Security Standards for Storage Area Networks

Storage Forum
Brussels 2004

Franjo Majstor
Cisco Systems, Inc.

In coordination with the SNIA

© 2003 Cisco Systems, Inc. All rights reserved.

Agenda

- Scope of Storage Security
- Storage Security Architecture
- Securing the Storage Layer
  - Fibre Channel SAN
  - IP Storage (iSCSI+FCIP)
- Securing Storage Management
- What's Next
- References

Scope of Storage Security

- Storage Security focuses on protecting data
  - While in transport (Storage Networking Security)
  - While at rest (Storage Data Security)
- Storage Security should be included in the broader design of a company's security policy
  - Detecting sensitive data
  - Designing and deploying security solution to protect sensitive data
  - Monitoring the efficiency of deployed solutions
  - Reacting to attacks and security breaches improving the design and deployment of security

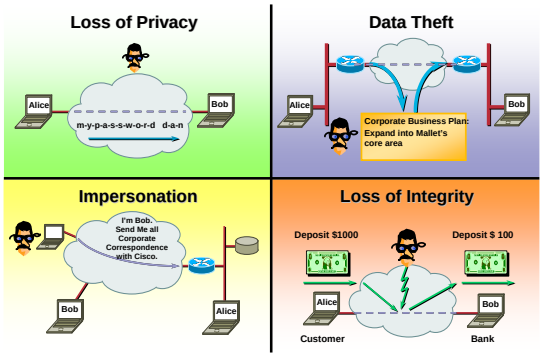
SAN Protocols

- IP storage networking - carrying storage traffic within TCP/IP
- A cost-effective, complementary technology to Fibre Channel
- Extend Fibre Channel SANs to the midrange class of applications and servers
- Uses TCP, a reliable transport for delivery and security
- Two primary protocols:

iSCSI - Internet SCSI - allows storage to be accessed over a TCP/IP network as though it was locally attached

FCIP - Fibre-Channel-over-IP - used to tunnel Fibre Channel frames over TCP/IP connections

Network Vulnerabilities



Network Security

Data Security Assurance

Confidentiality

Benefit:
Ensures data privacy

Shuns:
- Sniffing
- Replay

Integrity

Benefit:
Ensures data is unaltered during transit

Shuns:
- Alteration
- Replay

Authentication

Benefit:
Ensures identity of originator or recipient of data

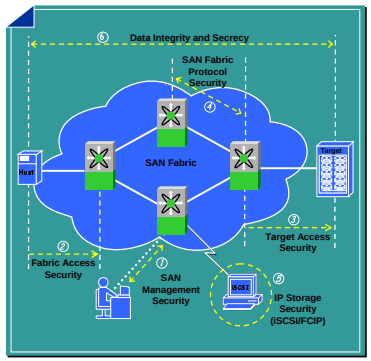
Shuns:
- Impersonation
- Replay

Agenda

- Scope of Storage Security
- Storage Security Architecture
- Securing the Storage Layer
  - Fibre Channel SAN
  - IP Storage (iSCSI+FCIP)
- Securing Storage Management
- What's Next
- References

Storage Security Architecture

- Fabric security augments overall application security
  - Not sufficient on its own - host and disk security also required
- Six key areas of focus
  1. SAN Management Access - secure access to management services
  2. Fabric Access - secure device access to fabric service
  3. Target Access - secure access to targets and LUNs
  4. SAN Protocol - secure switch-to-switch communication protocols
  5. IP Storage Access - secure FCIP and iSCSI services
  6. Data Integrity and Secrecy - Encryption of data both in transit and at rest



Agenda

- Scope of Storage Security
- Storage Security Architecture
- Securing the Storage Layer
  - Fibre Channel SAN
  - IP Storage (iSCSI+FCIP)
- Securing Storage Management
- What's Next
- References

Securing Fibre Channel

Cisco.com

- The Data Center perimeter was considered the boundary of a Fibre Channel network
- Security Services have been limited to
  - Host and disk segregation via Zoning
  - Management protection
- Virtual SANs (VSANs) introduced a new concept
  - Segregation of (virtual) fabrics
- The FC Security Protocol (FC-SP) standard is the next step
  - Device authentication, per message secrecy and integrity protection, policy management

© 2003 Cisco Systems, Inc. All rights reserved.

