Storage Security

Presenter: Himanshu Dwivedi

BlackHat 2003

Agenda

- Introduction
- Fibre Channel Overview
- Attacks on Fibre Channel SANs
- Conclusion

Introduction

- Overview
  - What are SANs?
  - What is Storage Security?
  - Why Storage Security?
  - Why do I Care?
  - Importance of SAN Security

Introduction

- What are SANs?
  - Storage Area Networks (SANs) are entities in a network architecture that provide large amount of access to storage.
    - Most SANs use Fibre Channel
    - SANs are tasked with providing large amounts of storage to hundreds of diskless servers
- What is Storage Security?
  - Storage security is the act of protecting the **data** that resides in the SAN from unauthorized access

Introduction

- Why Storage Security?
  - Many storage administrators assume that security is an IP (Internet Protocol) issue, not an Fibre Channel issue
    - There is no question that IP security issues are more susceptible to attack than Fibre Channel networks
  - When addressing entities such as intellectual property, propriety information, and trade secrets, all aspects of data security must be addressed
    - Using invalid or unconfirmed assumptions, especially ones that pertain to security by obscurity, are inappropriate in order to secure highly sensitive data

Introduction

- Why Storage Security (Con't)
  - On average, most organizations spend more resources to **secure** their web servers, which may hold static marketing data, than protecting intellectual property held in their own SAN
- Connectivity
  - SANs often bridge several security zones (DMZ, Internal, Application, and Database networks) that are segmented on the IP network.
    - Without some type of segmentation on the Fibre Channel network, the segmentation on the IP network could be negated, allowing a single compromised server to open the gateway to the SAN

Introduction

- Why do I care?

Data

Introduction

- Why do I care? (con't)
  - Who cares about root or administrator access when data, and lots of it, can be compromised?
  - If an unauthorized user gets access to data, such as source code, via the SAN, they won't care about defacing a web page
  - Regulatory specifications, such as HIPAA and SEC Rule 17a-4, may hold organizations liable

Introduction

- Importance of SAN Security
  - What we see: Organizations dedicating large budgets to SANs
    - SANs are becoming the core repository of data
      - Storing intellectual property, proprietary data, etc.
  - What we know: Attacks rarely change, they get modified
    - Core security aspects have been ignored
      - Authentication, Authorization, and Encryption
    - Old IP vulnerabilities mirror existing Fibre Channel issues
  - What vendors know:
    - "How do you secure a Storage Area Network in today's environment? Quite frankly, there is no security. And that is why people don't talk about it."
      - Wayne Lam, Vice-President of FalconStor Software

Introduction

Security Measures	SAN Practices
-> Authentication	= Poor
-> Authorization	= Average
-> Encryption	= None
RESULTS:	= Not Good

Fibre Channel Overview

Fibre Channel Overview

- What is Fibre Channel
  - A technology used to transfer data between two nodes at speeds up to 2Gbps
  - Replaces SCSI
  - Physical medium can be optical fibre, coaxial cable, and twisted pair
  - The amount of overhead required to transmit a Fibre Channel frame remains constant regardless of frame size.
    - This makes Fibre Channel very efficient for high volume data transfers

Fibre Channel Overview

- Fibre Channel Frames
  - It may be fast, but its ALL in the clear
    - Fabric name/allocation
    - Domain Identification
    - Broadcast information
    - Switch information
    - Management information
    - SES usage
    - FC-SNMP community strings
    - Name server information
    - Limited credit information

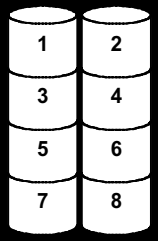
Fibre Channel Overview

- Terms
  - HBA: Host Bus Adapter (Network Interface Card)
  - LUNs: Logical Unit Numbers (A logical array of storage units. One storage node can be divided into multiple LUNs)
  - WWN: World Wide Name (MAC address for HBAs)
  - NS: Name Server (A table on a fibre channel switch that maps each node's 64-bit WWN to their 24-bit fabric address)
  - Zoning: Logical segmentation FC nodes connected on a FC switch
  - N_port: A Node Port, usually client nodes
  - F_port: A Fabric Port, usually switch ports
  - FLOGI: Fabric Login, the process of logging into the fabric

