Fibre Channel and Security

Live Webcast
August 27, 2019
10:00 AM PT

Today's Presenters

J Metz
Cisco

Nishant Lodha
Marvell

Brandon Hoff
Broadcom

About the FCIA

- The Fibre Channel Industry Association (FCIA) is a mutual benefit, non-profit, international organization of manufacturers, system integrators, developers, vendors, and industry professionals, and end users
  - Promotes the advancement of Fibre Channel technologies and products that conform to the existing and emerging T11 standards
  - Maintains resources and supports activities to ensure multi-vendor interoperability for hardware, interconnection, and protocol solutions
  - Provides promotion and marketing of FC solutions, educational awareness campaigns, hosting public interoperability demonstrations, and fosters technology and standards conformance

https://fibrechannel.org/

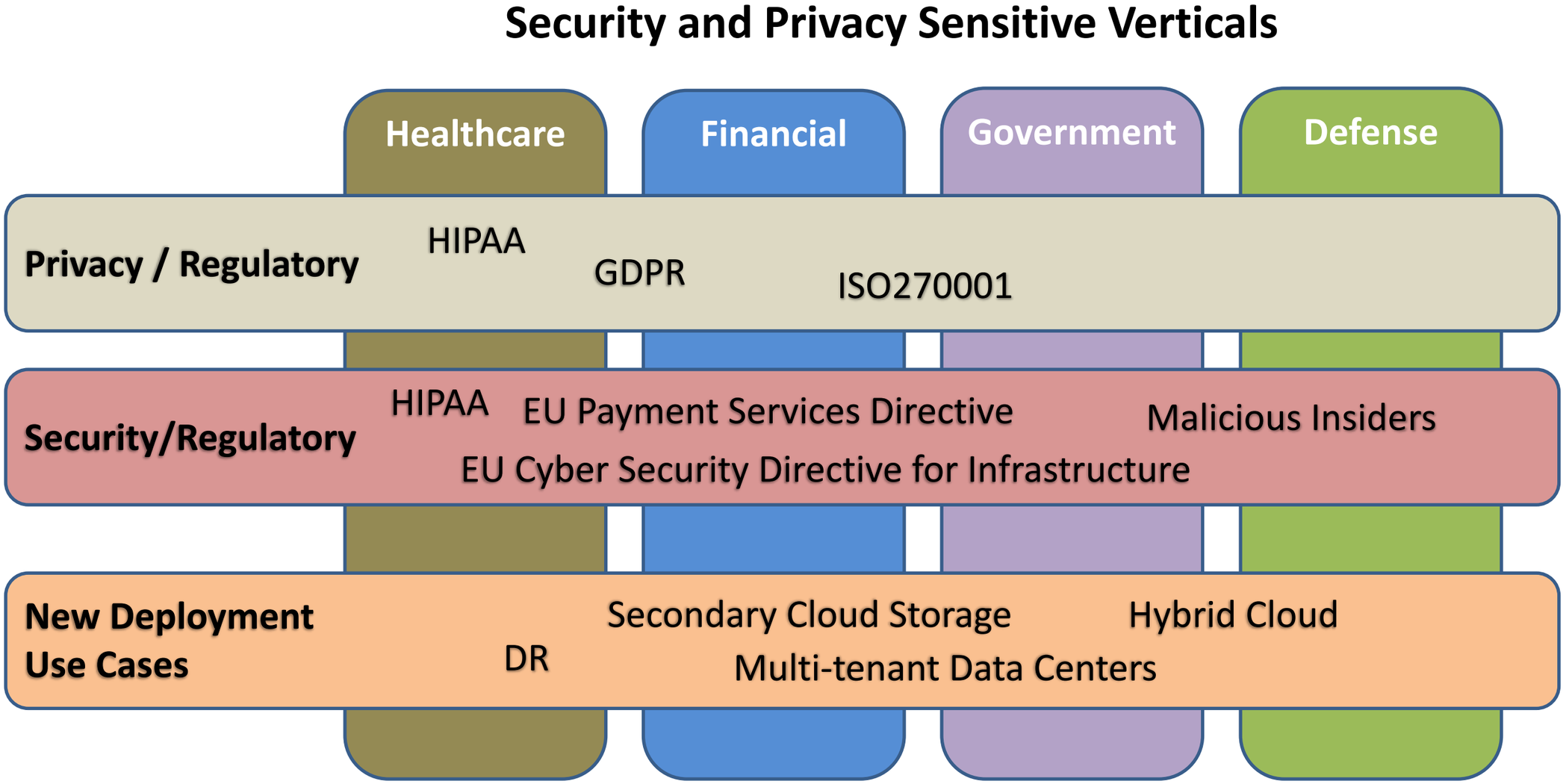
FCIA
FIBRE CHANNEL INDUSTRY ASSOCIATION

FCIA
FIBRE CHANNEL INDUSTRY ASSOCIATION

Key Discussion Points

- Industry trends driving data protection and security
- Existing SAN security mechanisms
- Potential data center security threats
- Fibre Channel authentication and encryption
- Protections provided by Fibre Channel security protocol
- Implementing FC encryption
- Trade offs and caveats

Drivers for Storage Security



Isn't FC Secure Already?

Trusted Storage Interconnect for Decades

Physical Security	• Data Centers are physically secured
Segregation	• Fibre Channel SANs are segregated networks
Partitioning	• FC Zoning ensures fabric partitioning
Masking	• LUN masking restricts access to specific LUNs
Management	• Out-of-Band Management (IP) is secure, OS Controls

