 Storage Networking Industry Association. All Rights Reserved.

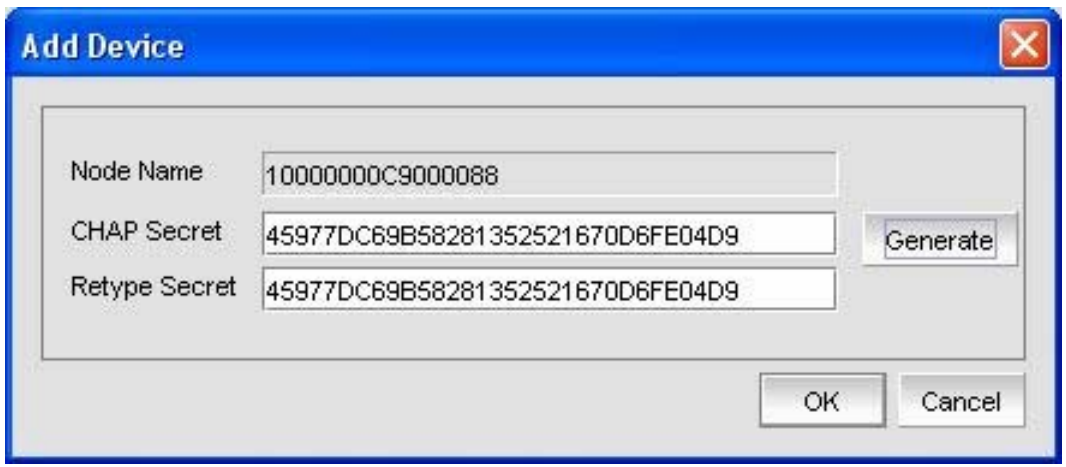
Secrets & Names UI – how to represent?

- 128 bit random secrets
  - Fine, but what does the user interface look like?
  - UI representation not mandated by FC-SP.

  Should it be “hex or decimal representation”?
  Can it be done with “alphanumeric characters”? (would need to be longer)

- WWN’s represented with or without “:” with or without “Ox_” prefix?

One example:



© 2007 Storage Networking Industry Association. All Rights Reserved.

FC-SP Authorization

© 2007 Storage Networking Industry Association. All Rights Reserved.

Access Control Overview

- FC-SP Policies
  - Switch membership, Device Membership, IP Management Lists
    - Fabric Wide Policy
    - Management and enforcement defined
  - Switch Connectivity – per switch access controls
  - Attributes – Fabric wide recognized attributes of switches or devices
  - Stored on Switches
- Enforcement is via definition of a Summary Policy Object
  - Switches exchange list of hash values (SHA-1 or SHA-256) representing fabric policy
  - No merges allowed as done in traditional zoning
- Summarizing Policies – N_Port verification of select policies
  - Especially important for FICON environments

© 2007 Storage Networking Industry Association. All Rights Reserved.

