SNIA

Education

Saving Private Data
An Introduction to Storage Security

Richard Austin, MS, CISSP, MCSE

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.

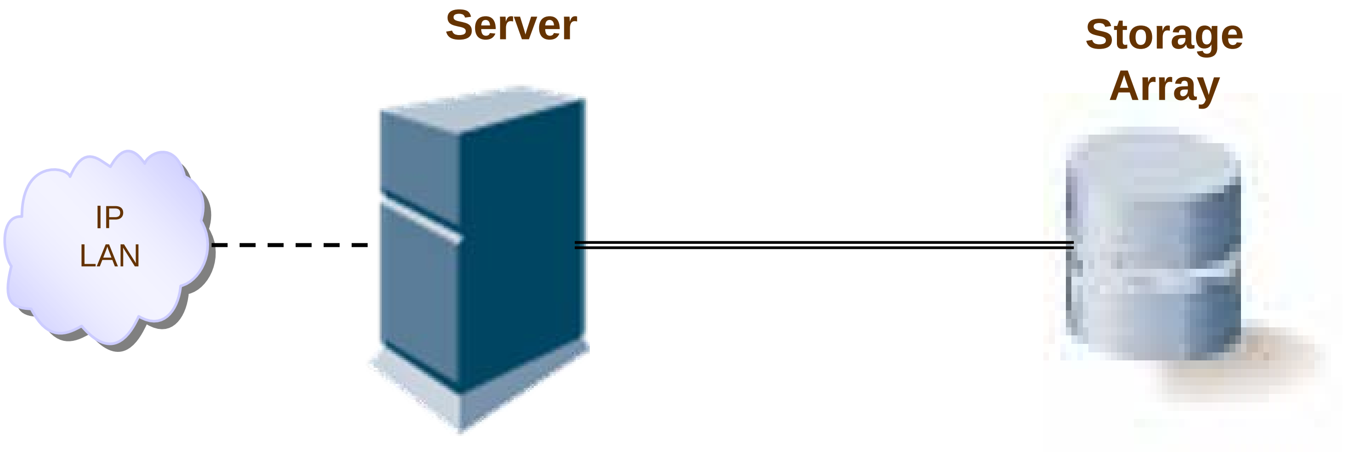
Abstract

- Saving Private Data
- In their relentless drive to master the ever increasing floods of data, organizations increasingly exploit the efficiencies and cost reductions realized through storage networking. But as these information assets centralize, their value as targets increases dramatically. Tales of breaches litter the popular and industry press as more organizations find themselves becoming statistics in the struggle to safeguard their information.
- This tutorial introduces the newly revised best common practices for storage security developed by SNIA's Security Technical Working Group and will provide timely guidance on how you can succeed in the mission of saving your organization's Private Data.

Welcome to our world

- Availability and integrity of data are critical to organizational survival
- Mishandling of sensitive data can result in severe consequences
- Organized crime has discovered that cyber crime (such as identity theft) is more profitable (and less risky) than drug trafficking
- Data is no longer safely tucked away behind servers