Yes, But…

- New Data Center Architectures bring new threats
  - Distributed data centers - Remote replication and DR backups may be accessed by different users over Fabrics that span several sites
  - Multi Tenant data centers – Need to segregate and protect data traversing the same wire
- Increasing scale of FC SANs
  - Networks can be misconfigured
  - Fabric configuration databases are shared (not restricted to zones), have WKAs
- Existing mechanisms may not be enough
  - Switches are the sole entity that grant/deny access
    - Authorization based
  - “Segmentation” tools being used to implement “Security”
    - Soft zoning, LUN Masking

“Appropriate” Security

- **No amount of security is “enough”**
  - And no amount of security will “*guarantee*” protection
- Highly **business**- and **technology**-environment **dependent**
  - Balance between cost of protection technologies and business impact from lost data, credibility and its legal implications
- Users are highly advised to analyze their security needs
  - The FC / FC-NVMe / FICON protocol can’t make that decision for you
  - A good data protection plan should define recovery strategies, RPO, and RTO
- **Nothing in this presentation constitutes warranty or guarantee of any kind!**

Potential DC Storage Security Threats

Sniffing Storage Traffic

Storage Masquerading

Data Corruption

Session Hijacking

Mitigated by Fibre Channel SAN Security

FC-SP-2: What and Why?

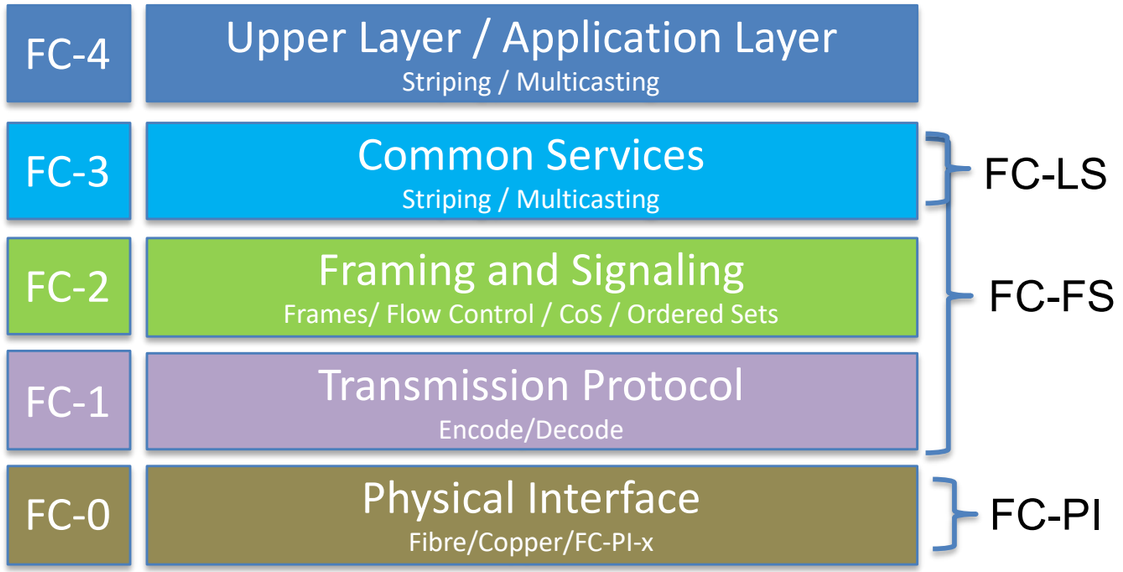
- **Why?** : Need to transition SANs from **Authorization and segmentation** based FC security to **authentication and encryption** based security!