Fibre Channel Overview

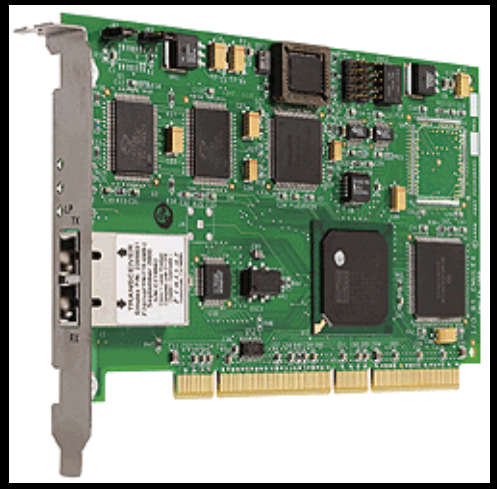
- Terms with Pictures

Storage Controller



2 Disks, 8 LUNs

WWN: 10:00:00:00:CB:24:72:2C



HBA

Name Server

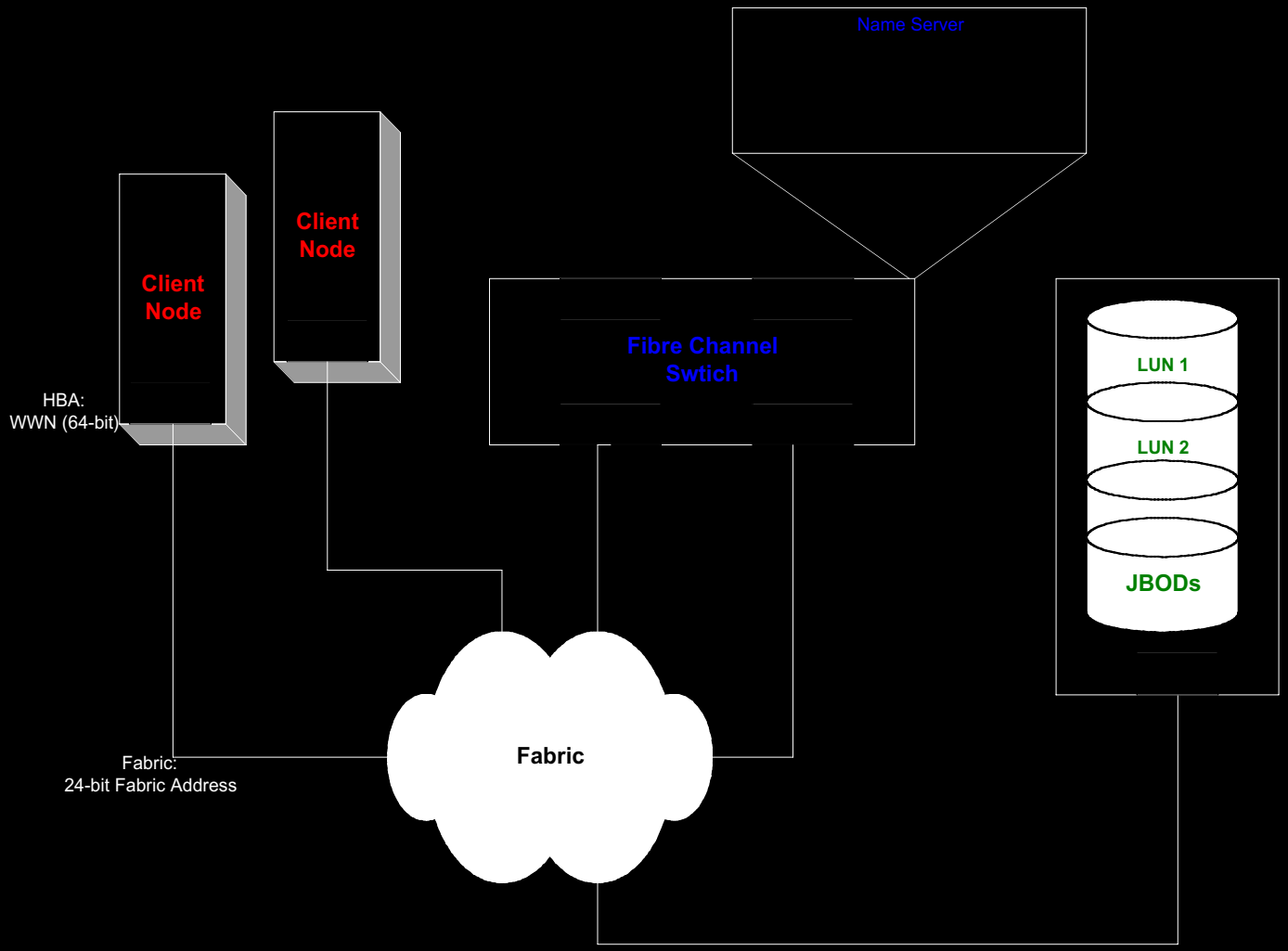
24-bit Fabric Address == 64-bit WWN

Fibre Channel Switch

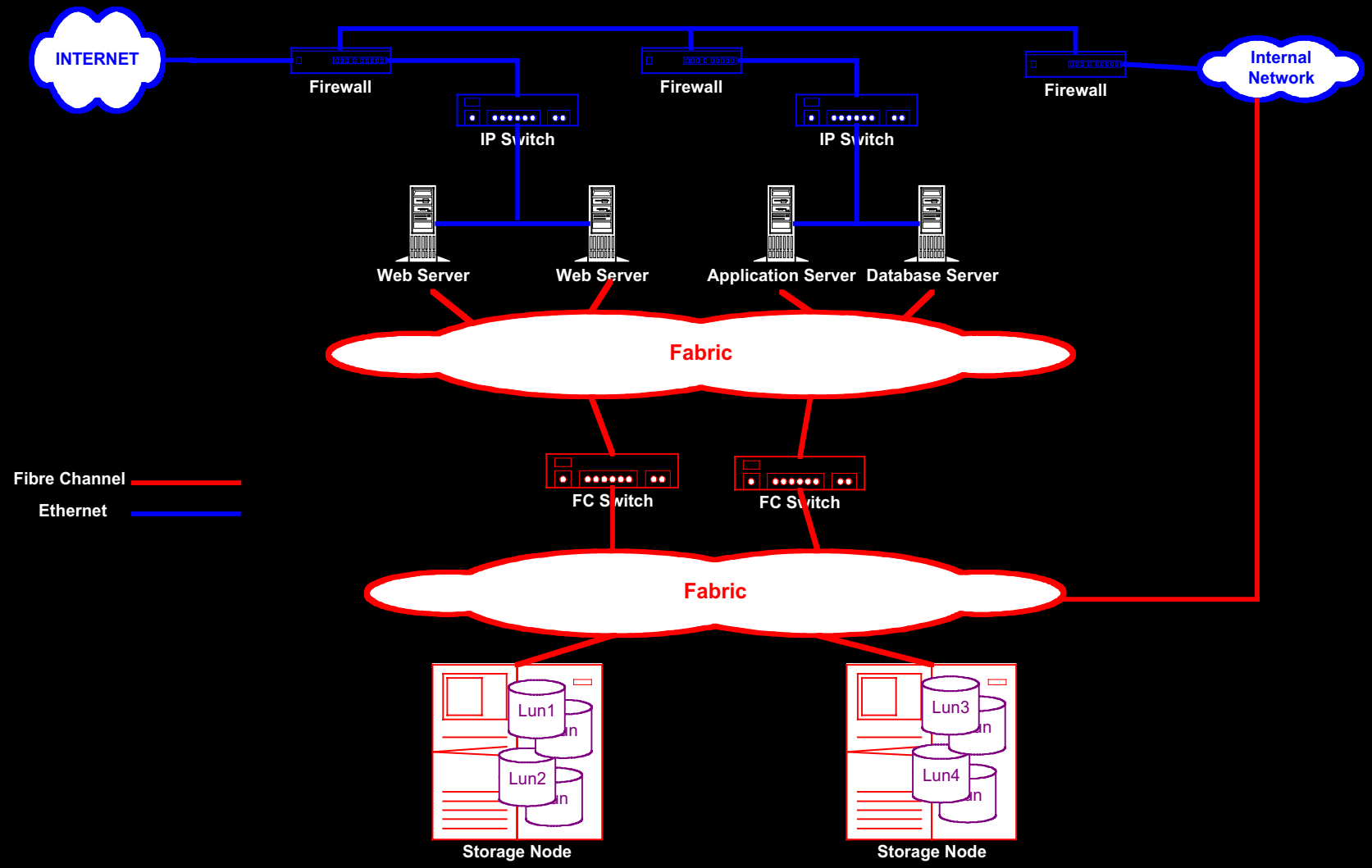
Fibre Channel Overview

- The Fabric
  - SAN Fabrics are switched topologies that are used to connect the different nodes on the network
- Each node in a FC SANs has
  - A 24-bit address administered by the fabric
    - Received when the client node logs into the fabric (FLOGI)
    - Used for routing, among other things, within the fabric
  - A 64-bit WWN determined by the HBA
    - Given by the manufacturer, modifiable
  - A port type association with its HBA, including F_port or N_port
  - An N_Port ID (8 bits) is received after login (FLOGI) from the adjacent switch in order to register the client node

Fibre Channel Overview – Example 1



Fibre Channel Overview – Example 2

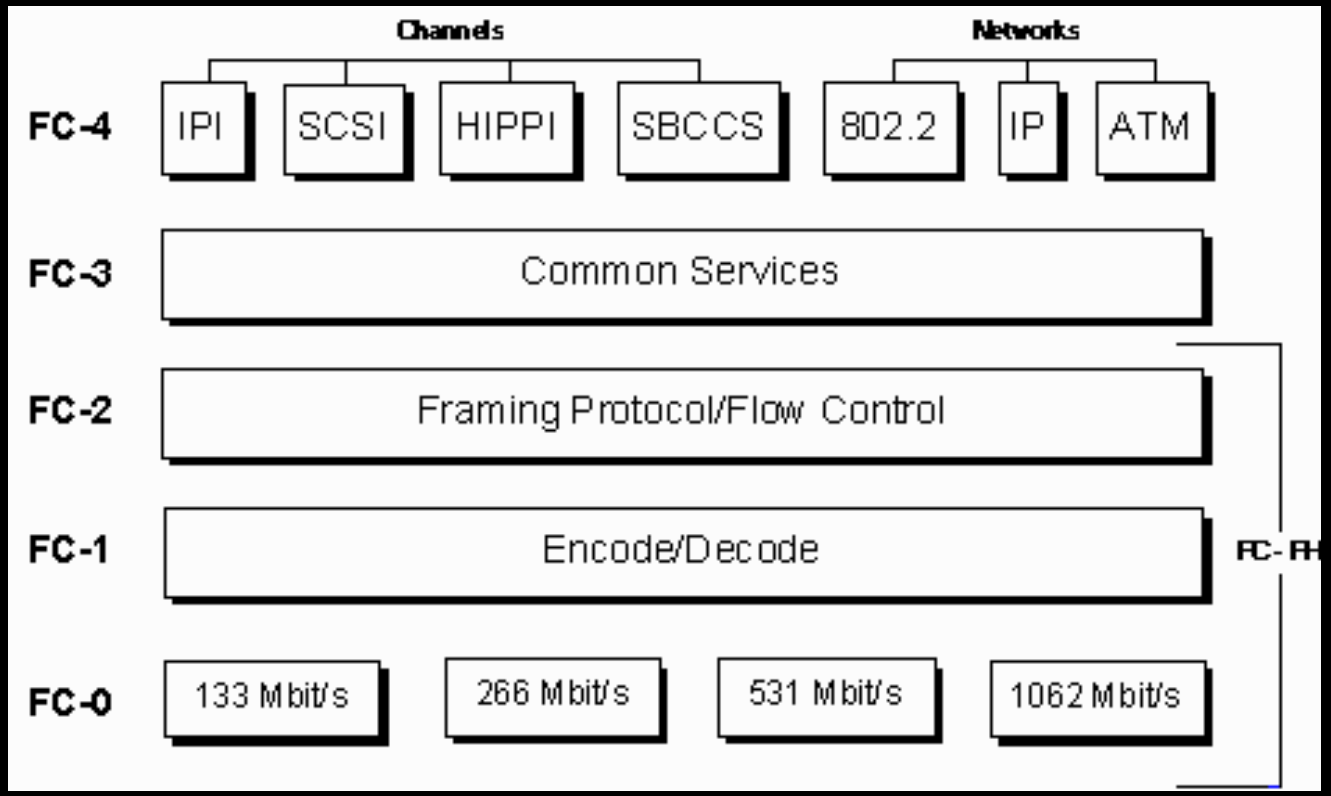


Fibre Channel Overview

- Fibre Channel Frame
  - Frames are composed of:
    - a starting delimiter (SOF)
    - a header
    - the payload
    - the Cyclic Redundancy Check (CRC)
    - The ending delimiter (EOF).

Fibre Channel Overview

- Structure of Fibre Channel Frames



Fibre Channel Overview

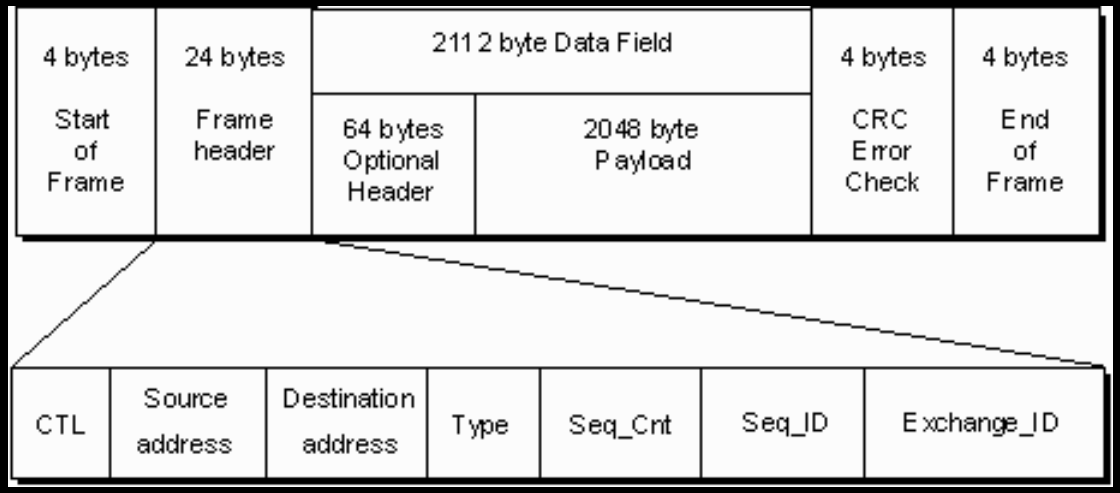
- Fibre Channel (FC) – Layer 2
  - Layer 2 in the FC frames contains several weaknesses
  - These weakness are associated with the lack of
    - Authentication – No authentication in the fabric
    - Authorization – Authorization parameters are weak, at best
    - Encryption – No encryption currently exist

Fibre Channel Overview

- FC-2
  - FC-2 is similar to what other protocols define as a Media Access Control (MAC) layer, which is typically the lower half of the Data Link layer.
    - Frame format
    - Sequence management
    - Exchange management
    - Flow Control
    - Classes of Service
    - Login/Logout
    - Topologies
    - Segmentation and Reassembly

Fibre Channel Overview

- FC-2



- Layer 2 in FC frames contain several of the security weaknesses identified earlier in IPv4

Fibre Channel Overview

- FC Frame – Layer 2
  - The 24-byte header contains information about the frame, including:
    - The source ID - S_ID
    - The destination ID - D_ID
    - Routing information
    - The type of data contained in the payload
    - Sequence/exchange management information
  - The payload contains the actual data to be transmitted, and may be 0-2112 bytes in length.