Zoning: Hosts/Disks Segregation

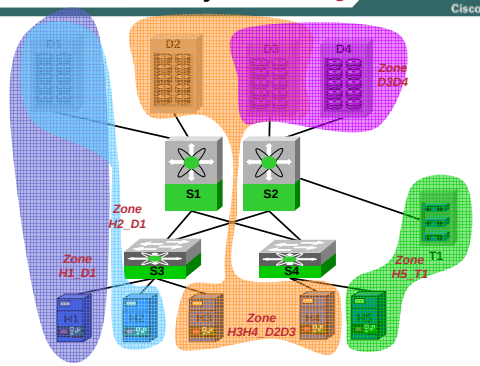
Cisco.com

- Zoning provides segregation between groups of hosts and disks within a SAN
  - Some operating systems attempt to access (write) all discovered disks causing data corruption or loss
- Zoning provides segregation, but authentication is never enforced
  - Circumventing zones through impersonation of a member (identity spoofing) is possible

© 2003 Cisco Systems, Inc. All rights reserved.

Fabric Access Security - FC Zoning

Cisco.com



© 2003 Cisco Systems, Inc. All rights reserved.

Fabric Access Security – FC Zoning - Zones & Zone Members

Cisco.com

- A *Zone* consists of one or more Zone Members
- Zone membership is specified by any of
  - Port WWN of device (specific to a given interface)
  - Node WWN of a device (global to a device)
  - Port WWN of switch port
  - Switch + Interface (port-based)
  - Symbolic Name (iSCSI)
  - One or more zone members can be also be identified by an *Alias Name*

© 2003 Cisco Systems, Inc. All rights reserved.

Hard and Soft Zoning

Cisco.com

- Soft Zoning: the fabric restricts information made available to non-members
  - Software-enforced
  - E.g., names of non-members are not resolved by the name server
  - Restricting only ***VISIBILITY***
- Hard Zoning: the fabric denies access to non-members, even if they attempt to do so
  - Hardware-enforced
  - Restricting ***CONNECTIVITY***

© 2003 Cisco Systems, Inc. All rights reserved.

Securing iSCSI

Cisco.com

- iSCSI relay on in-band authentication
  - CHAP-based (other mechanisms are optional)
  - Supported by a AAA infrastructure

- IPsec tunnels provide, where required per message security
  - Origin authentication, integrity, anti-replay protection, and privacy

© 2003 Cisco Systems, Inc. All rights reserved.

iSCSI In-Band Authentication

Cisco.com

- CHAP-based (Challenge Handshake Authentication Protocol) RFC 1994
  - Challenge/response mechanism
  - Password is never sent over the wire
  - Optionally bi-directional authentication
- AAA service provides centralized password management
  - Authentication
  - Authorization
  - Accounting

© 2003 Cisco Systems, Inc. All rights reserved.

Hosts/Disks Segregation

Cisco.com

- iSCSI-based access control for static iSCSI targets
  - List of iSCSI initiators allowed to access a given target
- Fibre Channel Zoning-based access control
  - Statically mapped iSCSI initiators
    - Regular zone membership rules applies
  - Dynamically mapped iSCSI initiators
    - Zone membership is extended to support iSCSI host's initiators node name

© 2003 Cisco Systems, Inc. All rights reserved.