- **What?** FC-SP-2 is a ANSI/INCITS standard (2012) that defines protocols to –
  - **Authenticate** Fibre Channel entities
  - **Setup** session **encryption keys**
  - Negotiate parameters to ensure per **frame integrity and confidentiality**
  - Define and **distribute security policies** over FC

- Designed to protect against several classes of threats

FC-SP-2 and the FC Stack

- FC-SP-2 defines two security protocols that provide security services
  - **ESP_Header** (defined in FC-FS)
  - **CT_Authentication** (defined in FC-GS)
- Choose one:
  - ESP_Header
  - CT_Authentication
- **RFC 4595** specifies FC AUTH protocol for IKEv2 key exchange



Key Terms

- **Entities**: Fibre Channel devices – HBAs, Switches, end points
- **Security Associations (SA)**: Shared security attributes (cryptographic algorithm, encryption key) between communicating entities
- **ESP_Header**: Protocol to provide security for FC data frames
- **CT_Authentication**: Protocol to provide security for FC control frames
- **Re-play protection**: Protocol to detect and reject old/duplicate packets to protect entity from replay attacks
- **IKEv2:** Internet Key Exchange v2 as defined for IPsec. RFC4595 specifies IKEv2 use for FC

Fabric Security Architecture

Components of FC-SP-2 Security Architecture

Authentication Infrastructure

- Secret, certificate, password and pre-shared key based architecture

Authentication

- Protocol to assure identify of communicating entities, negotiation of security requirement and protocol

Security Associations

- Protocol to establish Shared key between communicating entities, Based on IKEv2 (RFC4595)

