SNIA

Education

Cryptographic Use Cases and the Rationale for End-to-End Security

Larry Hofer, CISSP
Emulex

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

Cryptographic Use Cases and the Rationale for End-to-End Security

The variety of environments in which Fibre Channel (FC) fabrics and other technologies such as iSCSI and FCIP are deployed makes it likely that customers will have many choices for data protection in the future. Data protection solutions such as data integrity, data-at-rest, and in-flight data protection are among those choices. This tutorial surveys many use cases that identify the locations in a SAN where security may be applied and explores an end-to-end security approach.

Learning Objectives

- Develop an understanding of various data protection alternatives, including data integrity, data-at-rest, and data in-flight and how they mitigate different threats in SANs
- Identify numerous locations in a SAN where security technologies can be applied and the pros/cons of each alternative
- End-to-end security is studied in-depth as one common approach

Storage Security Terminology

- **Data Integrity:** the assurance that data is consistent and correct. In cryptography and information security in general, integrity refers to the validity of data. *http://en.wikipedia.org/wiki/Data_integrity*
- **Data at Rest:** Data residing on servers, storage arrays, NAS appliances, tape libraries, and other media (e.g. tape). *
- **Data in Flight:** Data as it is transferred across the storage network, the LAN, and the WAN. The data may include management traffic. *
- Also important to secure:
  - **Storage System:** embedded OS and applications as well as integration with IT and security infrastructure (e.g. external authentication services, logging, firewalls) *
  - **Storage Resource Management:** Provisioning, monitoring, tuning, reallocating, and controlling the storage resources so that data may be stored and retrieved. (i.e. represents all storage management) *

**Source: Introduction to Storage Security, A SNIA Security White Paper, October, 2005.*

Data Protection & Privacy

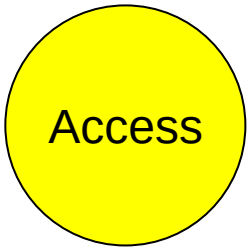
- Simply stated for this tutorial:
  - Getting the right information to the right people or systems at the right time.
  - Preventing the wrong information from being accessed by the wrong people or systems at any time.
- For security professionals these are fundamental:
  - Confidentiality – Is the data private?
  - Integrity – Is the data accurate?
  - Availability – Is the data accessible?
- From the web:
  - **Data protection:** The implementation of administrative, technical, or physical measures to guard against the unauthorized access to data. *http://www.atis.org/tg2k/_data_protection.html*
  - **Data privacy:** refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data. *http://en.wikipedia.org/wiki/Data_privacy*

Threats and Attacks

Attack Scenarios

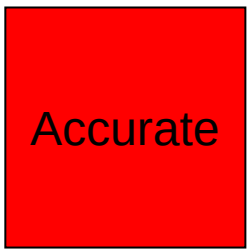
1. **Accidental Corruption**
2. Theft of privileged access (access to root and admin accounts)
3. Privilege Abuse (e.g. Authorized users doing unauthorized things)
4. Application compromise
5. **Sniffing for Confidential Data**
6. **Sniffing for Identities**
7. **Spoofing (i.e. Impersonation)**
8. **Media or Hardware Theft**
9. **Unauthorized data moves, e.g. Cut and Paste**
10. **Tampering with Data at Rest**
11. **Modify Packets**
12. **Inject Packets**
13. **Hijack Connections**
14. **Destruction of Data**
15. **Traffic Replay Attacks**
16. **Man in the Middle Attacks**
17. **Unauthorized Access of Data (e.g. Data Copies)**
18. **Unauthorized Management or Maintenance Control**
19. **Single Point of Failure (Natural Cause Denial of Service)**
20. **Accidental Access or Changes**
21. **Disaster Recovery, Insecure Remote Data**
22. Denial of Service (e.g. Too many connections, Bandwidth Stealing, Too Many Cycles, Access Disablement)
23. Server Compromise
24. Software Compromise
25. Driver Compromise
26. **Unintended Disclosure of Data/Information** (Caution: e.g. Inferences or Traffic Analysis)
27. Encryption Key Loss or Deletion or Corruption
28. **Encryption Key Disclosure**
29. Disrupt Security Negotiation to Downgrade Authentication or access passwords
30. **Compromised discovery systems.**