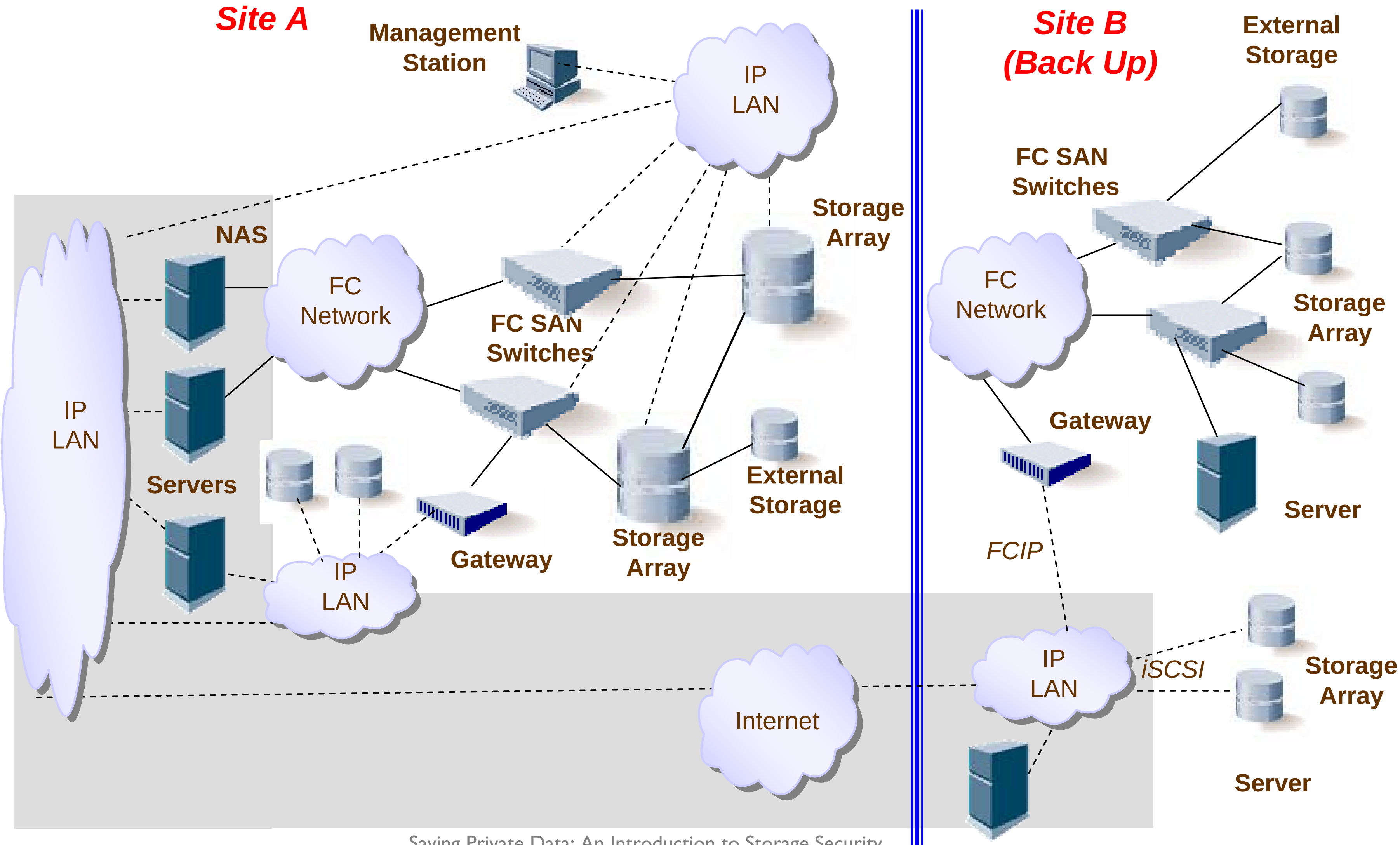
The way it used to be (server-attached storage)



Secure the server and you secure the storage.