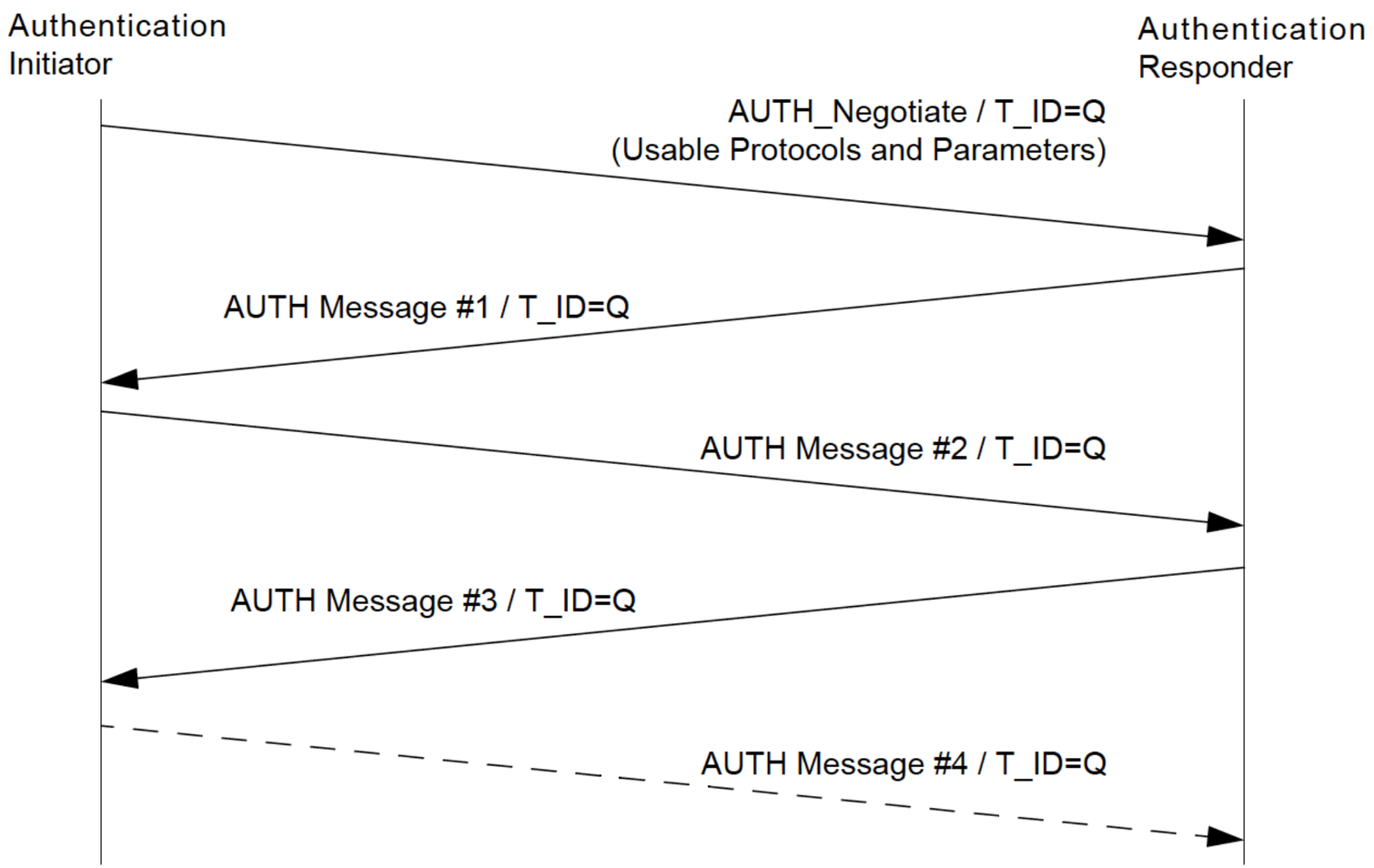
Cryptographic Integrity and Confidentiality

- Frame by frame encryption, replay protection, origin authentication, ESP_Header or CT_Authentication

Authorization

- Fabric policies that control which entities can connect with each other, management access to the fabric