The Big Picture



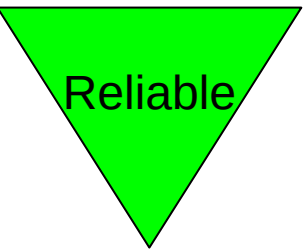
Protecting sensitive data from unauthorized access

- Portable information like CD's, Tapes?
- Data in a 3rd Party's Data Center?



Ensuring the integrity and authenticity of data

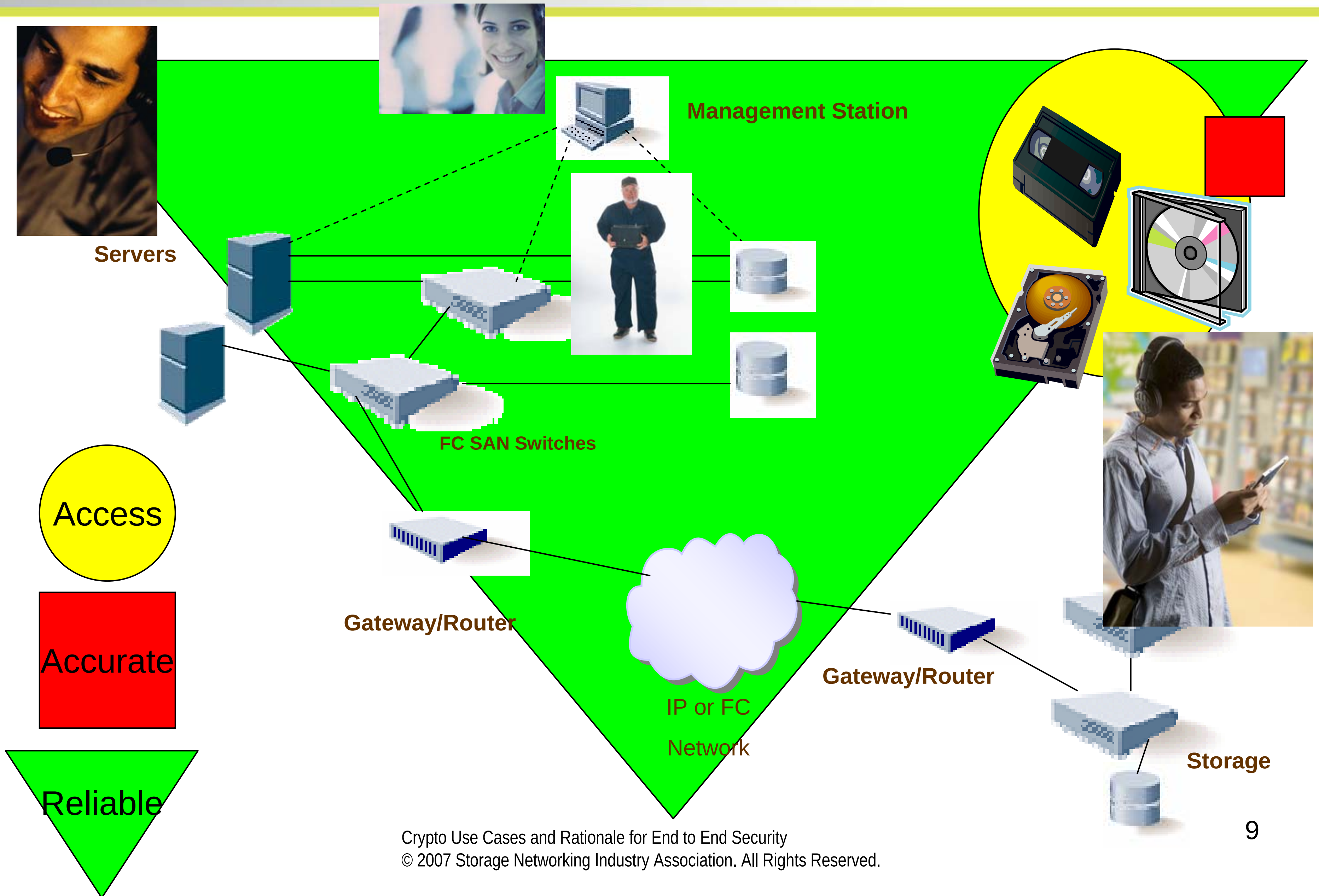
- Connection taps or tampered data
- Physical protection, ends of cables too
- And everything in between it?