Fabric Wide Policy Implication on Management

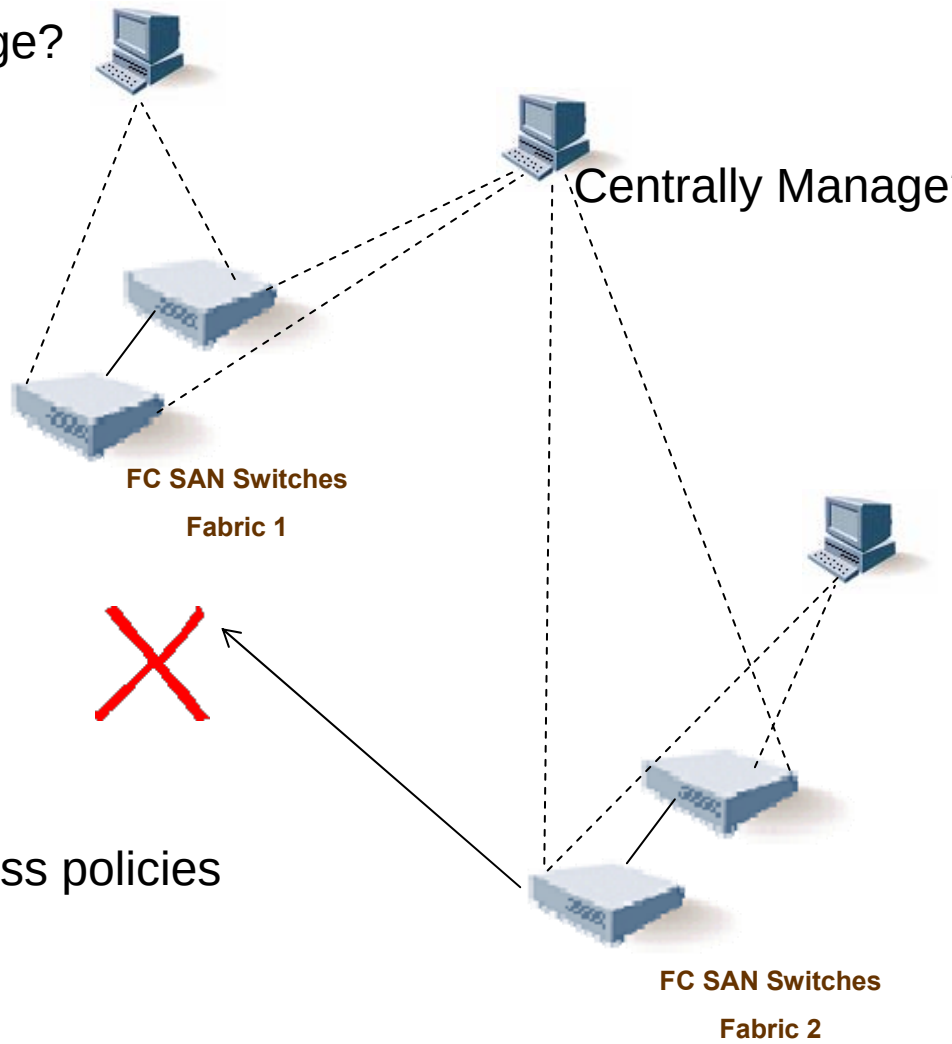
Separately Manage?

Will Fabrics Join?

How it is done:

Checks Hash List Representing Policies Of the Fabric For Exact Match

Centrally Manage?