Generic Authentication Transaction



Embedded in the FC-SP-2 Protocol

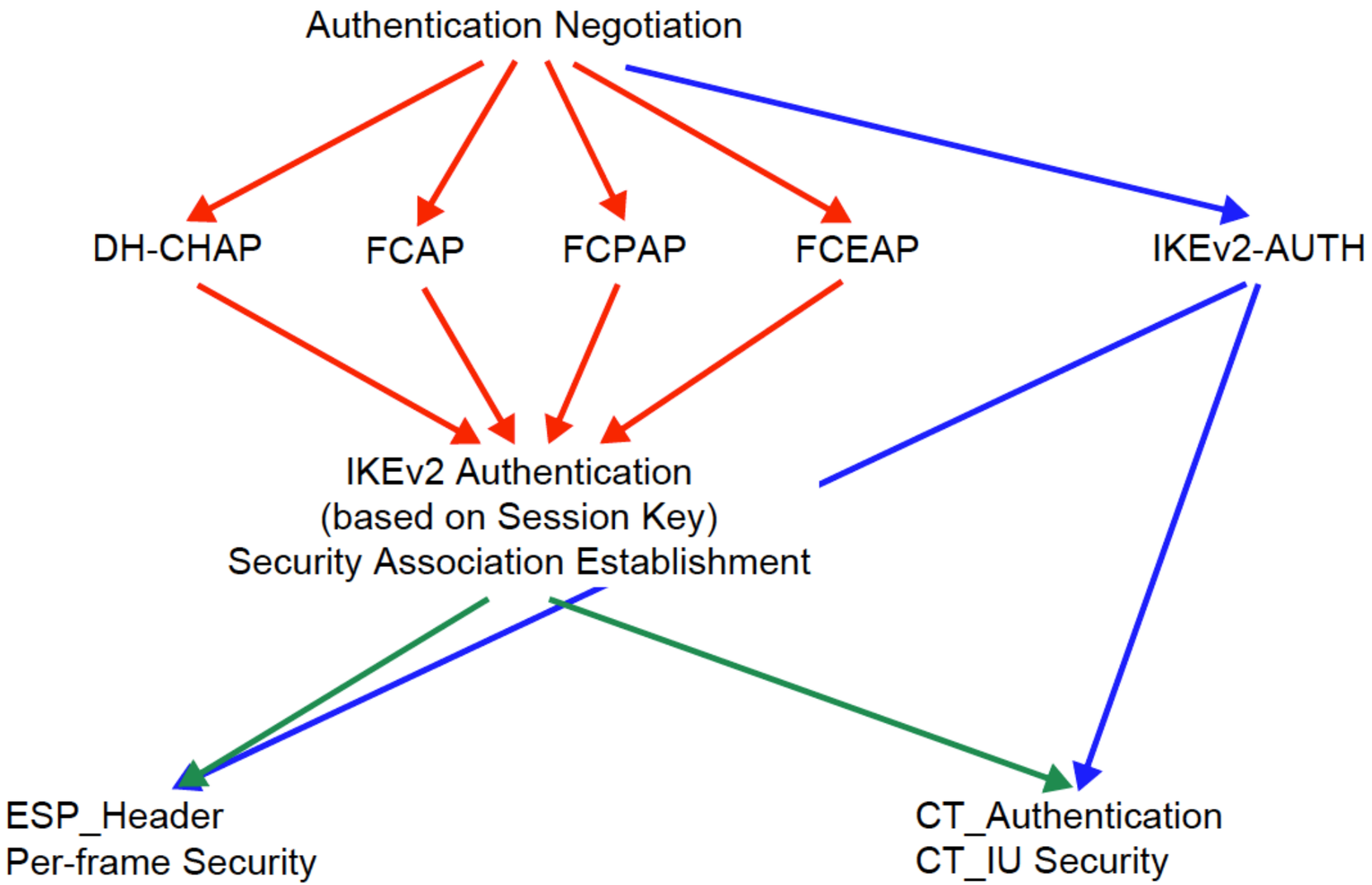
Authentication Details

- Authentication Protocols for the Authentication Infrastructure
  - DH-CHAP
    - Secret-based authentication and key management protocol
  - Fibre Channel Certificate Authentication Protocol (FCAP)
    - x.509 certificate based authentication and key management protocol
  - Fibre Channel Password Authentication Protocol (FCPAP)
    - Password based Authentication and key management protocol that uses the SRP Algorithm (RFC 2945)
  - Fibre Channel Extensible Authentication Protocol (FCEAP)
    - The Extensible Authentication Protocol (EAP) supports multiple authentication methods (RFC 3748)
  - The Security Association Management Protocol (IKEv2-AUTH)
    - When IKEv2 is used for both authentication and the establishment of a SA
- Authentication type
  - Secrets
  - Passwords
  - Certificates