Ensuring the accessibility and reliability of data

- Did the data get corrupted ANYWHERE along the way?
- Will I know where it happened to fix the faulty item?

Attack, Information Breach, or Denial Points



Response Strategies

SNIA Storage Security Best Current Practices (BCPs)

- Core:
  - General Storage Security
  - Storage Systems Security
  - Storage Management Security
- Technology Specific:
  - Network Attached Storage (NFS & CIFS)
  - Block-based IP Storage (iSCSI & FCIP)
  - Fibre Channel Storage
  - Encryption for Storage
  - Key Management for Storage
  - Archive Security

Reference: www.snia.org/ssif/documents

Relevant BCPs

- General Storage Security
  - Stop Accidents, etc.
- Protect Storage Management
- Technology:
  - Encryption of Storage, FC, Block-based IP
    - Lost or distant media or data

Data Protection – Selected Use Cases

- Protecting Data At Rest (DAR)
- Protecting Data In-flight (DIF)
- End-to-End Security
  - Including Protecting Data Integrity
- For all: Importance of Authentication
  - Security Perspective!

Threats Mitigated Summary 1

Use Case	Threats Mitigated (see slide 8)
Host Based At Rest Network Based At Rest Device Based At Rest	**Accidental Corruption** **Sniffing for Confidential Data** **Media or Hardware Theft** **Unauthorized data moves, e.g. Cut and Paste** **Tampering with Data at Rest** **Destruction of Data** **Man in the Middle Attacks** **Unauthorized Access of Data (e.g. Data Copies)** **Disaster Recovery, Insecure Remote Data** **Unintended Disclosure of Data/Information** **Encryption Key Disclosure**

Threats Mitigated Summary 2

Use Case	Threats Mitigated (see slide 8)
Host Based Data Integrity	Accidental Corruption Destruction of Data Single Point of Failure (Natural Cause Denial of Service) Accidental Access or Changes Disaster Recovery, Insecure Remote Data
Data In Flight	Accidental Corruption, Destruction of Data Single Point of Failure (Natural Cause Denial of Service) Accidental Access or Changes Sniffing for Confidential Data, Sniffing for Identities Spoofing (i.e. Impersonation) Modify Packets, Inject Packets, Hijack Connections Destruction of Data Traffic Replay Attacks Man in the Middle Attacks Unauthorized Management or Maintenance Control Disaster Recovery, Insecure Remote Data Unintended Disclosure of Data/Information Encryption Key Disclosure Compromised discovery systems.

Authentication - Important!

Relevant Best Current Practices

- Use DH-CHAP for FC devices
- Use CHAP for iSCSI devices
- Use good User Passwords for human interfaces

- Stops – Spoofs of User Names, WWN's, iSCSI Names

Encryption - Where? Why?

Why Apply Encryption?