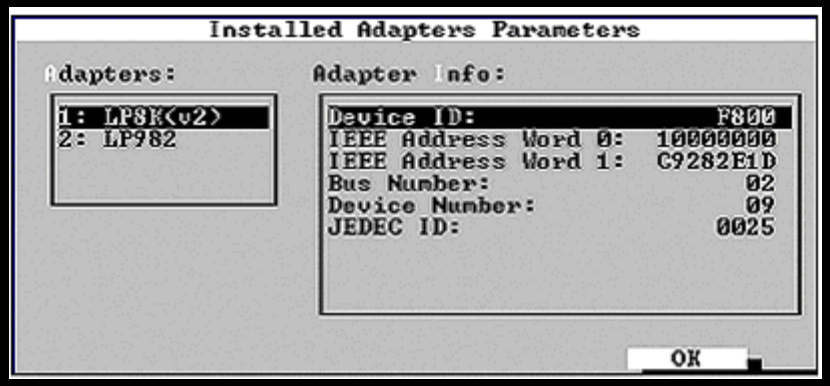
Fibre Channel Attacks
a.k.a.
“Attacks of Mass Destruction”

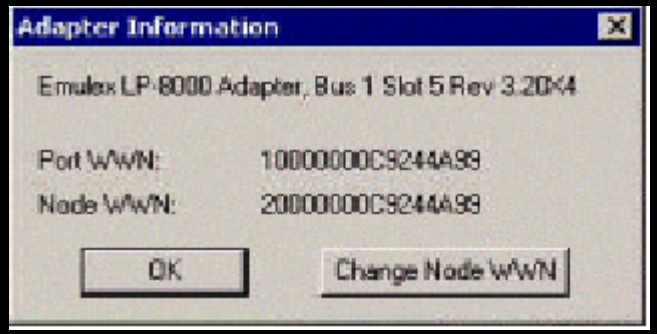
Attacks on FC SANs

- Attack Classes
  - Fibre Channel HBAs
  - Fibre Channel Switches
  - Fibre Channel Frames

Attacks of FC SANs: HBA

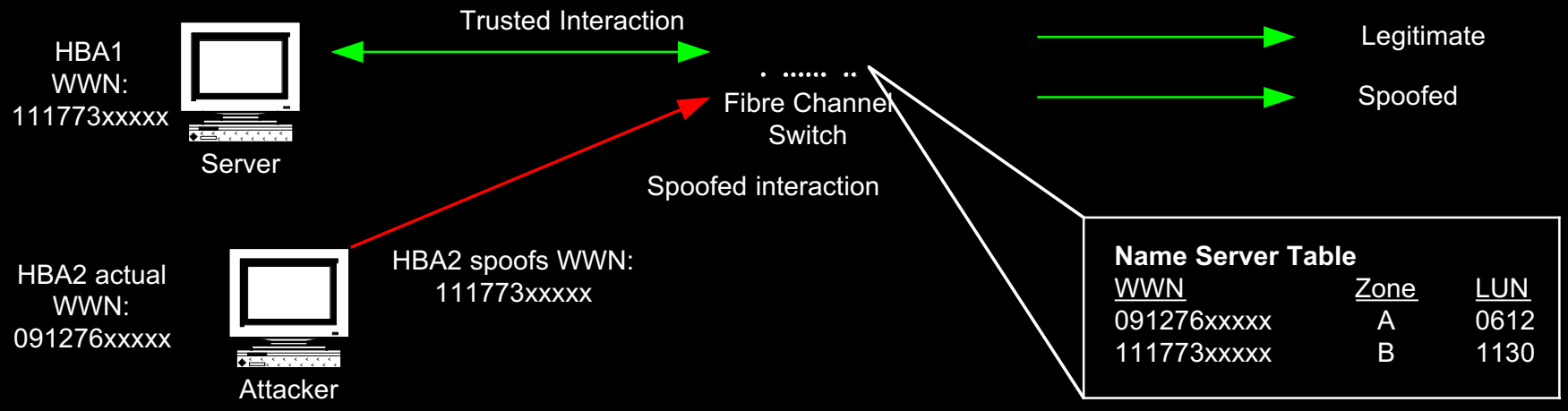
- Spoofing
  - The WWN of an HBA is used to authorize the client node to the FC switch, which allows it to get access to certain LUNs on the storage node
  - A WWN can be changed (spoofed) relativity easily.
    - Changing WWN information is actually a feature provided by HBA vendors
  - After an attacker spoofs a WWN, they will gain unauthorized access to data that has been allocated to the spoofed WWN





Attacks of FC SANs: HBA

- Spoofing



Attacks on FC SANs: Switch

- Switch Zoning
  - Switch zoning allows specific nodes on a fabric to access to other nodes based on the hard/soft zoning policies
  - Currently, switches are the sole entity in many SANs that grant/deny access to nodes
    - Unfortunately, the access that is granted or denied is usually based on authorization only (based on WWNs), without any involvement of the other major security entities, such as authentication, integrity, or encryption

Attacks on FC SANs: Switch

- Zoning – Defined
  - Types
    - Hard zoning – Enforcement based zoning. Two or mode nodes must be a part of the same zone receive route information and to communicate. Hard zoning does restrict traffic
    - Soft zoning – Information based zoning. Two or mode nodes must be a part of the same zone to receive route information on each other. Soft zoning will not restrict traffic
  - Hard or Soft zoning can be based on
    - WWN zoning – A zone based on WWNs
    - Port zoning – A zone based on physical ports numbers on the FC switch
  - Zoning was not created to be a security tool, but rather a segmentation tool
    - Zoning often gets used as security tool, but does not always contain any enforcement capabilities

Attacks on FC SANs: Switch

- Zone Hopping
  - Soft zoning based on WWN
    - Spoofing a WWN will subvert the zoning table, allow an unauthorized WWN to access information of the spoofed WWN
    - Without spoofing a WWN, if an unauthorized WWN knows the route to another WWN in a different zone, which can be enumerated via the fabric, access will be granted
  - Soft zoning based on port numbers
    - Spoofing a WWN will not subvert the zoning table since each WWN is locked to a specific port.
    - Without spoofing a WWN, if unauthorized WWN knows the route to another WWN in a different zone, which can be enumerated via the fabric, access will be granted
  - Hard zoning based on WWN
    - Spoofing a WWN will subvert the zoning table, allow an unauthorized WWN to access information of the spoofed WWN
    - Without spoofing a WWN, a node will not be allow granted access to another node, even if they know the correct route
  - Hard zoning based on port numbers
    - No spoofing or route attacks will be successful