Enforcing Access Control

Cisco.com

- At iSCSI discovery
  - IPS module returns only the list of iSCSI targets that an iSCSI host can access
- At iSCSI session creation
  - IPS module checks if the iSCSI initiator is in the list of initiators allowed to access the given target
  - A virtual FC N_port is created (if dynamically mapped)
  - The name server resolves the FC_ID of the pWWN accessed by the iSCSI initiator
    - If the virtual N_port and target port are on the same zone the FC_ID is returned and the login is completed, otherwise the login is rejected

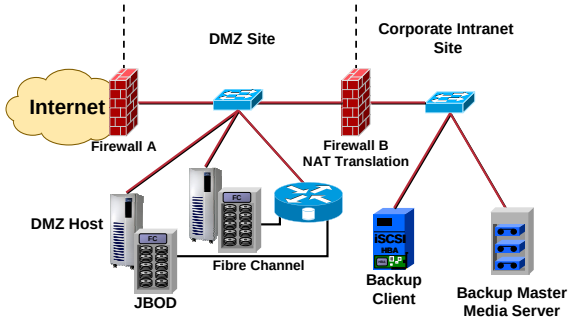
© 2003 Cisco Systems, Inc. All rights reserved.

iSCSI/IP Traffic Segregation

- Storage routers are used to consolidate access to FC disks over IP
- Essential design goals are
  - Segregation of the iSCSI traffic from the general purpose network traffic
  - Prevent unauthorized access to iSCSI targets
- Let's consider the example of backup consolidation for the storage in the De-Militarized Zone (DMZ)

© 2003 Cisco Systems, Inc. All rights reserved.

Example: iSCSI Backup Consolidation



© 2003 Cisco Systems, Inc. All rights reserved.

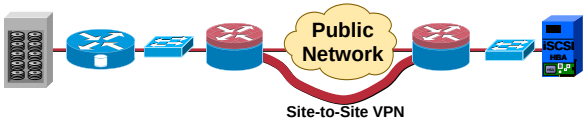
Example: iSCSI Backup Consolidation (Cont.)

- Access Control to iSCSI devices
  - Firewall A prevents iSCSI access from Internet
  - Firewall B
    - Prevents access to internal hosts including backup clients/servers
    - Provides Network Address Translation (NAT)
- iSCSI traffic segregation
  - Use of VLANs in DMZ provide segregation between iSCSI storage traffic and general purpose traffic

© 2003 Cisco Systems, Inc. All rights reserved.

iSCSI per Message Security

- The iSCSI protocol doesn't provide native per message security
  - Relies instead on IPSec to provide per-message origin authentication, integrity, anti-replay protection, and privacy
- When iSCSI traffic is sent over a public or un-trusted network a Virtual Private Network (VPN) shall be deployed
  - E.g., for asynchronous remote backup over the Internet



© 2003 Cisco Systems, Inc. All rights reserved.

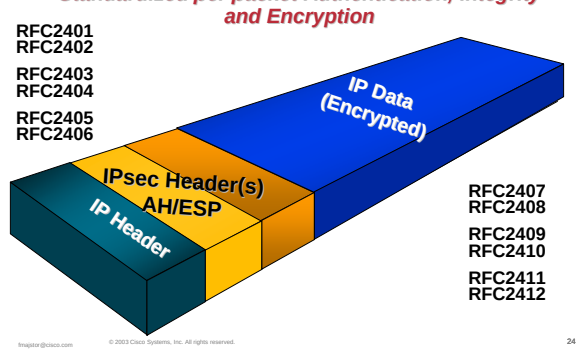
Securing FCIP

- Fibre Channel over IP allows for interconnection of SAN islands via IP networks
- FCIP doesn't provide in-band security mechanisms
- Per message origin authentication, integrity, anti-replay protection, and privacy are provided, where required, by independent IPsec tunnels

© 2003 Cisco Systems, Inc. All rights reserved.

IPsec

Standardized per packet Authentication, Integrity and Encryption



© 2003 Cisco Systems, Inc. All rights reserved.