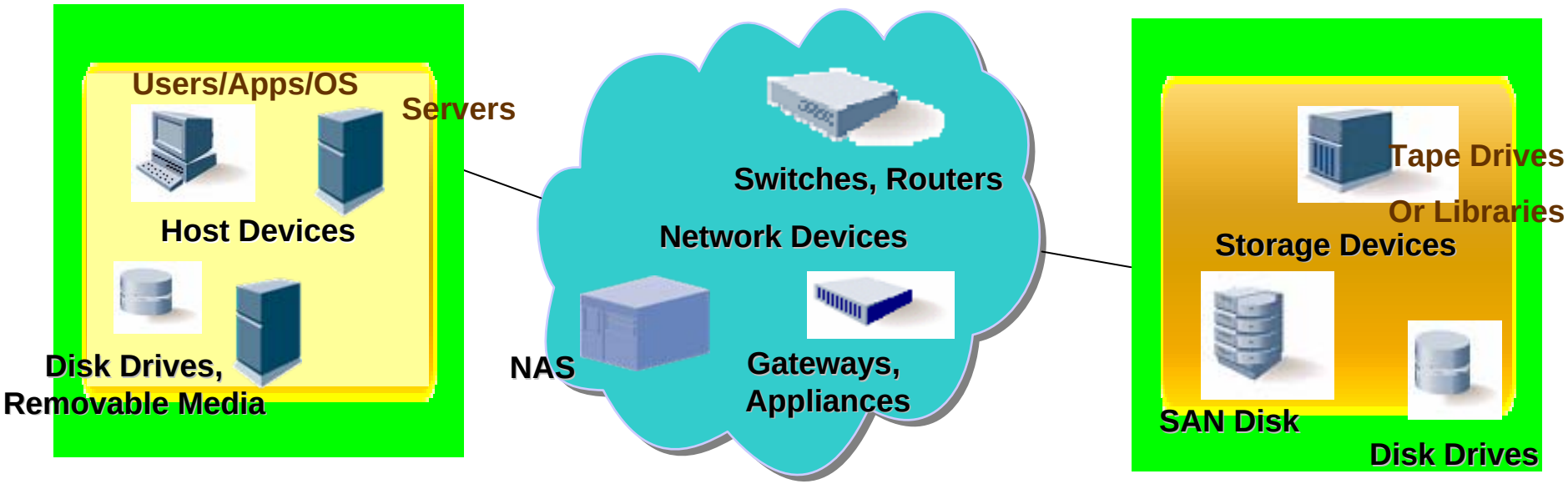
- Compliance or security?
  - Alternatives to encryption – examine your current practices
  - Cost and impact vs risk of doing nothing
  - Legal, ethical, or economic loss concerns are compelling
- Often times cryptographic solutions are deployed
  - After basic processes and access controls, such as user authentication
  - Can be more cost effective than the $ loss of data breaches
    - E.g. Notification expenses
  - Can help reduce likelihood of lost reputation due to data breaches
    - What is your corporate reputation worth?
  - Will it become so common that there is little reason or risk to not to use it?
  - Complicated systems make it more difficult to assess holes in coverage
  - To stay a step ahead of adversaries
- Keep in mind some challenges that may be encountered.
  - Performance
  - Combinations of technologies (DAR, DIF)
  - Key Management
  - Understanding differences in encryption modes
  - How and when to upgrade/migrate and potential disruption of existing practices

Where to Apply Encryption

- Depends on the **business drivers***
  - Depends on data confidentiality and integrity drivers
  - Depends on if security or compliance driven
  - Depends on if data classification and flow understood
- Depends on **the threats** to be mitigated
- Best practice from security perspective is to encrypt **as close to the information source** as possible

*Source: Encryption of Data at Rest Checklist www.snia.org

Points of Encryption



- Application Level
- File System Level
- Data Set/Volume Level
- Transport Level