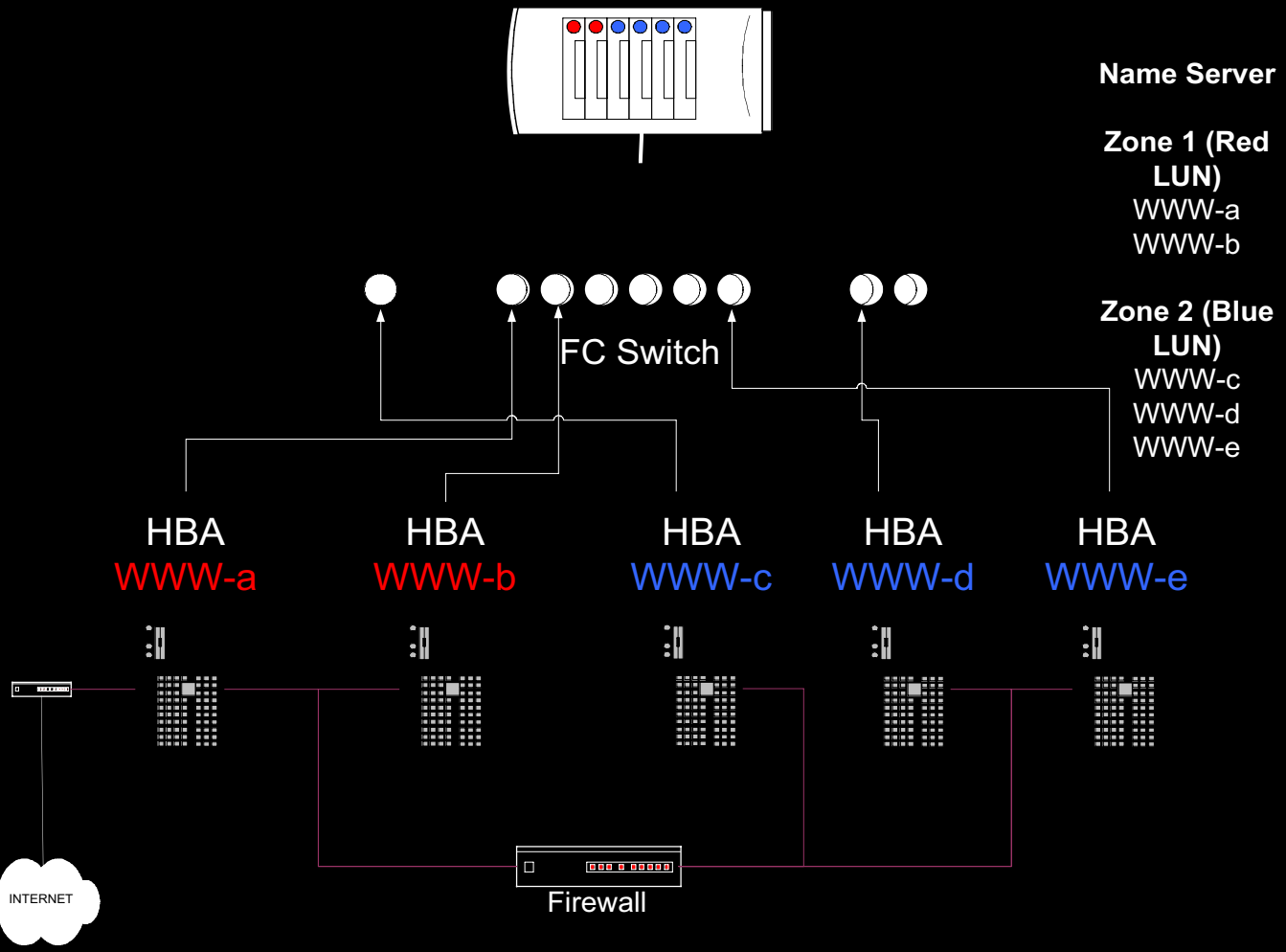
Attacks on FC SANs: Switch

Attacks on Soft zoning with WWNs:
After the Web or FTP server is compromised, an attacker can either access corporate data or access internal devices by:

1. Spoofing their WWN as WWN-c, WWN-d, or WWN-f, and get access to the data allocated for the internal network only (blue)

2. Subverting the firewall on the IP network and directly access the internal file server, internal database server, and internal backup server by directly routing to these devices.

Is OS security the only item protecting your SAN?



Attacks on FC SANs: HBA

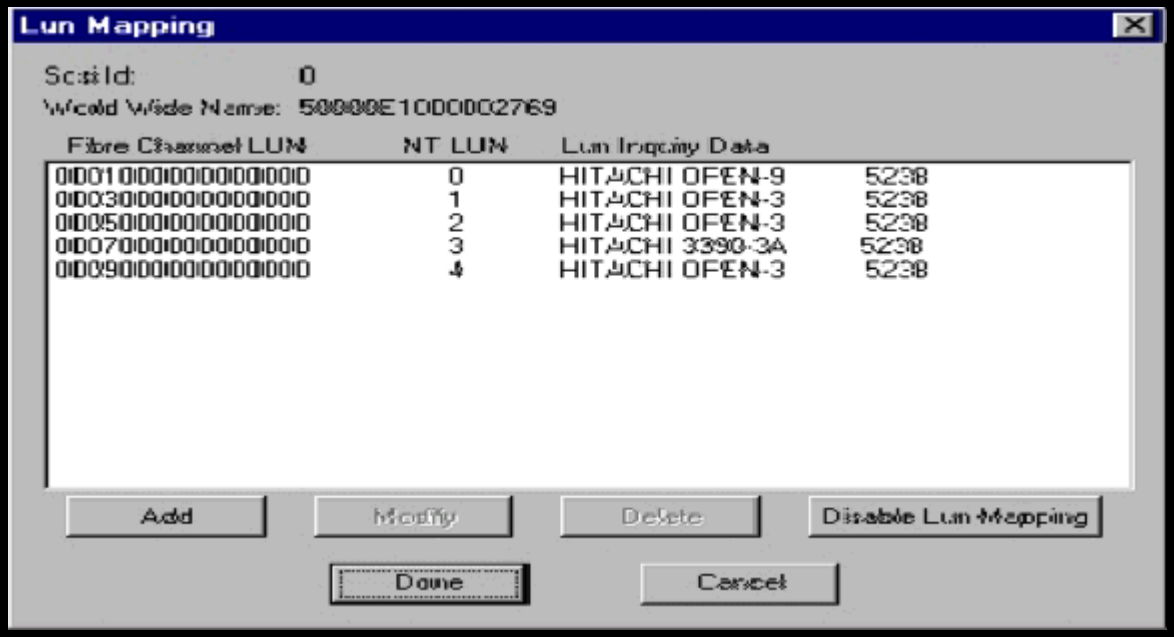
- LUN Masking
  - LUN masking is the process of hiding or revealing parts of a storage disk (specific LUNs) to a client node
    - LUN masking creates subsets of storage within the SAN virtual pool and allowing only designated servers to access the storage subsets.
    - LUN Masking basically presents a limited set of LUNs to client nodes.
  - LUN Masking can occur at four different places: on the client node, the FC switch, the storage-node, or a third-party masking application/device
  - Remember: LUN masking was not created to be a security tool, but rather a segmentation tool
    - LUN masking often gets used as security tool, but does not contain any enforcement capabilities

Attacks on FC SANs: HBA

- LUN Masking Attacks
  - If LUN masking is occurring on the client node, using HBA drivers, then an attacker can perform the following steps to subvert it:
    - Open the the LUN Masking properties on the client node, which has no authentication parameters
    - Change the settings to remove any and all masking
  - This will allow the client node to view all the LUNs that it has identified, authorized or not!

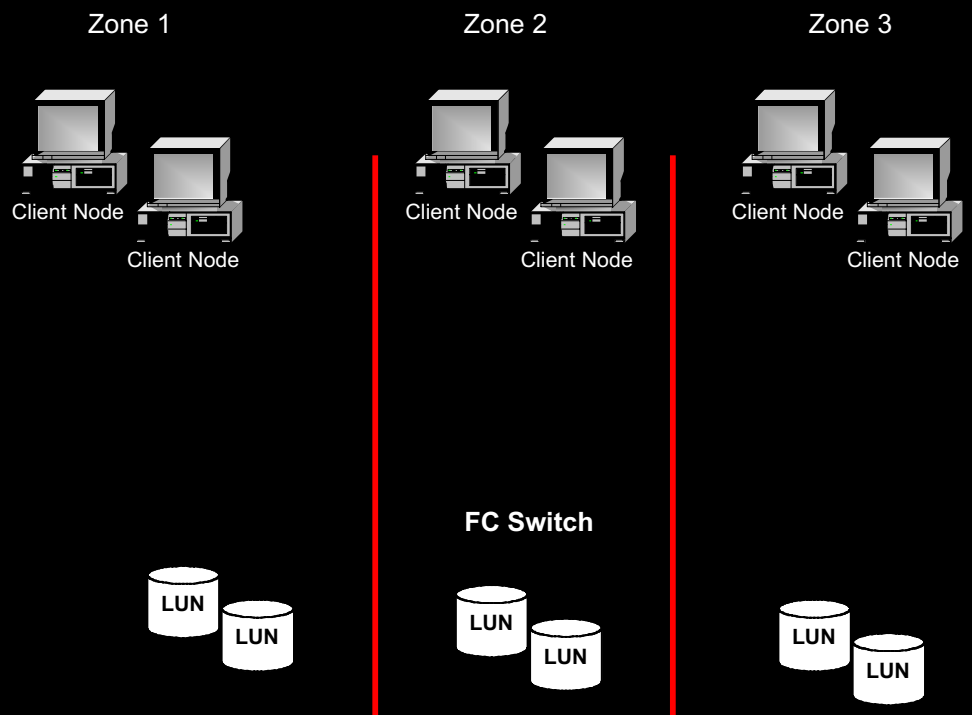
Attacks on FC SANs: HBA

- LUN Masking Attacks
  - HBA Driver to change LUN information



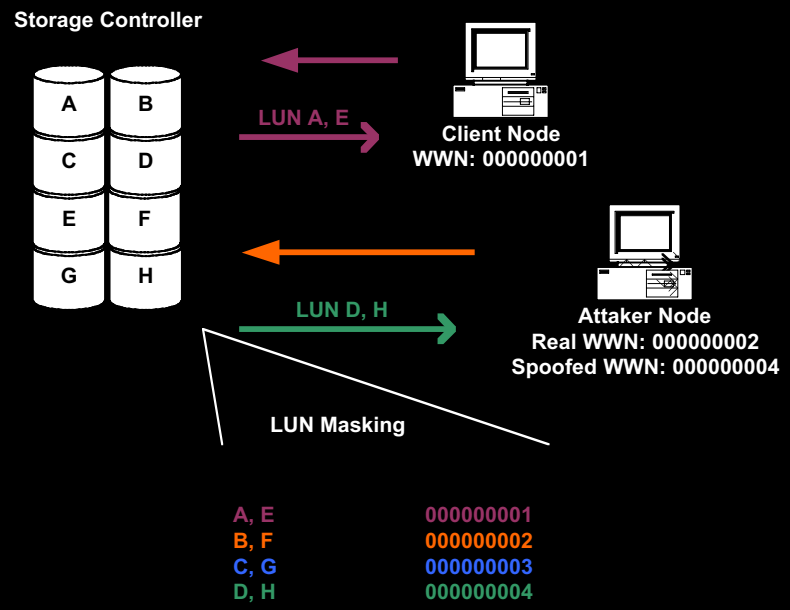
Attacks on FC SANs: HBA or Switch

- LUN Masking Attacks
  - If LUN masking is occurring on the FC Switch, then a spoofed WWN would subvert the LUN Masking properties