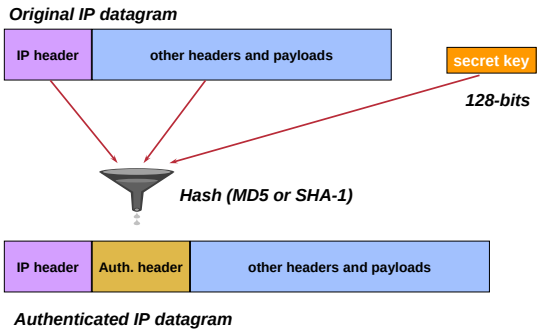
What is IPsec?

Internet Protocol Security

- A set of security protocols and algorithms used to *secure IP data at the network layer*
- IPsec provides data *confidentiality* (*encryption*), *integrity* (*hash*), *authentication* (*signature/certificates*) of IP packets while maintaining the ability to route them through existing IP networks

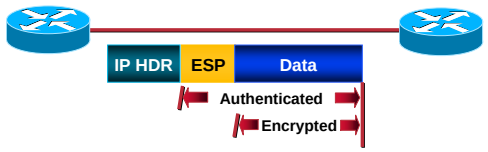
© 2003 Cisco Systems, Inc. All rights reserved.

IPsec Authentication Header (RFC 2402)



© 2003 Cisco Systems, Inc. All rights reserved.

Encapsulating Security Payload (RFC 2406)



- Data integrity & confidentiality
- Data origin authentication
- Anti-replay protection
- Two modes: transport and tunnel
- IP protocol type 50

© 2003 Cisco Systems, Inc. All rights reserved.

IPsec Algorithms and Protocols

Cisco.com

Encryption	Integrity/Authentication	Modes
Data Privacy	Data Exchange Verification	Transport Format
• DES *Data Encryption Standard* • 3DES *Triple Data Encryption Standard* • *AES* *Advanced Encryption Standard*	• IKE - pre-shared *Internet Key Exchange* • IKE RSA / DSS *Rivest, Shamir, Adelman / Digital Signature Standard* • IKE X.509v3 *Digital Certificates* • MD5/ SHA/ AES *Message Digest 5 / Secure Hash Algorithm AES-CBC-MAC*	• AH / ESP *Authentication Header / Encapsulating Security Payload* • Tunnel / Transport *Network to Network / Host to Host*

iSCSI & FCIP:
MUST,SHOULD, MAY

© 2003 Cisco Systems, Inc. All rights reserved.

Agenda

Cisco.com

- Scope of Storage Security
- Storage Security Architecture
- Securing the Storage Layer
  - Fibre Channel SAN
  - IP Storage (iSCSI+FCIP)
- Securing Storage Management
- What's Next
- References

© 2003 Cisco Systems, Inc. All rights reserved.

Securing Storage Management

Cisco.com

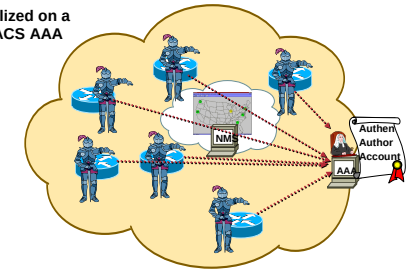
- Storage Management Security includes
  1. Authentication Authorization Accounting (AAA) of management actions
     - RADIUS/TACACS+
     - Role-based management access control
  2. Secure transport of management actions
     - SSH,
     - SNMPv3

© 2003 Cisco Systems, Inc. All rights reserved.

Local vs. Centralized Management Authentication and Authorization

Cisco.com

- The lookup database
  - Can be stored locally on every networking device
  - Can be centralized on a RADIUS/TACACS AAA infrastructure



© 2003 Cisco Systems, Inc. All rights reserved.