- Network Level
- File System Level
- Transport Level
- Data Set/Volume Level

- Controller Level
- Data Set/Volume Level
- Device Level
- Transport Level

Use Cases

Storage System Layers and Likely Use Cases

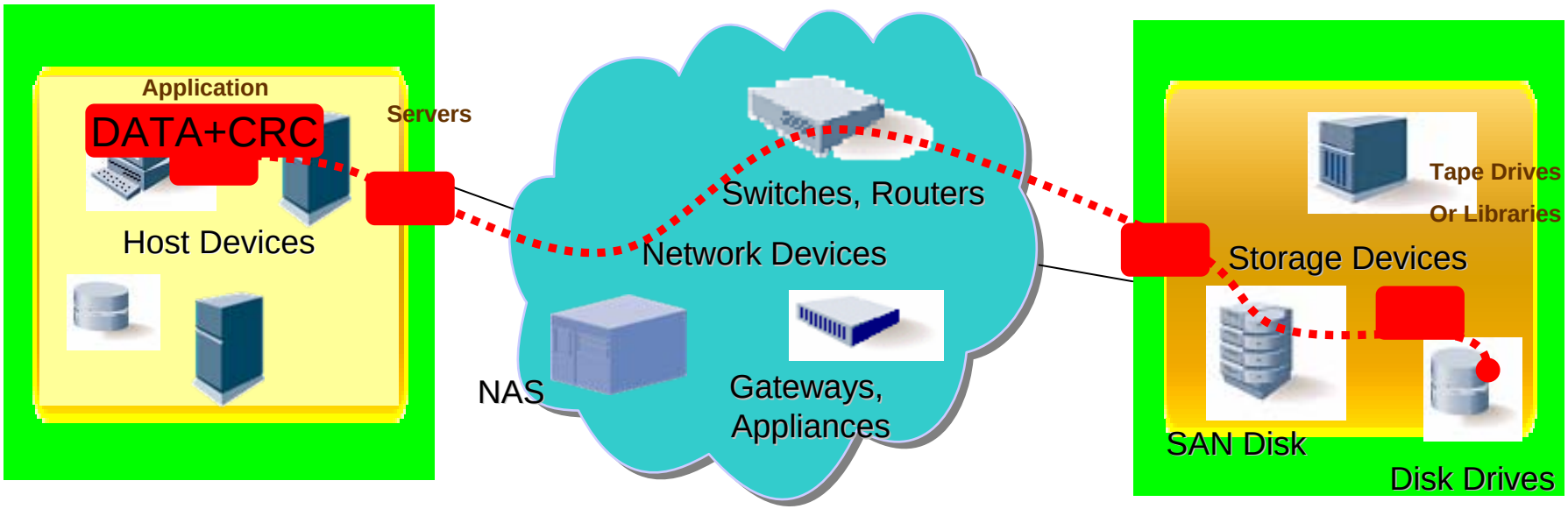
Applications	Data Integrity, Data At Rest, Data In Flight*
Server OS and File System	Data Integrity, Data At Rest, Data In Flight
Command Set (e.g. SCSI)	Data Integrity, Data At Rest, Data In Flight
Transport/Storage Network	Data Integrity, Data At Rest , Data In Flight
Storage Device	Data Integrity, Data At Rest, Data In Flight
Storage Media	Data Integrity, Data At Rest

Note: It depends on the application whether the coverage was meant to Cover Data At Rest or Data In Flight. (e.g. DB or storage applications)

Primary Use Cases - Overview

1. Data Integrity Protection at SCSI layer (Business case – data corruption.)
   - SCSI Protection Information end-to-end security
   - ILM or OSD Authenticated Integrity
2. Data At Rest Protection by Storage (Business case – Lost storage)
   - Tape Drive
   - Library
   - Disk Array
   - Full Disk Drive Encryption
3. Data At Rest Protection by Host End (Business case – Lost storage)
   - Software
   - Hardware
   - Local storage devices encryption (e.g. HDD, USB flash drives)
4. Data At Rest Protection By Network (Business case – Lost storage)
   - Switch or Appliance
5. Data In Flight Protection Point to Point (Business case –Lost or tampered data)
   - Within network
   - End point to End point across network
   - Hop by Hop End to End