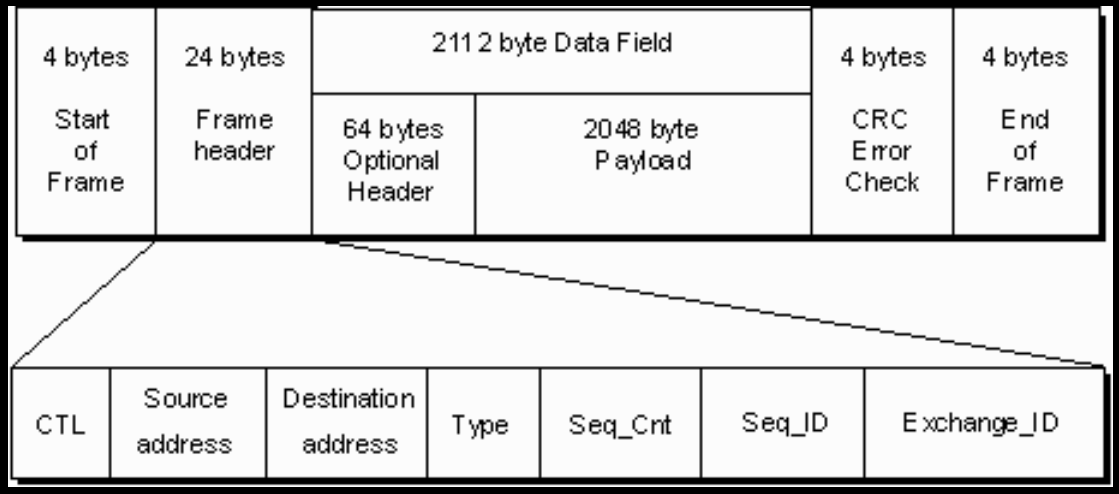
Attacks on FC SANs: HBA or Switch

- LUN Masking
  - LUN masking at the storage controller
    - The storage controller can be used to only expose certain LUNs to certain WWNs
  - Spoofing a WWN will subvert the security control



Attacks on FC SANs: Frame

- Session Hijacking - Sequence ID Weakness
  - SEQ_CNT and SEQ_ID
    - All frames must be part of a Sequence. Frames within the same Sequence have the **same** SEQ_ID field in the header.
    - For each frame transmitted in a Sequence, SEQ_CNT is incremented by **1**.



Attacks on FC SANs: Frame

- Session Hijacking
  - SEQ_CNT and SEQ_ID
    - A Fibre Channel Sequence is a series of one or more related frames transmitted unidirectionally from one port to another.
    - All frames must be part of a Sequence. Frames within the same Sequence have the same SEQ_ID field in the header.
    - The SEQ_CNT field identifies individual frames within a Sequence. For each frame transmitted in a Sequence, SEQ_CNT is incremented by 1.
      - This provides a means for the recipient to arrange the frames in the order in which they were transmitted and to verify that all expected frames have been received.
    - This is similar to what???

Attacks on FC SANs: Frame

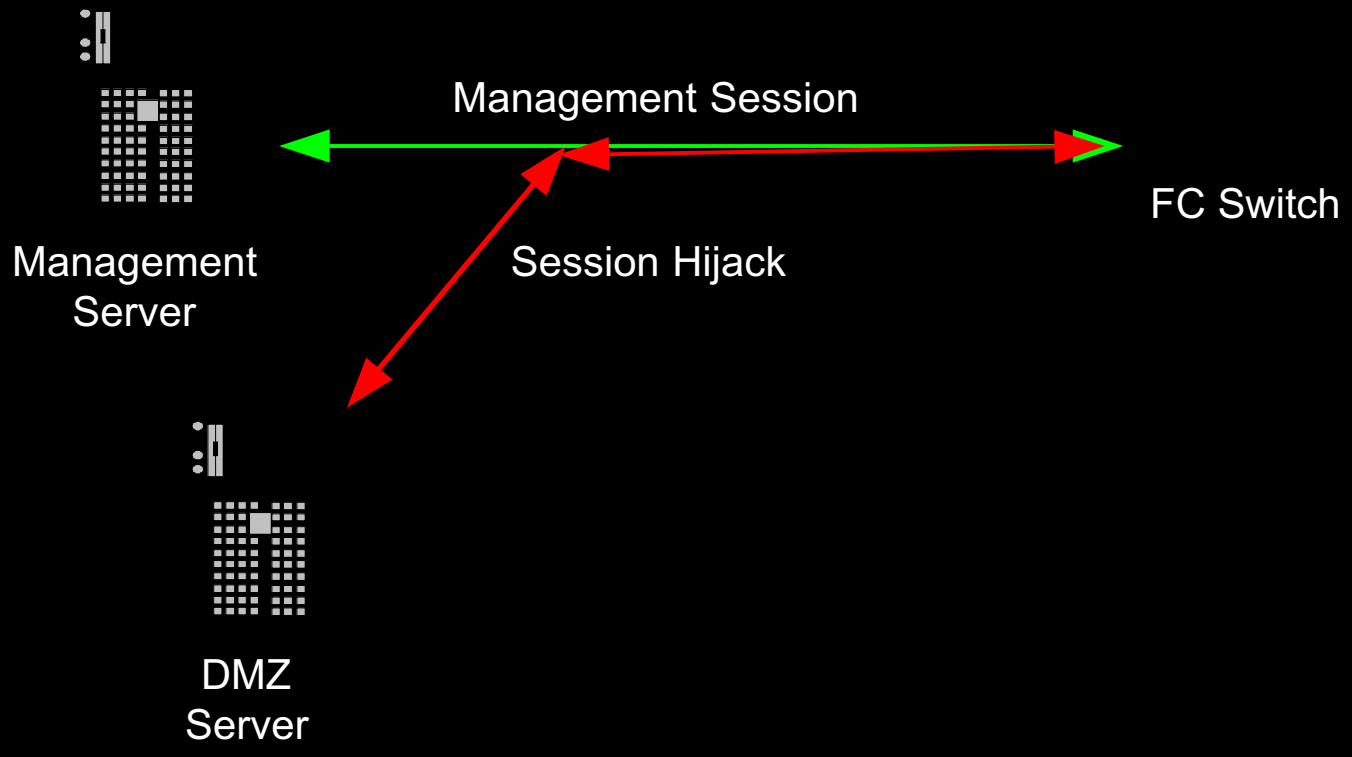
- Session Hijacking
  - FC session hijacking could be conducted if a third party takes control of an existing session between two trusted machines by predicting the Sequence ID and Sequence Control number in FC-Layer 2
    - In FC-2, the SEQ_CNT field identifies individual frames within a Sequence. For each frame transmitted in a Sequence, SEQ_CNT is incremented by 1.

Attacks on FC SANs: Frame

- Session Hijacking
  - In order to hijack a session between two nodes, an attacker can:
    - Capture the Sequence ID (SEQ_ID) value
      - Clear-text
    - Predict the value of the the control number (SEQ_CNT)
      - Incremented by 1, so it is not very hard to predict
    - Since there is no integrity checks on the frames, session can be hijacked

Attacks on FC SANs: Frame

- Session Hijacking



Attacks on FC SANs: Frame

- Addressing and Routing
  - 24-bit Address
    - 8bit Domain (unique switch ID), 8bit Area (groups of F_Ports), 8bit Port (N_port)
  - Routing
    - A node (N_Port) is dynamically assigned a 24-bit address, usually by a switch but performed by the topology (fabric), that is used for frame routing.
    - Name Servers in switches maintain an table that has the 24-bit port address and the 64-bit World Wide Name
  - What does this remind you of?