Security Associations

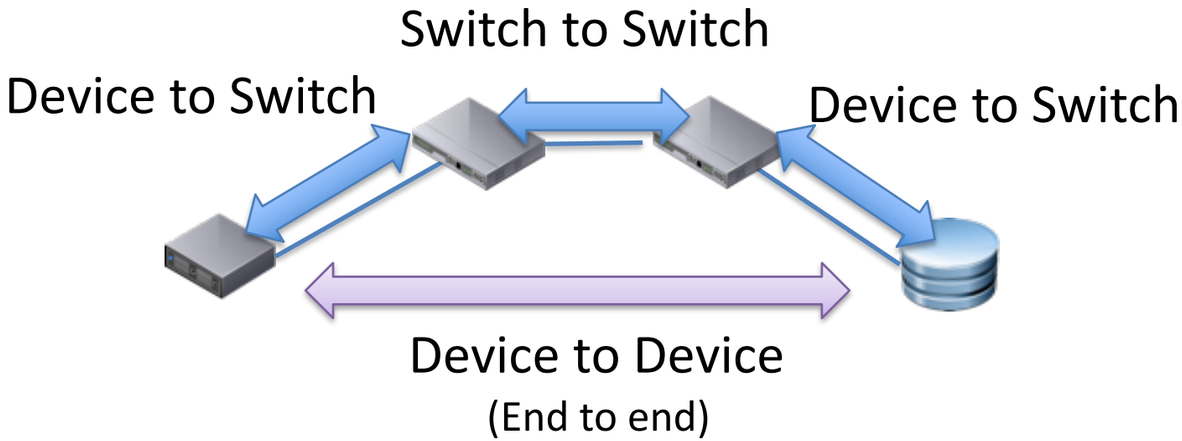
- Subset of the IKEv2 protocol suitable for Fibre Channel establishes Security Associations (SA) between entities
- Traffic selectors specify what needs to be protected by the SA and what the protections are
- Two mechanisms are available to protect traffic
  - ESP_Header for FC-2 Frames to protect data
  - CT_Authentication is used to protect management traffic in the Fabric
- Each SA defines
  - SPI, Sequence Number counter, and parameters for the selected transforms
  - IKE_SA is used for secure SA management functions, Child_SAs secure FC traffic
- Security Association Database (SADB) stores the SAs
  - Includes the SA's SPI, a Sequence Number counter, and parameters for crypto graphic transforms for integrity, confidentiality, mode of operation, and keys

Authentication Protocols and SAs



Authentication Options

- Switch-to-Switch
  - Mutual authentication for a switch to join a Fabric
- Device-to-Switch
  - Mutual authentication for a device to connect to a Fabric
- Device-to-Device
  - Mutual authentication from one end device to another

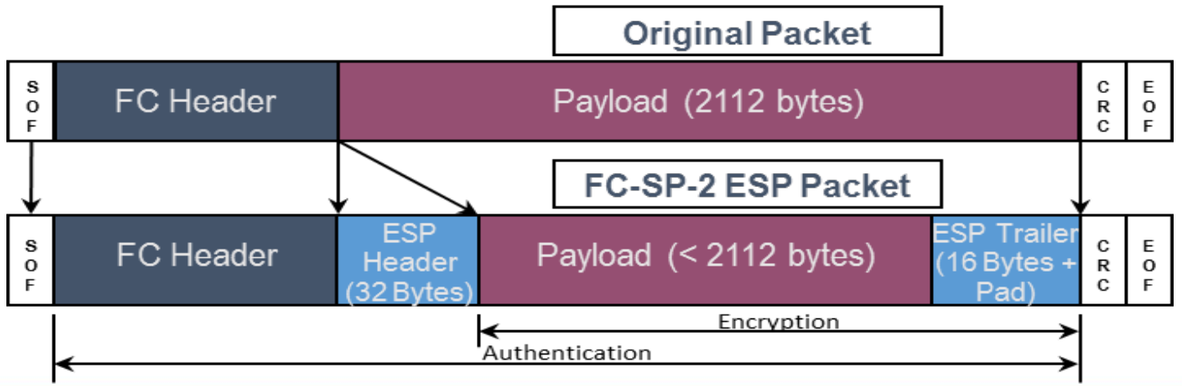


Authorization (Access Control)

- Fabric policies provide basic authorization controls in the form of Access Control Lists
  - Policies that contain Fabric-wide data, distributed to every switch on the Fabric
  - Policies that contain per Switch data, sent to an individual switch
- Policy enforcement occurs when
  - A connection is attempted
  - A management application tries to access the management services of the Fabric
- Policy Check
  - When two switches join they ensure that policy information is the same