To get the data, you have to compromise the server

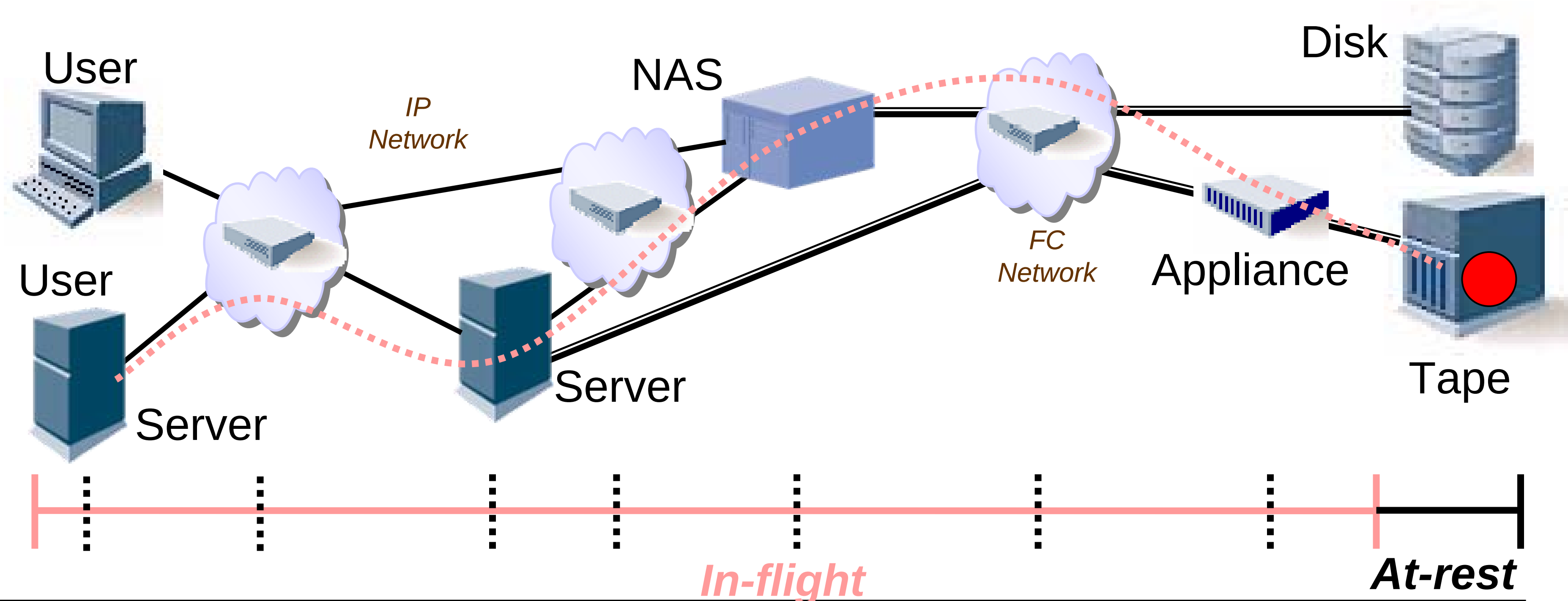
A Modern Storage Ecosystem



The Situation Changes

- With ease of management, operational efficiency and the other advantages of a SAN, comes two significant changes:
  - Our data is concentrated in **FEWER** places (targets) and the **VALUE** of those targets has been increased
  - Our data spends its time in two states:
    - In-flight
    - At-rest

In flight and at rest



In-flight:

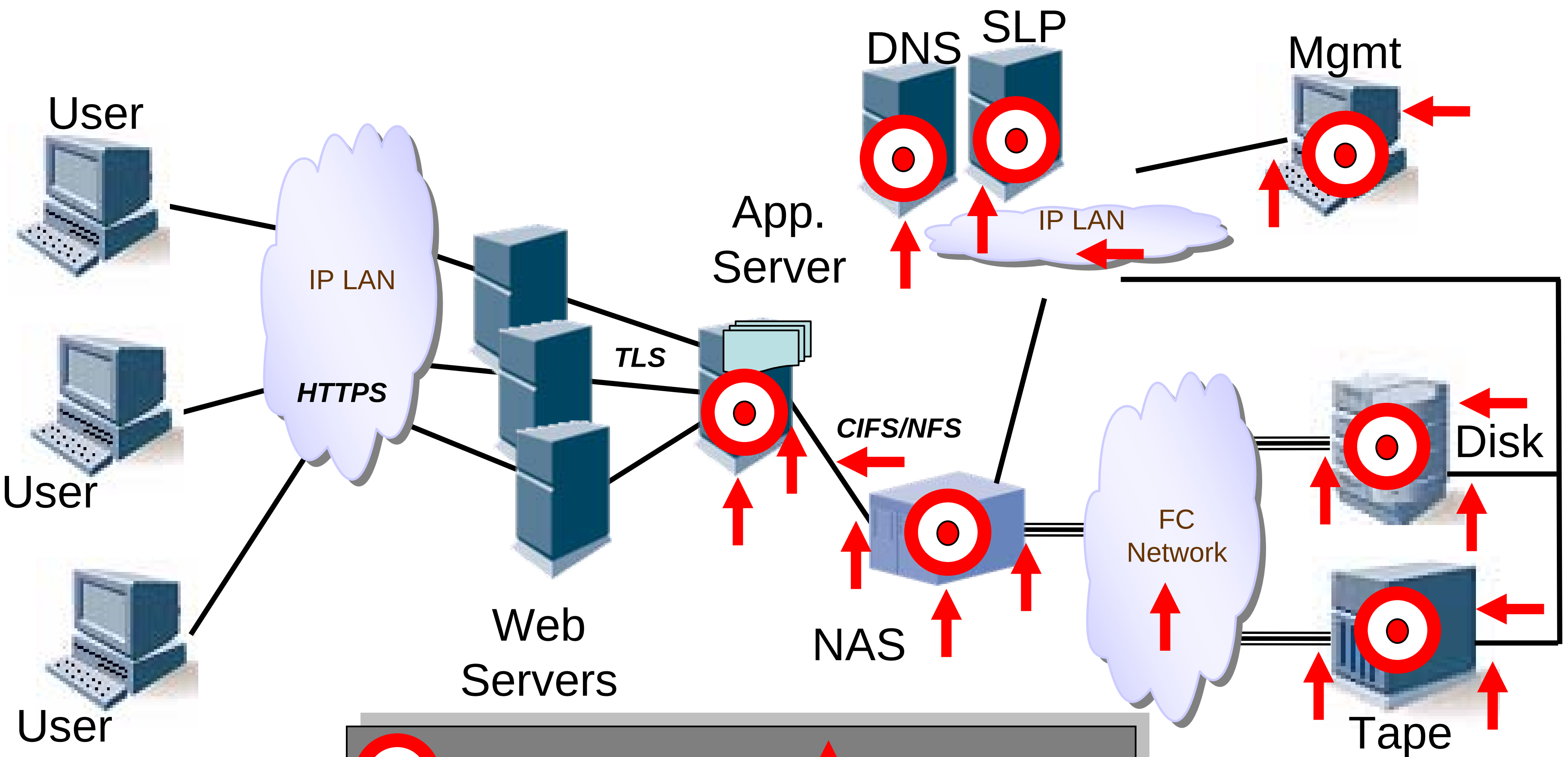
- Two end points (communication)
- Interoperability – network layers
- Data is transitory (temporary)