Attacks on FC SANs: Frame

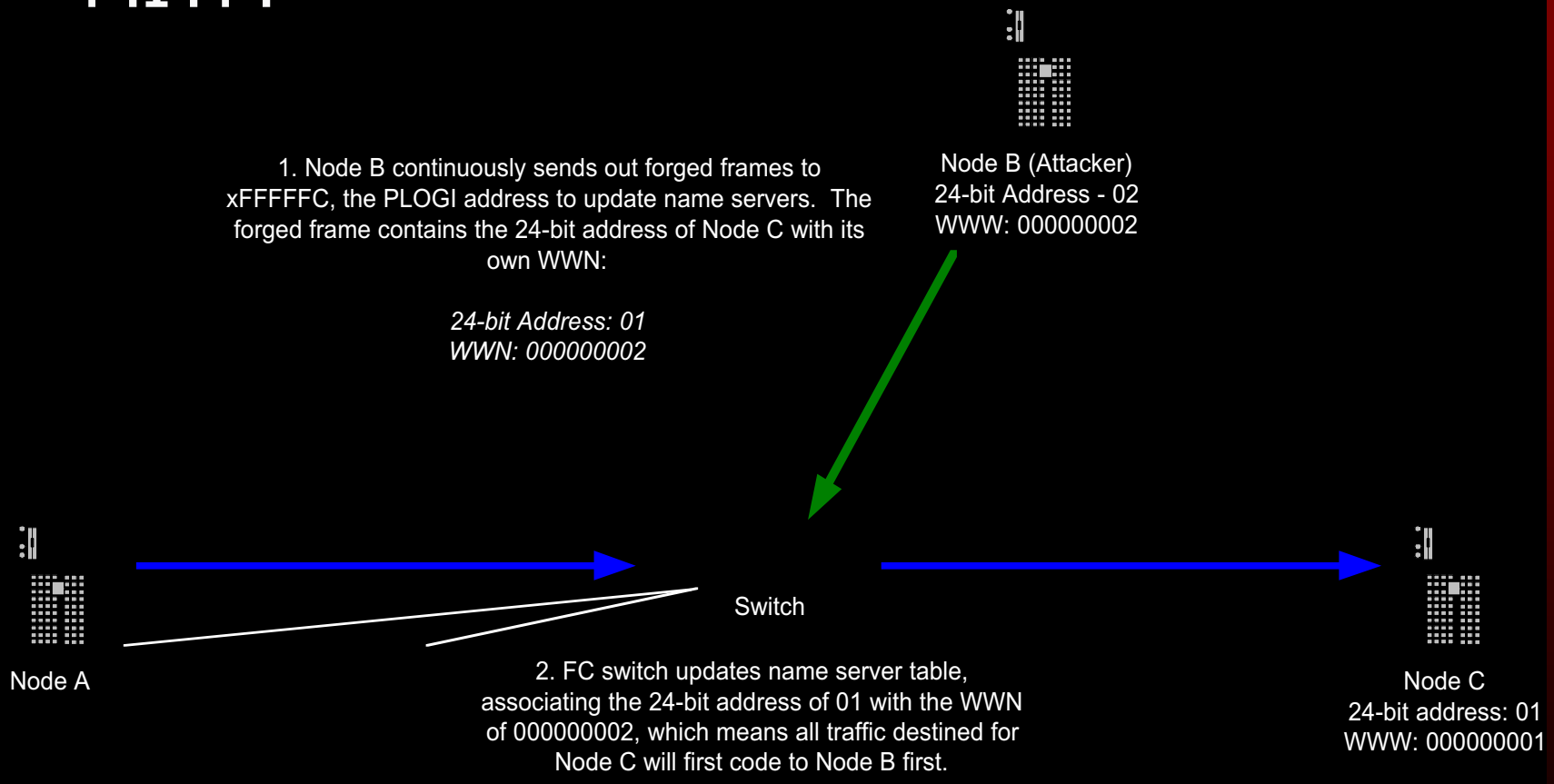
- Man-in-the-Middle – Fabric Weakness
  - Joining the fabric
    - The unauthorized N_Port can send a Fabric login (FLOGI) to the well know address of xFFFFFE (similar to broadcast) using an address of of 0x000000
    - The fabric and connected switches receive the frame at the address of xFFFFFE and return an accept frame (ACC). The ACC frame has the N_port's new 24-bit address in it.
    - Once the N_Port has its new 24-bit fabric address, it needs to send a port login (PLOGI) to xFFFFFC, which is the address that allows name servers on the switches to update their WWN to 24-bit address associations.

Attacks on FC SANs: Frame

- MITM
  - Polluting the Name Server
    - Knowing there is no validation or authentication required when using sending a PLOGI, an attacker can spoof their 24-bit address and send it to xFFFFFC (PLOGI destination address), causing the NS information in the switch to be polluted
      - An attacker sends out a forged frame to xFFFFFC with the 24-bit address of the target node and the WWN of itself.
      - The fabric (and switch) registers the new information
      - Since the fabric now assumes that the target's 24-bit address should be routed to the WWN of the attacker, all frames destined for the target node are passed to the attacker first