Role-Based Management

Cisco.com

	Config	Debug	Exec
Rule1: feature zone	permit		
Rule2: feature fspf	permit		
Rule3:	deny		
Rule4:		deny	
Rule5:			permit

- Role-based management provides fine grain access control for management operations
  - Granting the minimum privilege required to perform a task

© 2003 Cisco Systems, Inc. All rights reserved.

Secure Management Transport: SSH

Cisco.com

- Telnet to a storage device, as well as transfer of configuration files via FTP or TFTP, over an un-trusted network should be avoided
  - Authentication passwords are sent in clear over the network
    - No authentication at all is provided in the case of TFTP
  - An attacker can easily gain access to the device simply sniffing the un-trusted network
- Secure Shell (SSH) or Secure FTP (SFTP) should be used instead

© 2003 Cisco Systems, Inc. All rights reserved.

Secure Shell

Cisco.com

- Secure Shell (SSH) is a client/server public key-based application protocol, used to secure
  - Remote shell connections (SSH)
  - Remote file copy (SFTP)
- Each SSH server is configured with a unique (randomly generated) private/public key pair
  - RSA or DSA key types can be used

© 2003 Cisco Systems, Inc. All rights reserved.

SNMPv3 Security

Cisco.com

- The Simple Network Management Protocol (SNMP) is an application layer protocol for the exchange of management information
  - SNMPv1 and SNMPv2 should be avoided
    - Since they provides a weak form of authentication, based on a simple community string match
- SNMPv3 should be deployed instead, since it provides
  - User based authentication
  - Group (roles)-based access control
  - Per-message origin authentication, integrity, anti-replay protection, and privacy

© 2003 Cisco Systems, Inc. All rights reserved.

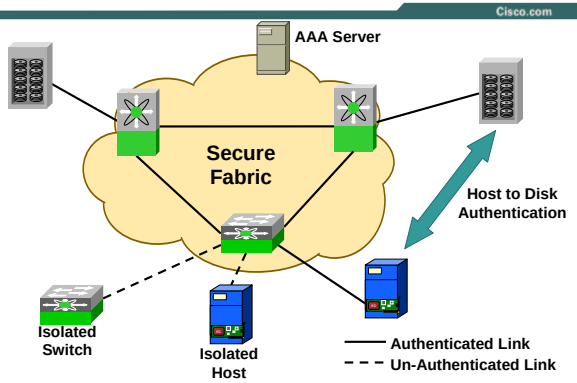
Agenda

Cisco.com

- Scope of Storage Security
- Storage Security Architecture
- Securing the Storage Layer
  - Fibre Channel SAN
  - IP Storage (iSCSI+FCIP)
- Securing Storage Management
- What's Next
- References

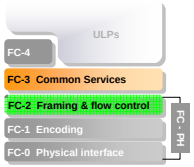
© 2003 Cisco Systems, Inc. All rights reserved.

Secure Fabric



FC-2/3: Common Services

- FC-3 is an "expandable" layer that is designed to support services, such as:
  - Name server
  - Secure key server
  - Management server
  - Time server
- Future services on FC-2
  - Compression
  - Encryption
  - Link multiplexing



SAN Security in Perspective: FC-SP

- FC Security Protocol (FC-SP) working group is defining a security architecture for FC
  - Proposed by INCITS' T11 group (ANSI's International Committee for Information Technology Standards)
- FC-SP goal is to enhance the security properties of FC networks, introducing
  - Authentication between FC entities (node to node, node to switch, and switch to switch)
  - Security Association negotiation and setup between FC entities
  - Per-Frame Security
  - Policy Distribution