At-rest:

- Interoperability – media interchangeability
- Data is persistent on media

Very Different Threats and Threat Agents

Storage Ecosystem Attack Points



◎ Potential Target ↑ Attack Point

Security Challenges

- Control of Privileged Users (Administrators)
- Protection of Storage Management
- Credential & Trust Management
- Data In-flight Protection
- Data At-rest Protection
- Data Availability Protection (redundancy, resiliency, integrity, performance)
- Data Backup & Recovery (disaster recovery, business continuity)
- Long-term Archive (access, crypto, authenticity)
- Defense & Intelligence (labeled storage)
- Information Lifecycle Management (ILM)
- Compliance

What should we do?

Best Current Practices

- Begin with the guidance available
  - ISO 27002
  - FFIEC
  - PCI DSS
  - ISACA auditor guidance
- Apply to the storage ecosystem to develop best practices

SNIA Storage Security BCPs

- Core (Applicable to Storage Systems/Ecosystems):
  - General Storage Security
  - Storage Systems Security
  - Storage Management Security
- Technology Specific:
  - Network Attached Storage (NAS)
  - Block-based IP Storage
  - Fibre Channel Storage
  - Encryption for Storage
  - Key Management for Storage
  - Archive Security

SNIA Storage Security – Best Current Practices (BCPs) Version 2.0, http://www.snia.org/forums/ssif/programs/best_practices/

Starting Points with the BCPs

- Storage Management
- NAS
- iSCSI
- Data Sanitization
- Encryption of Sensitive Data

Storage Management

- Remember: If an attacker can get management access to your SAN, it’s not your SAN anymore!
- What to Check:
  - Compliance with authentication and authorization requirements
  - Appropriate segregation of management traffic
  - Use of secure channels for all remote management
  - Audit logging with full traceability of all privileged user actions
  - Configuration management practices
  - Protections against indirect attacks from IT infrastructure
  - Appropriate controls and monitoring of vendor maintenance
  - Consistent controls on in-band and out-of-band management
  - Protections against malware

Network Attached Storage (NAS)

- Remember: With network access to data comes the possibility of network attacks.
- What to Check:
  - Use of data access protocols with significant security flaws
  - Network based protections to establish risk domains
  - Use of secure channels for all remote data access
  - User-level authentication employed whenever possible
  - Granting unrestricted (root) access to files on NAS or file server
  - Enabling multi-protocol (e.g., NFS & CIFS) configurations for users who do not use these services
  - Protections against malware
  - Encryption of sensitive files and directories

Internet SCSI (iSCSI)

- Remember: iSCSI is a storage protocol BUT it runs over a TCP/IP network!
- What to Check:
  - Network based protections to establish risk domains
  - Use of entity-based, mutual authentication (CHAP) for all iSCSI initiators and targets
  - Appropriate segregation of iSCSI traffic for security and performance
  - Use of IPsec to ensure in-flight confidentiality of sensitive data
  - Protections against indirect attacks from IT infrastructure

Data Sanitization

- Remember: Manage your data end-of-life to avoid unauthorized disclosure.
- What to Check:
  - Mechanisms actually clear the data residing on the media
    - Recommendations in NIST SP800-88
  - Performed in compliance with a data sanitization policy
  - Sanitization does not violate laws, regulations, or court orders
    - Is there a discovery request or a preservation order for this data?
  - Sufficient controls to ensure the mechanisms are not attack vectors
  - Use of "crypto shredding" factors in the strength of the ciphers
  - Applied to all copies of data residing in backups, at BC/DR sites, in system caches, application caches (e.g., search engines), device mirrors, etc.

Encrypting “Sensitive” Data

ABC’s of Encryption

- Focus on Data Leaving Your Control
  - Data stored on removable media like backup tapes, must be encrypted while at-rest
  - Data stored in third-party (untrusted) data centers must be encrypted both in-flight and at-rest
  - Data transferred between “trusted” data centers must be encrypted in-flight
- Encrypting Data At-rest – A measure of last resort
  - Use extreme care when encrypting primary data
  - Long-term key management is a ***critical*** element

PERIGO DANGER

Encryption of Data At-rest – A Step-by-step Checklist, http://www.snia.org/forums/ssif/knowledge_center/white_papers/

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

Richard Austin, CISSP
Eric Hibbard, CISSP, CISA
Andrew Nielsen, CISSP, CISA
Roger Cummings
Jim Norton
Phil Huml

Anthony Whitehouse
Larry Hofer, CISSP
Walt Hubis
Vinod Bhat
Leroy Budnik, CISA