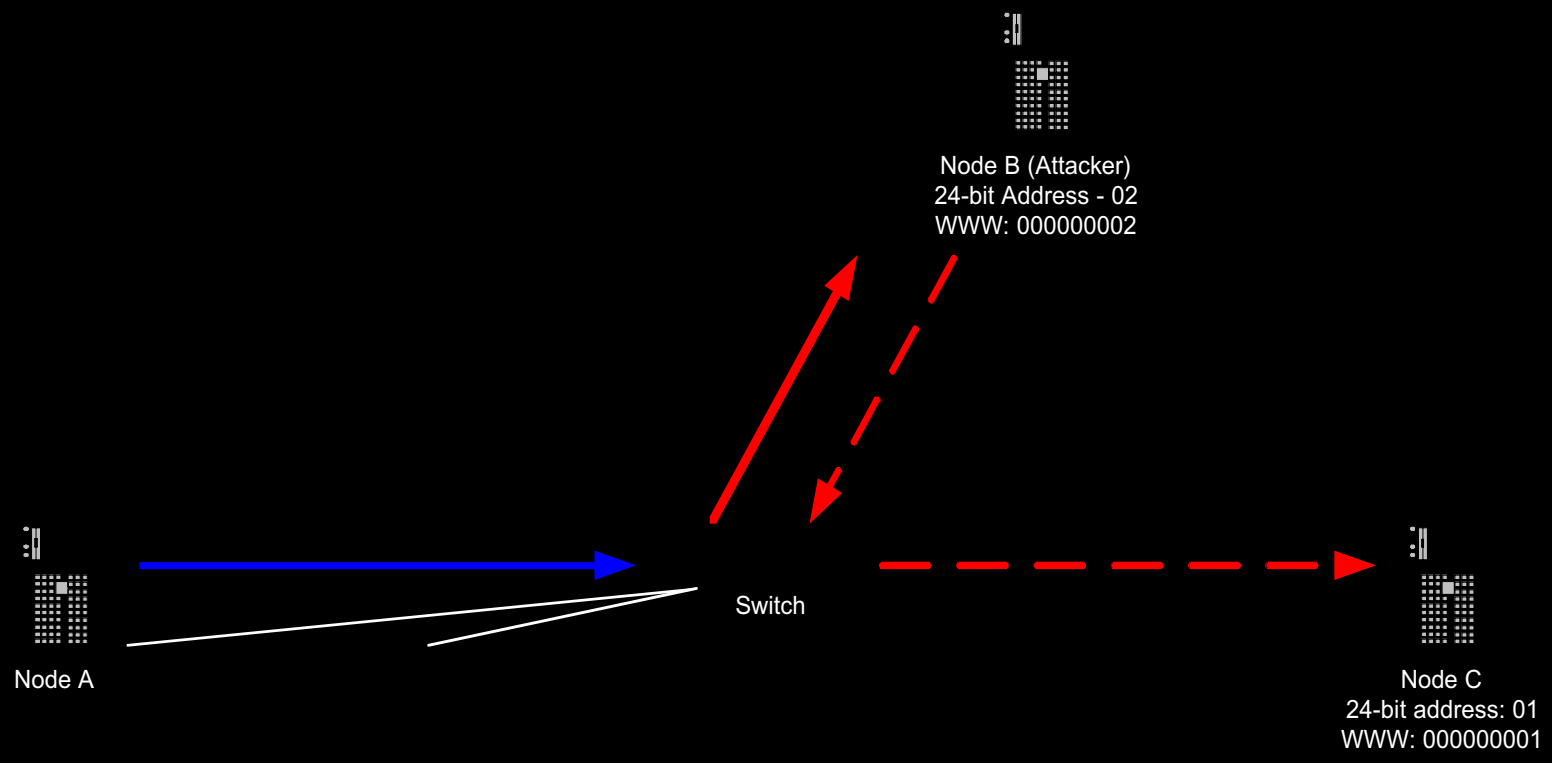
Attacks on FC SANs: Frame

- MITM



Attacks on FC SANs: Frame

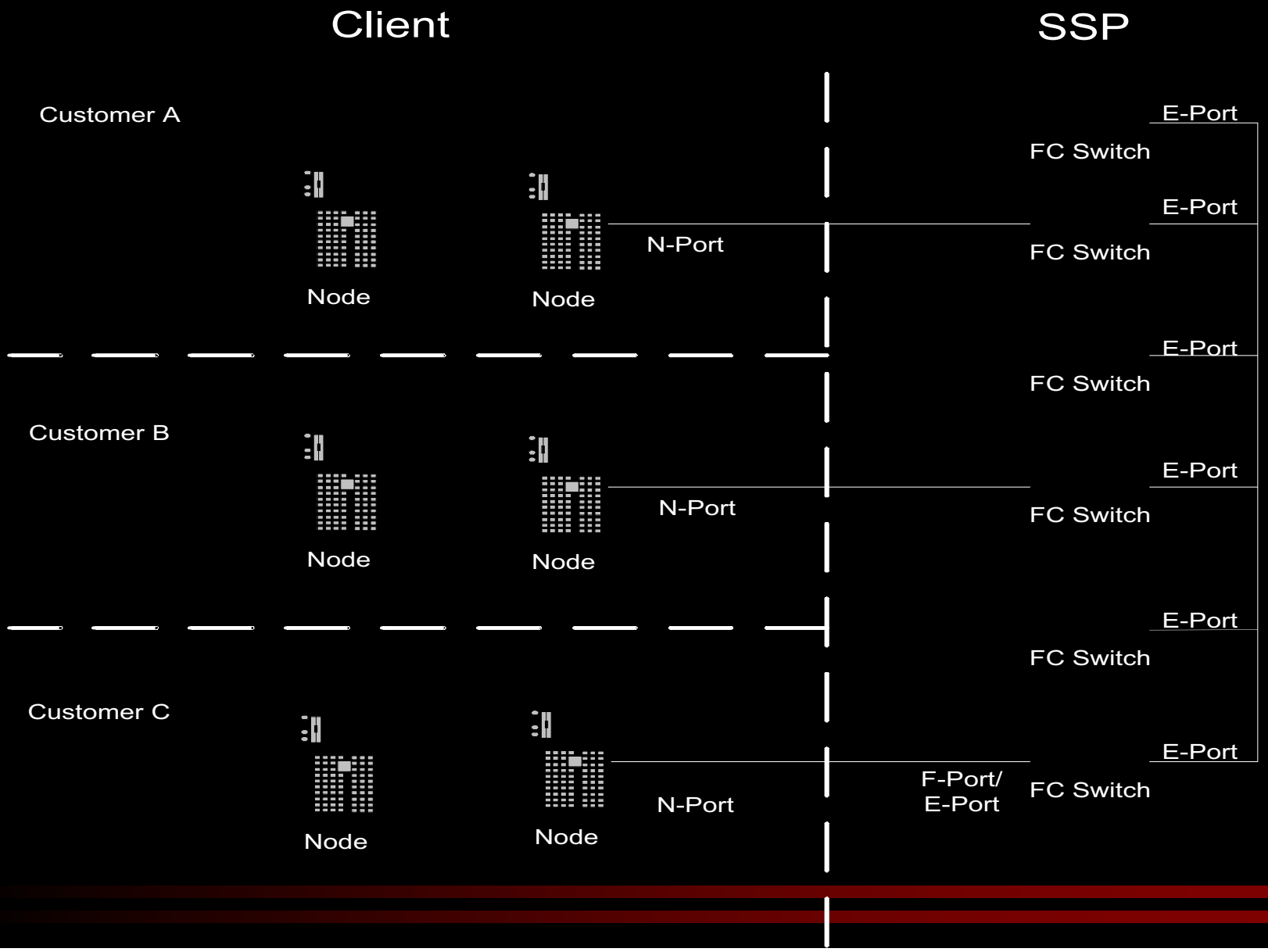
- MITM



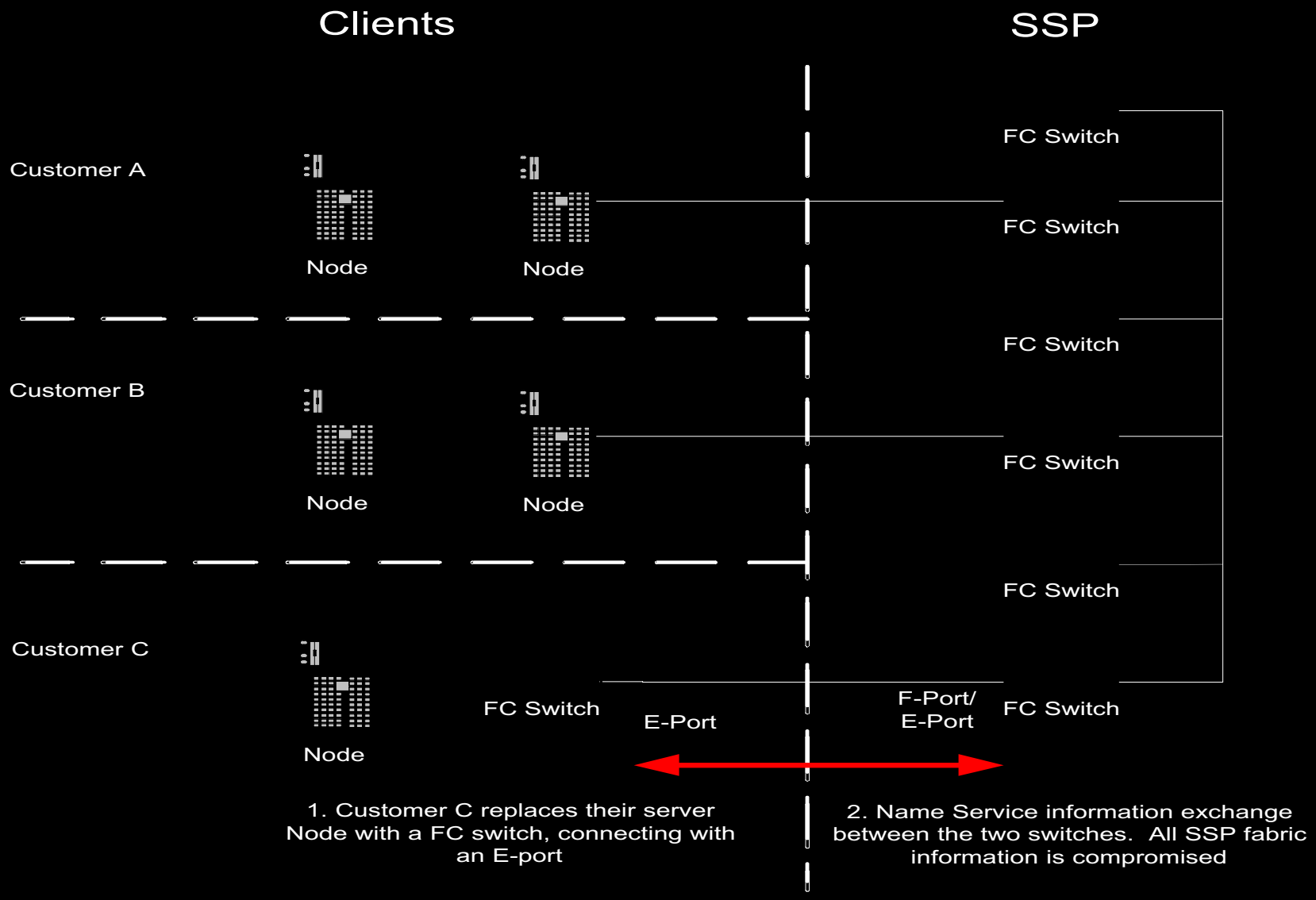
Attacks on FC SANs: Switch

- E-port Replication
  - Share Infrastructure attack
  - E-port (Expansion Ports) on a FC switch provides an "uplink" to other switches
  - Once both switches recognize they are connected to E-ports on the other end, fabric information is automatically transferred between each other, such as Name Server information, management, zoning tables, etc.
    - Often times authentication is required for E-port replication
  - By default, all ports on many FC switches can be both F-ports and E-ports

Attacks on FC SANs: Switch



Attacks on FC SANs: Switch



Attacks on FC SANs: Frame

- Exchange ID – Flow Control Weakness
  - Disruption of Flow Control
    - A device can transmit frames to another device only when the other device is ready to accept them. Before the devices can send data to each other, they must login to each other and establish credit.
    - Credit
      - Credit refers to the number of frames a device can receive at a time. This value is exchanged with another device during login, so each knows how many frames the other can receive.
    - Disruption of Flow control
      - Since this is no authentication or integrity checking of exchange information, an attacker can modify the exchange service information between two authorized nodes, disrupting the service

Attacks on FC SANs: Switch

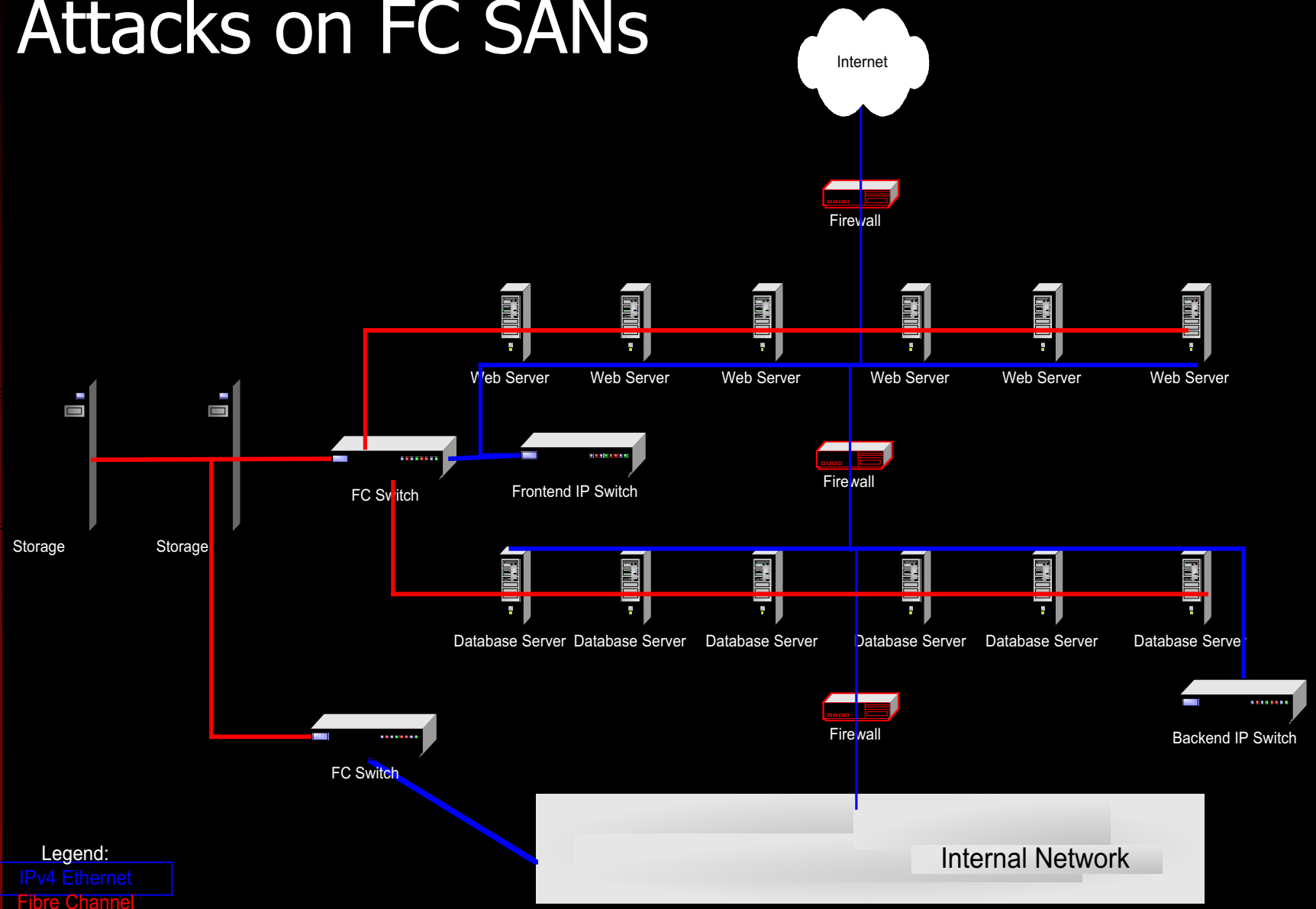
- Cut-through switching
  - Some switches only look at the D_ID (24-bit Destination address) to route the frame
  - Increases performance by reducing the time required to make a routing decision
  - However, there is no verification of the S_ID (Source address) and the frame is passed

Attacks on FC SANs: Switch

- Web Management
  - Just like everything else, clear-text management, such as HTTP, is BAD
  - Common Passwords for FC Switches

password	monitor	<switch vendor>	Config
admin	temp	<company name>	test
manage	root	letmein	secret
prom	backup	secureme	keepout
filer	KuSuM	abcd1234	test123
netcache	momanddad	money	green

Attacks on FC SANs



Attacks on FC SANs: Switch

- Web Management
  - There are two attack vectors here for the SAN:
  1. Compromise the web server
  2. Via the Web server, gain access to the database sever
  3. Via the database server, subvert the internal firewall
  4. Once inside the internal network, attack the IP interface of the SAN Switch
  5. Compromise the internal FC switch
- Or
1. Compromise the web server
2. Attack the IP interface on the SAN Switch
3.