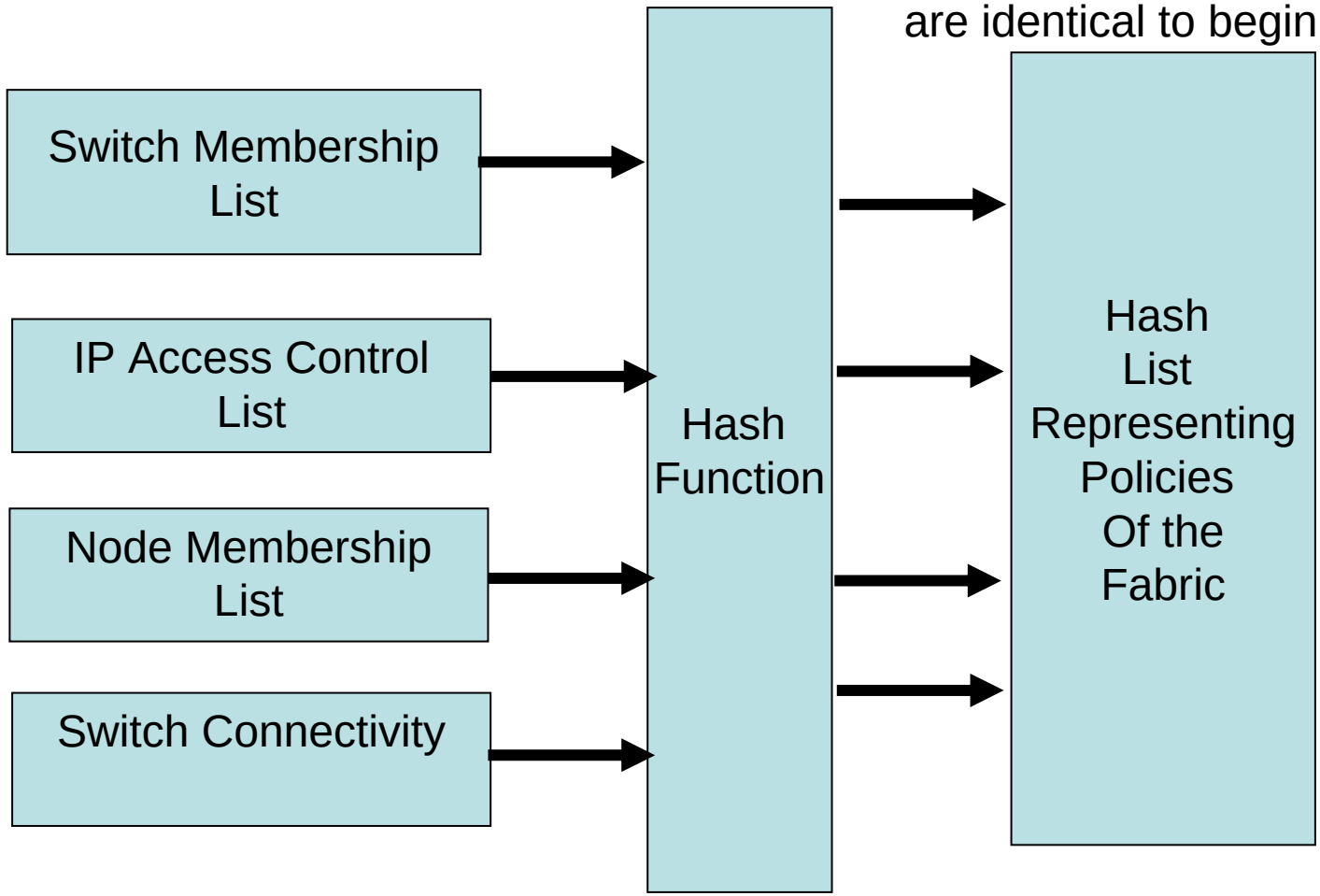


Fabrics won't join unless policies are identical to begin with.

© 2007 Storage Networking Industry Association. All Rights Reserved.

Access Control *a la* FC-SP

Fabrics won't join unless policies are identical to begin with.



© 2007 Storage Networking Industry Association. All Rights Reserved.

FC-SP Zoning Overview

FC-SP Zoning

- Standalone policy approach to zoning that leverages hash checking instead of zone merges of other standards (FC GS & FC SW)
- Improved scalability possible via Switch type definitions

© 2007 Storage Networking Industry Association. All Rights Reserved.

FC-SP Policy Implementation Checks

Review Notes:

- FC-SP Supports mostly Fabric Wide Policy
- Vendors may have interoperable pre-standard alternatives
- Firmware upgrade

Ask:

- Which FC-SP Policies are supported?
  - Switch Membership policies or equivalent should be supported.
  - Annex A of FC-SP offers some possible combinations to consider.
- Do I need to centrally manage multiple fabrics?
- Mainframe? Summarizing Policies should also be supported.
- Do I need to support Basic Zoning due to legacy products?
- What management interface do I use and does it support this?

© 2007 Storage Networking Industry Association. All Rights Reserved.

FC-SP Policy Power Tip

Decide if you want to use FC-SP policies for interoperability. Decide if you want to use FC-SP Zoning for improved scalability and security. Policies slower to be deployed due to transition from pre-standard implementations.

© 2007 Storage Networking Industry Association. All Rights Reserved.