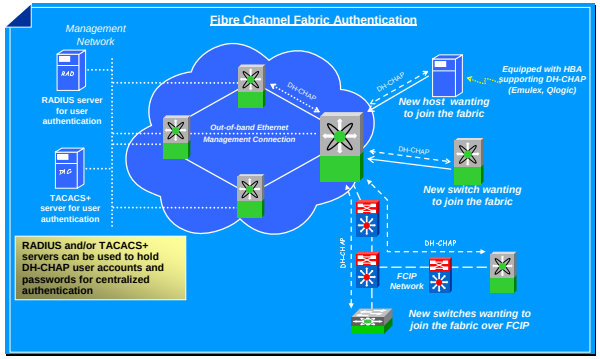
FC-SP Authentication

- Device authentication with FC-SP provides stronger means of ensuring device identity
  - WWNs are easily spoofed
- ANSI T11.3 FC-SP v1.3 draft specification - Security Protocols working group
- A common authentication framework supports different mechanisms
  - Password based (DH-CHAP or SRP)
  - Certificate based (FCAP)

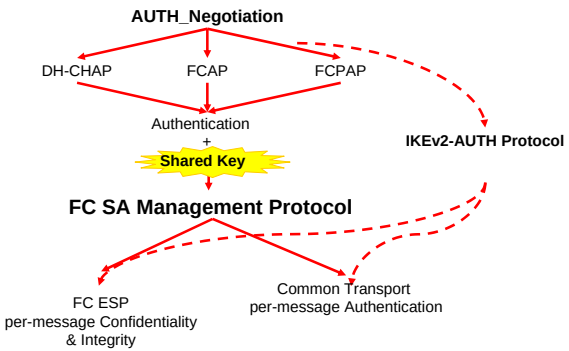
FC-SP Authentication (DH-CHAP)

- The DH-CHAP password-based authentication mechanism enables RADIUS/TACACS AAA based infrastructures
  - Centralized management of switch and node authentication information
- Applications:
  - Secure fabric building
  - Node to fabric authentication
  - Host to disk authentication

Fabric Access Security – FC Security Protocol (FC-SP) DH-CHAP



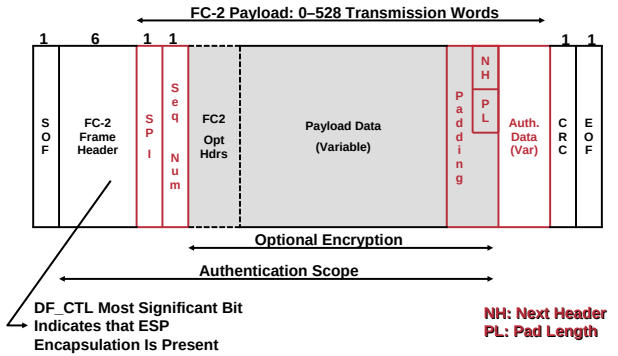
Authentication, Key Exchange, and SA Management



Per-Frame Security and SA Management

- The FC-2 frame format is extended to optionally support *Encapsulation Security Payload (ESP)*
- Each frame can be cryptographically protected
  - Origin authentication, integrity, anti-replay, and secrecy
- The shared key generated by the authentication exchange
  - Is used to establish a Security Association (SA) that provides the required cryptographic parameters

ESP Encapsulated FC-2 Frame



Agenda

- Scope of Storage Security
- Storage Security Architecture
- Securing the Storage Layer
  - Fibre Channel SAN
  - IP Storage (iSCSI+FCIP)
- Securing Storage Management
- What's Next
- References

© 2003 Cisco Systems, Inc. All rights reserved.

References

STANDARDS:

http://www.t10.org (SCSI specs)

http://www.ietf.org/html.charters/ips-charter.html (IETF ips wg)

http://www.ietf.org/internet-drafts/draft-ietf-ips-iscsi-20.txt (iSCSI)

http://www.t11.org (FC-SP specs)

ftp://ftp.t11.org/t11/pub/fc/sp/04-112v0.pdf (FC-SP v1.3)

FORUMS:

http://www.snia.org

http://www.snia.org/ssif

Whitepaper:

ftp://ftp-eng.cisco.com/ltd/mds_security_whitepaper16.pdf

© 2003 Cisco Systems, Inc. All rights reserved.

Cisco Systems

Empowering the Internet Generation℠