FC-SP: An Overview of the Standard for Fibre Channel Security

DISC: Third Intelligent Storage Workshop
University of Minnesota DTC – Minneapolis, MN

Fabio Maino <fmaino@cisco.com>
Cisco Systems, Inc.

Agenda

- Isn’t Fibre Channel already secure?
- FC-SP, Fibre Channel Security Protocols
  - Device Authentication
  - Per Message Security
  - Policy Distribution
Isn’t Fibre Channel Already Secure?

- Data centers are physically secured
- FC Zoning ensure fabric partitioning
- Out-of-Band Management (e.g. SNMPv3) is secure

Yes, but…

- Data Centers are growing
  Remote replication over FCIP, DWDM/CWDM, …
- Networks are misconfigured
- Fabric Configuration Databases are shared
- Device impersonation is trivial
- Management is done in-band
Agenda

• Isn’t Fibre Channel already secure?
• FC-SP, Fibre Channel Security Protocols
  Device Authentication
  Per Message Security
  Policy Distribution

FC-SP: Fibre Channel Security Protocol

• INCITS ANSI T11.3 grouped the Security Solutions for the Fibre Channel Architecture in FC-SP
  Started as a study group in mid 2001
  Is going through a first round of letter ballot comment resolutions
  Standard will likely closed by the fall 2005
• Parts of the standard are already implemented and interoperable
FC-SP: Security Architecture

- Device Authentication (sw2sw, sw2host, host2host)
- Per-message data origin authentication, integrity protection, anti-replay, and secrecy
- Fabric Management Policy Set (as a generalization of the zoning policy set)
  provides role management within a fabric, and access control to fabric membership, and fabric management

Device Authentication

- Switch to switch, switch to host, and host to host authentication
  As an optional extension of the LOGI procedure
- Enables secure fabric building, edge authentication, and end-to-end authentication
- A shared key is derived as a by-product of authentication
Secure Fabric Building

Fibre Channel Fabric Authentication

Authentication Mechanisms

- **DHCHAP**: password based, mandatory
- **FCAP**: certificate based, optional
- **FCPAP**: password/verifier based, optional
  - SRP, Secure Remote Password
- Transported over FC AUTH Protocol
- All mechanisms provide
  - bi-directional authentication
  - Key exchange to enable Security Association Negotiation
**DHCHAP**

- Challenge Authentication Protocol (CHAP), augmented with a Diffie-Hellman exchange
  - Better resistance to off-line dictionary attacks
  - Generates a Shared Key as a by-product of authentication
- Can be integrated with a back-end AAA Infrastructure (RADIUS)
  - Enables effective centralized management of device password

**DH-CHAP and RADIUS**

![Diagram showing DH-CHAP and RADIUS integration in a network context](image)
Agenda

- Isn’t Fibre Channel already secure?
- FC-SP, Fibre Channel Security Protocols
  - Device Authentication
  - Per Message Security
  - Policy Distribution

Per-Message Security

- FC frame formats have been extended to provide per-message security
  - ESP_Header: protection is afforded at the FC-2 Layer, the FC “network layer” that transports the bulk of FC traffic (including SCSI commands and data)
  - CT_Authentication: protection is afforded for Common Transport Information Units (CT_IUs), a protocol used for many control protocols in FC
- Security Services provided are:
  - Data origin authentication
  - Integrity protection
  - Replay protection
  - Confidentiality
ESP_Header (FCsec)

- It's the FC equivalent of IPsec
  - Protects frames at the FC-2 layer
  - Based on IETF's ESP (Encapsulated Security Payload) Protocol
- AES GCM (Galois Counter Mode) likely to be mandatory to implement
  - High speed/highly efficient combined mode (Confidentiality+Integrity)

FC-ESP: Frame Format

<table>
<thead>
<tr>
<th>SOF</th>
<th>DF_CTL bit-22 indicates that the ESP header is present</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Payload Data (variable)</td>
</tr>
<tr>
<td></td>
<td>Auth. Data (var)</td>
</tr>
<tr>
<td></td>
<td>NH: Next Header</td>
</tr>
<tr>
<td></td>
<td>PL: Pad Length</td>
</tr>
<tr>
<td></td>
<td>Opt. Encryption Scope</td>
</tr>
<tr>
<td></td>
<td>Authentication Scope</td>
</tr>
</tbody>
</table>

42 44 4 1 6
CT_Authentication

- Protects Common Transport Information Units (CT_IU)
  - Used for FC control protocols
- A “Traditional” encryption + Integrity mode is likely to be mandatory (i.e. AES CBC + XCBC)
- Typically implemented in SW to protect control traffic only

FC Security Association Negotiation Protocol

- A subset of IKEv2 (over FC AUTH protocol) is used to negotiate
  - ESP_Header SAs, or
  - CT_Authentication SAs
- The shared key resulting from the authentication exchange is used to authenticate the IKEv2 exchange
- It’s also possible to use a static pre-shared key, without going through authentication
Authentication + SA Negotiation

AUTH_Negotiation

DH-CHAP  FCAP  FCPAP

Authentication + Shared Key

Security Association Establishment (IKEv2)

FC ESP per-message Security

Common Transport Security

Secure Fabric

AAA Server

Secure Fabric

Host to Disk Authentication and Encryption

Authenticated Links

Un-Authenticated Links

Isolated Switch

Isolated Host

Host to Disk Authentication and Encryption

Authenticated Links

Un-Authenticated Links

Copyright © 2005, Cisco Systems, Inc. All rights reserved. Printed in USA.
Agenda

• Isn’t Fibre Channel already secure?
• FC-SP, Fibre Channel Security Protocols
  Device Authentication
  Per Message Security
  Policy Distribution

FC-SP Policy Management

• A framework for policy management of a FC fabric
• Generalization and extension of the zone set management
• A generic Policy Set defines the policies enforced by the fabric
  Fabric Wide Policies
  Switch-related Policies
Policy Objects

- **Policy Summary**: is an ordered list of pointers to policy objects
- **Switch Membership List**: fabric-wide list of switches member of a fabric
- **Device Membership List**: fabric wide list of devices (hosts/disks) member of a fabric
- **IP Management List**: fabric wide list of IP addresses enabled for out-of-band management
- **Switch Connectivity**: per-switch topology policy
- **Attribute**: fabric wide extensible attribute to be associated with members of a fabric
Scalability

- Scalability for policy information management is obtained specializing the behavior of the switches:
  - **Autonomous Switches**, that maintain the Fabric-wide Policy Objects, their own Switch Connectivity Object, and a full copy of the FC-SP Zoning Database;
  - **Client Switches**, that maintain the Fabric-wide Policy Objects, their own Switch Connectivity Object, and a subset of the FC-SP Active Zone Set; and
  - **Server Switches**, that maintain the Fabric-wide Policy Objects, all the Switch Connectivity Objects, and a full copy of the FC-SP Zoning Database.

References