4 Create Risk Domains

Risk domains can be logical or physical

Examples:

- FC Zoning – Consider FC-SP Zoning as it becomes available.
  - Leverages FC-SP Policy, for improved scalability
  - Supports enhanced zoning data structures
- Isolation of management traffic from other traffic
- Use independent fabrics and storage, virtually or physically
- Isolate production from other system classes (QA, development, etc.)

© 2007 Storage Networking Industry Association. All Rights Reserved.

5 Monitor/Control Physical Access

Examples:

- Disable unused ports (e.g. E_Ports, management ports)
- Use port authentication if available (FC-SP defines this for FC)
- Require physical smart cards/badge access, keeping in mind social engineering risks

© 2007 Storage Networking Industry Association. All Rights Reserved.

6 Protect Externalized Data

Examples:

- Encrypt off-site backup tapes of sensitive or regulated data generally. Must encrypt when they leave direct control of the organization.
- Use only secure and bonded shippers if not encrypted
- Data transferred to remote data centers must be encrypted in-flight (FC-SP) when sensitive/regulated

© 2007 Storage Networking Industry Association. All Rights Reserved.

FC-SP Security Association Management

Integrity & Confidentiality (in-flight data) Interfaces
(Security Association Management)

- Switch to Switch
- Device to Switch
- Device to Device

Security Association Management Protocol

- A subset of IKEv2 applied to FC
- Supports ESP_Header frame by frame security
- Also supports a FC message security, applicable to the Name Server and Management Server, called Common Transport (CT)

Hardware? Software? Performance Tradeoffs?

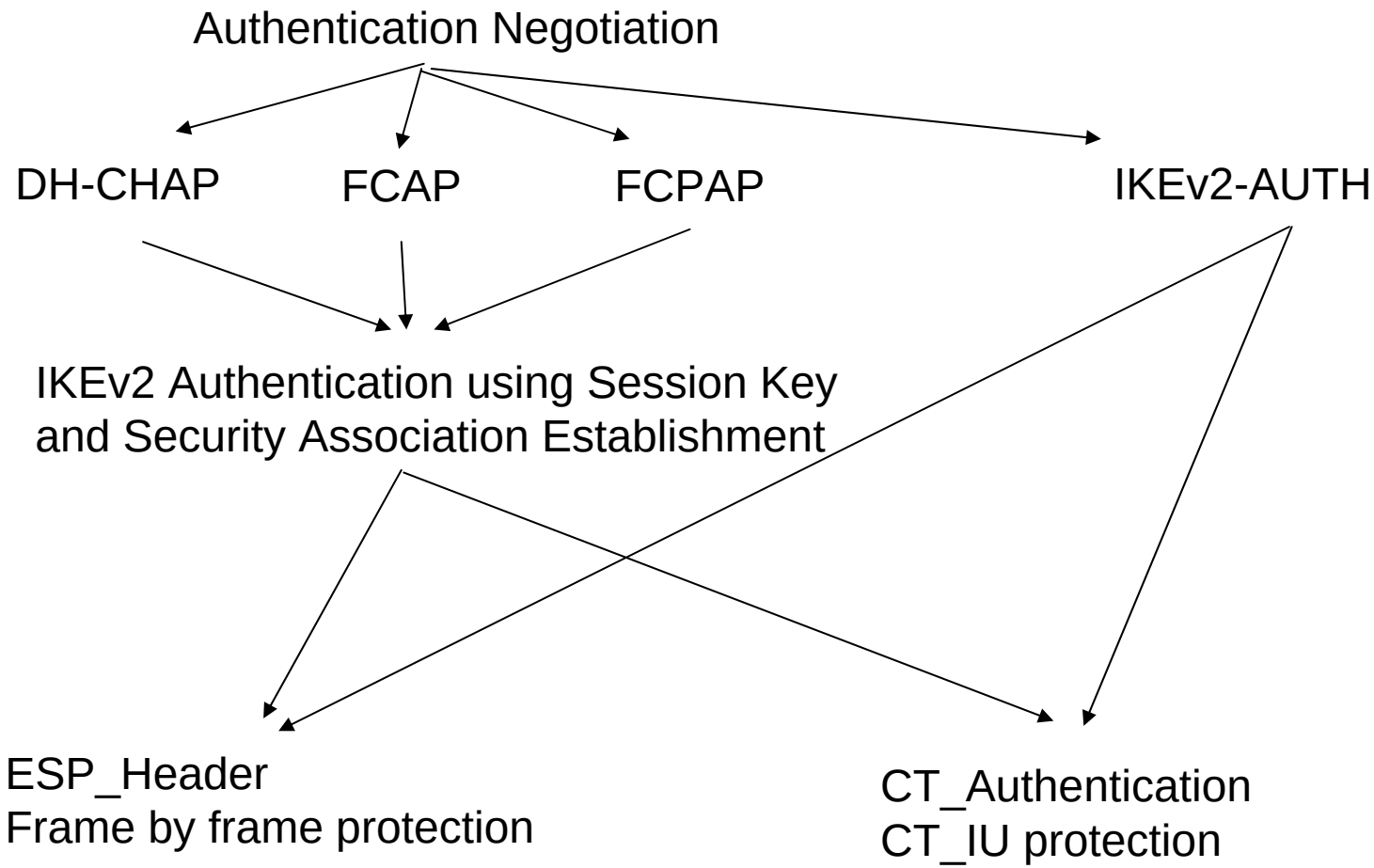
© 2007 Storage Networking Industry Association. All Rights Reserved.