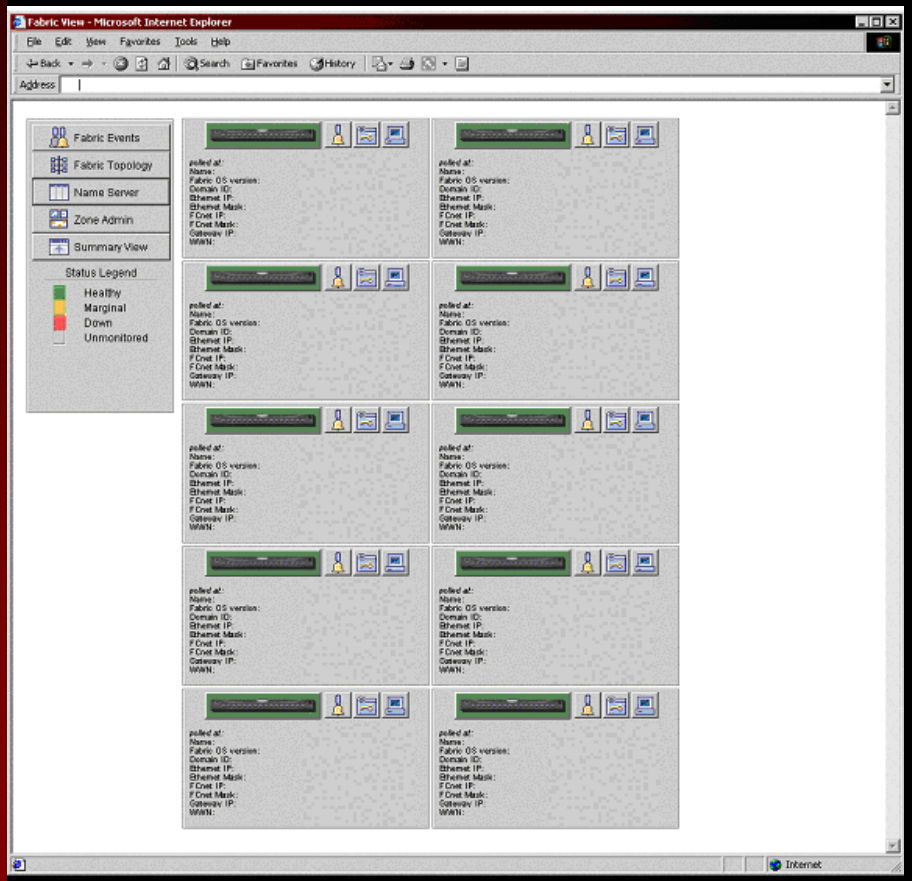
- Which one would you choose?
- Often times all internal network users, including contractors, consultants, business partners, have access to the management interface of the SAN

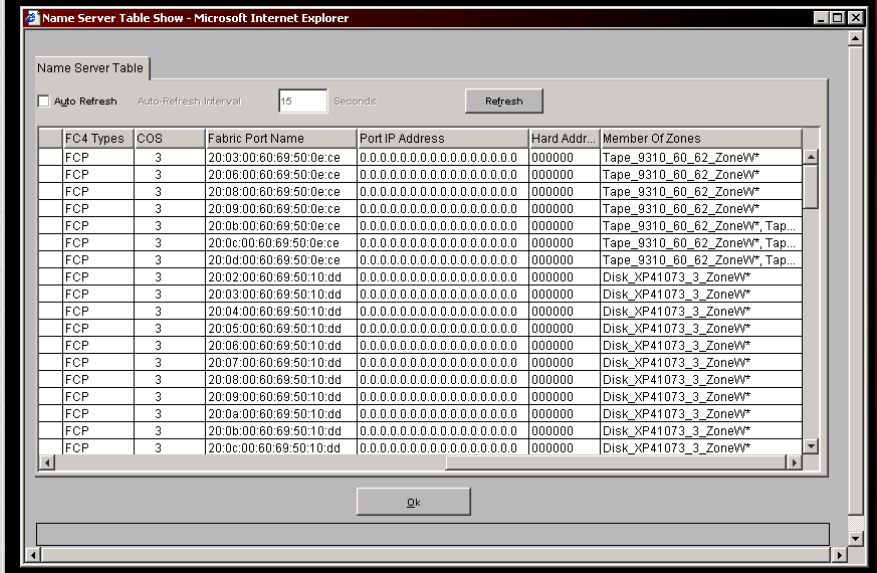
Attacks on FC SANs: Switch

- Web Management
  - Direct access to data is not possible, so what can be gained?
    - Enumeration of the SAN Topology
    - WWN information to conduct WWN spoofing attacks
    - Command line access to the switch
    - Complete Zone Information

Attacks on FC SANs: Switch

- Web Management





Conclusion

Conclusion

- Security Solutions
  - Despite the attacks we have reviewed, there are several mitigation solutions that can help you deploy and maintain a secure SANs

Conclusion

- FC Switches - Short-Term
  - Hard Zoning based on physical ports
    - Hard zoning based on physical ports, add a significant layer of security
      - Disables Spoofing Attacks
  - Port Binding (Locking)
    - Port Binding locks a physical port to an authorized WWN.
      - Disables Spoofing Attacks
  - Port-type Controls
    - Port-type Controls will lock a given port to a specific type, such as G-port, F-port, or E-port, according to their appropriate specifications.
      - Disables E-port replication attacks

Conclusion

- FC Switches - Long-term
  - SLAP
    - Switch Layer Authentication Protocol. Switch to switch authentication via digital certificates and unique private keys
      - Disables web management attacks
  - Fabric Membership Authorization
    - Fabric Membership Authorization incorporates an internal database on each switch with a list of authorized WWNs that may join the fabric.
      - Disables E-port replication
  - Fabric Configuration Servers
    - This switch is the only device allowed to manage the other switches. It uses its own database for authentication, rather than SNMP or regular username/password combination.
      - Disables web management attacks

Conclusion

- LUN Masking
  - Don’t rely on LUN masking as your sole source of security
- Secure entry points
  - Secure operating systems connected to SANs
  - Secure IP interfaces on SAN devices
  - Secure management stations connected to SANs

Conclusion

- Things on the horizon
  - Encryption of data in transit and in storage
    - Encryption will facilitate data integrity and confidentiality
      - FC-GS-4
      - FCSec (Fibre Channel Security)
      - FC Encryption devices (currently two vendors have products available)
- Authentication
  - Certificate based authentication to fabric
    - Switch to Switch and HBA to Switch

Conclusion

- General Attack Mitigations
  - If your SAN is not dynamic, consider using ports for zone allocation instead of WWNs for zone allocation
  - Consider using Hard zoning (enforcement based zoning) instead of soft zoning (non-enforcement based zoning)
  - Change default switch passwords
  - Do not implement LUN masking on the client node
  - Allow switch management from only secure networks, not the internal network
  - Study key authentication options for switch to switch access
  - Do not use one zone for the entire SAN, separate storage zones based on security zones established in IP network

Conclusions

- General Attack Mitigations (con't)
  - User separate IDs for administration and maintenance accounts
  - Disable In-band management (SES or FC-SNMP), if possible
  - Disable cut-through switching
  - Enabling port locking and port binding
  - Consider using data-at-rest and in-line encryption tools and products
  - Disable e-Port replication or any automatic Name Server transfers
  - Harden gateways (Secure any operating system with a connection to the storage network)

Conclusion

- *Vendor support*
  - Key Authentication between storage devices
    - WWN, Switches, etc.
    - Interoperability
  - ENCRYPTION
- Authenticated Frames
- Encrypted Data
- Unpredictable Sequence Control Numbers
- Two-Factor authentication in software management applications
  - Not just a username and password

Conclusion

- Follow Best Practices
  - Following simple **best practices**, where possible, may **partially** or completely prevent unauthorized access to the storage network or its data, creating a **difficult** attack vectors for the unauthorized user
- Manage Risk
  - 1st: Fully understand your risk exposure
  - 2nd: Figure out your risk tolerance
  - 3rd: Make decisions on storage security architecture

Questions

Himanshu Dwivedi
hdwivedi@lokmail.com or hdwivedi@stake.com

Storage Security Books co-authored by presenter:
Storage Security (NeoScale Publishing)
The Complete Storage Reference, Chapter 25 (McGraw-Hill)

Storage Security Whitepaper co-authored by presenter:
www.@stake.com/research/reports/index.html

Special Thanks:
Andy Hubbard, Joel Wallenstrom, Heather Mullane, and Kusum Pandey