FC-SP-2 *ESP_header*

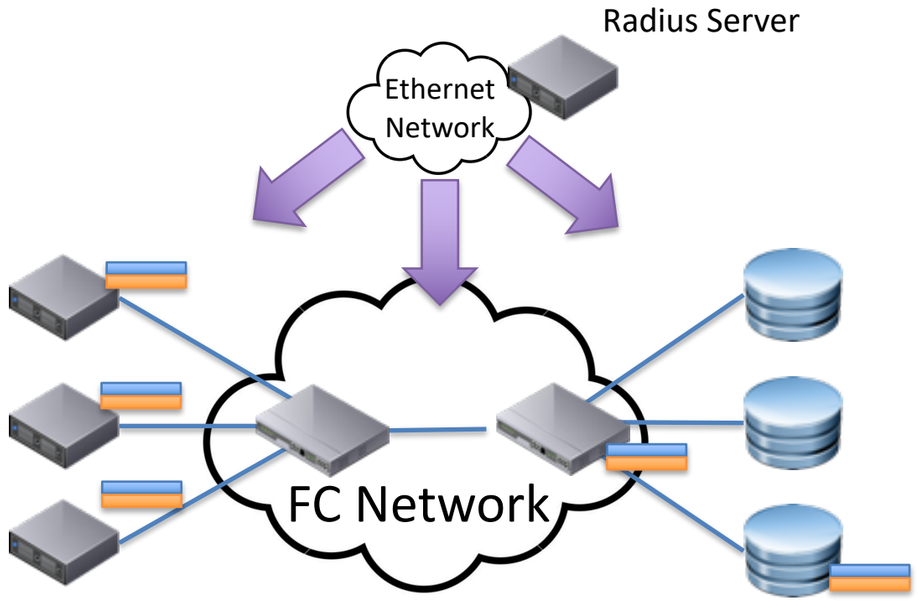
- *ESP_header* (optional) is a layer 2 security protocol that provides
  - Origin authentication
  - Integrity
  - Anti-replay protection
  - Confidentially
- Encapsulating Security Payload (ESP) is defined in RFC 4303
- FC-FS-3 defines optional headers for Fibre Channel, FC-SP defines how to use ESP in Fibre Channel
- Similar protections exist for CT_Authentication



Managing Secrets, Passwords, and Certs

- For mutual authentication, each device needs to know the credentials of
  - The adjacent device
  - End nodes for end-to-end
- Manual configuration becomes difficult
  - 50,000 or more credentials are possible in large environments
- Options for managing credentials
  - RADIUS
  - KMIP
  - Public Certificate Authority
  - Internal Certificate Authority

Sharing the credentials of one device



DH-CHAP Credentials: Name Secret

FC-SP-2

- Benefits
  - Supports in-band authentication and confidential traffic
  - Supports creation of trusted fabrics and FC SAN Infrastructure
  - Protects against certain operator errors and cable misconnections
  - Improved scalability promised in new zoning approach
  - Supports protecting data in-flight
  - Supports checking of network configuration for multi-fabric environments
- Standard conformance
  - FC-SP requires DH-CHAP with NULL for authentication
  - FC-SP-2 requires the support of AUTH-A Compliance Element (Annex A of FC-SP-2)
    - And the ability to re-authenticate

Aspects of Fibre Channel Security

- Physical security for the data center
- Securing management interfaces
- Encryption of data at rest
  - Disk, array, file, database
- Encryption of data in flight
  - DC to DC, End-to-End, hop by hop
- Negative impacts of encryption
- LUN Masking
- Zoning
- NPIV
- Security between data centers
- Proof of encryption
- Secret, password, and certificate management
- Vendor support
- And of course, FC-SP-2

Our Next FCIA Webcast:

Scaling Fibre Channel

Follow us @FCIANews

for date and time

After this Webcast

- Please rate this event – we value your feedback
- We will post a Q&A blog at http://fibrechannel.org/ with answers to the questions we received today
- Follow us on Twitter @FCIAnews for updates on future FCIA webcasts
- Visit our library of FCIA on-demand webcasts at http://fibrechannel.org/webcasts/ to learn about:
  - Fibre Channel Fundamentals
  - FC-NVMe
  - Long Distance Fibre Channel
  - Fibre Channel Speedmap
  - FCIP (Extension): Data Protection and Business Continuity
  - Fibre Channel Performance
  - FICON
  - Fibre Channel Cabling
  - 64GFC
  - FC Zoning Basics

Thank You