ESP_Header Security Associations

- **Security Associations (SA) stored in individual SADB entries, usually exist in pairs. One for outgoing, one for incoming traffic.**
- **SADB (an SA database) has:**
  - Traffic Selectors (negotiated with IKEv2) and Security Parameters
  - An associated action (bypass, drop, process)
  - SPI (index important to the protocol)
  - Other: Sequence number, sequ. Ctr overflow flag, anti-replay window counter, lifetime
- **Incoming frame**
  - If no ESP_Header received, check SADB to verify if frame matches any Incoming Traffic Selectors.
    - If match and process, discard the frame.
    - If no match, discard frame
  - If ESP_Header, the SPI is used to locate the protecting SA
- **Outgoing frame**
  - Check outgoing traffic selector, no match means send frame unchanged
  - If match and process, apply SA for this traffic selector

© 2007 Storage Networking Industry Association. All Rights Reserved.

Relationship of Authentication to Security Association



© 2007 Storage Networking Industry Association. All Rights Reserved.

In-flight Integrity and Confidentiality

- Support for Common Transport upper level protocol message
  - Common Transport header defined in FC Generic Services (GS) standard
- Support for ESP frame by frame level protection
  - ESP_header defined in FC Framing & Signaling (FS) standard
  - No tunnel mode defined – uses Encapsulation Header

Protocol	Mandatory	Optional
IKE(v2)	Integrity & Encr.	none
ESP_Header	Integrity	Encryption
Common Transport (CT)	Integrity	Encryption

© 2007 Storage Networking Industry Association. All Rights Reserved.

ESP_Header & CT_Authentication Implementation Checks

Review Notes:

- ESP_Header can protect more types of traffic
- CT_Authentication provides low overhead implementation for the FC Management interface

Ask:

- Does implementation support FC Management Interface protection?
- Is there data in-flight that needs to be protected?
- Is there any performance impact? Where is cable end?

Never use confidentiality without integrity (message authentication). Start with Authentication if you need to minimize the configuration. For bulk FC traffic protection, hardware ESP_Header is preferred for performance.

© 2007 Storage Networking Industry Association. All Rights Reserved.

7 Data Security Compliance

Examples:

- Implement Role Based User access control
- Support audit requirements
- Support logging attempted and successful management events, synchronized time of entries
- Destroy data when no longer needed
- Implement appropriate data retention, integrity, confidentiality measures
- Use APPROVED cryptographic algorithms

Approved by whom?

© 2007 Storage Networking Industry Association. All Rights Reserved.

FC-SP Algorithms

© 2007 Storage Networking Industry Association. All Rights Reserved.

Major FC-SP Crypto Algorithms

Protocol	Confidentiality Required	Confidentiality Optional	Integrity Required	Integrity Optional
ESP_Header	NULL AES-GCM	3DES-CBC	GMAC	HMAC-SHA1-96
CT	NULL, AES-CBC	3DES-CBC	HMAC-SHA1-160	HMAC-MD5-128
SA Mgt (FC IKEv2)	AES-CBC	3DES-CBC	HMAC-SHA1-96	HMAC-MD5-96

Required key lengths, required tag lengths, will follow NIST recommendations for GCM.

For CT and SA Management, AES_CBC a 128 bit key is required to support.

In addition, for SA management Pseudo Random Function, the HMAC_SHA1 is required, and the DH 2048 bit group is required.

1536 bit DH group is still required for DH-CHAP authentication using a non-Null DH.

AES = Advanced Encryption Standard **3DES = Triple (3x) Data Encryption Standard**

© 2007 Storage Networking Industry Association. All Rights Reserved.

Algorithm Implementation Checks

Review Notes:

- Applications for Crypto Algorithms
  - Traffic protection
  - Secret storage
  - Authentication/secret protection

For bulk FC traffic protection, hardware support for ESP_Header is preferred for performance.

Ask:

- Are the cryptographic algorithms on your internally approved list?
- Are they on or soon to be on NIST approved list?
  - Encryption, operating modes, hash algorithms

© 2007 Storage Networking Industry Association. All Rights Reserved.

Conclusion – A call to Arms!

FC-SP supports best practices in SAN security

- Authentication, Authorization, Integrity/Confidentiality

Authentication should be used in storage networks.

- FC-SP mandates authentication support for compliance
- Attacks mitigated include spoofing and replay attacks

CHAP is a widely used standard authentication method – a part of storage networking

- DH-CHAP is the FC-SP variation

RADIUS can be used to centralize secret and user and/or device authentication management

- Existing (network) security architectures can be leveraged in a storage network application
- There can be advantages and disadvantages

© 2007 Storage Networking Industry Association. All Rights Reserved.

There's more to come!

FUTURE:

- FC-SP-2 Security will extend Fibre Channel Security even further
- Examples:
  - Additional device policies,
  - Inter Fabric Routing (IFR) security
  - FC IKEv2 clarifications
  - Key distribution methods

© 2007 Storage Networking Industry Association. All Rights Reserved.

How to get involved

- T11.3 FC-SP-2 Work Group
  - Focus: Fibre Channel Security Protocols
  - http://www.t11.org - look under draft standards
- SNIA Security Technical Work Group (TWG)
  - Focus: Requirements, architectures, interfaces, practices, technology, educational materials, and terminology for storage networking.
  - http://www.snia.org/tech_activities/workgroups/security/

© 2007 Storage Networking Industry Association. All Rights Reserved.

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

Larry Hofer, CISSP
Eric Hibbard, CISSP
LeRoy Budnik
David Black
Roger Cummings
Phil Huml
Richard Austin, CISSP

© 2007 Storage Networking Industry Association. All Rights Reserved.

THANK YOU

© 2007 Storage Networking Industry Association. All Rights Reserved.

Bibliography

- Introduction to Storage Security SNIA white paper
  - http://www.snia.org/ssif/documents/Storage-Security-Intro.051014.pdf
- INCITS 426-2007, Fibre Channel Security Protocols, FC-SP
- INCITS 427-2007, Fibre Channel - Generic Services 5, FC-GS-5

© 2007 Storage Networking Industry Association. All Rights Reserved.