Data Integrity Host to Storage Use Case



Examples:
SCSI Protection Information
OSD Integrity Fields

Primary Threats mitigated:

Accidental Corruption
Accidental Access or Changes
Single Point of Failure

PROS:
End to End

CONS:
Doesn't cover malicious attacks

T10 DIF Data Integrity Overview

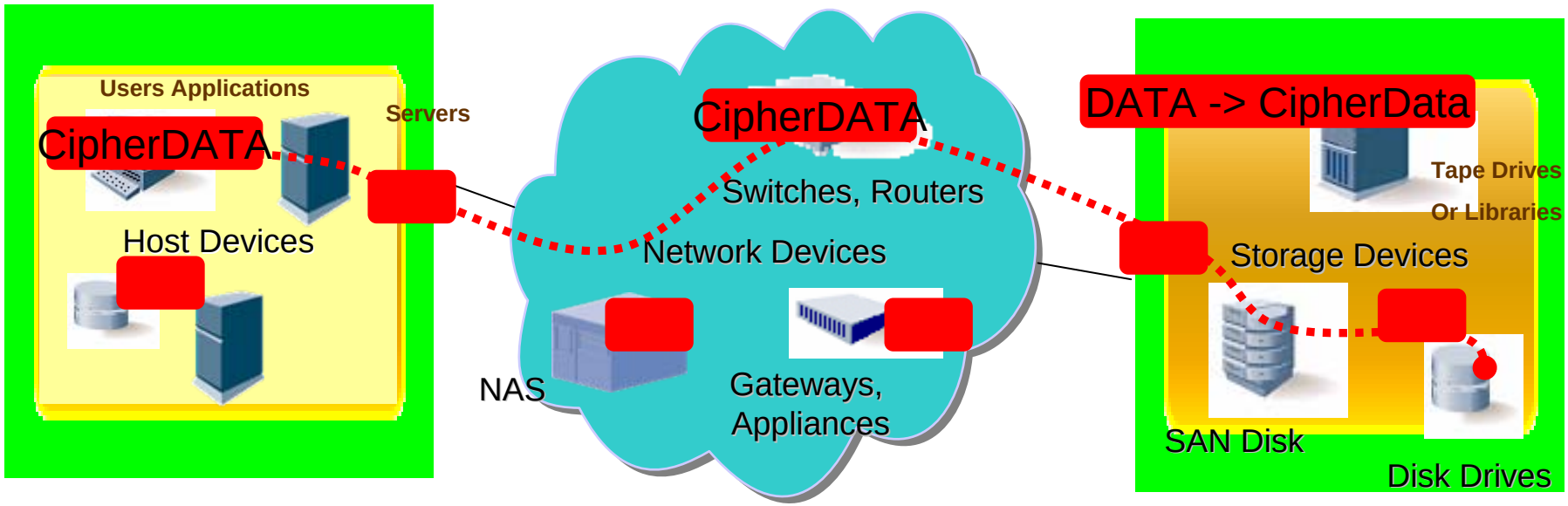
- May use SCSI Protection Information standard to attach a CRC to SCSI data, assuring integrity from end to end.
  - Implementation variations exist that, for example, strip and replace CRC as data progresses through the system.

  Reference: SCSI Block Commands (SBC – 2)
- ILM or OSD scheme
  - MetaData with Attributes associated to data objects (e.g. Confidentiality, Integrity)

  Reference: Information Technology – SCSI Object Based Storage commands

Note: SNIA Data Integrity Initiative task force recently formed.

Data At Rest Use Cases



Examples:
Encrypts SCSI I/O Commands Payloads or Data Files or Blocks and stores the data on the media, a la IEEE P1619.x.
Or encrypts the entire disk.

PROS:
Supports non-disclosure goals

Primary Threats mitigated:

Media or Hardware Theft
Unintentional Disclosure

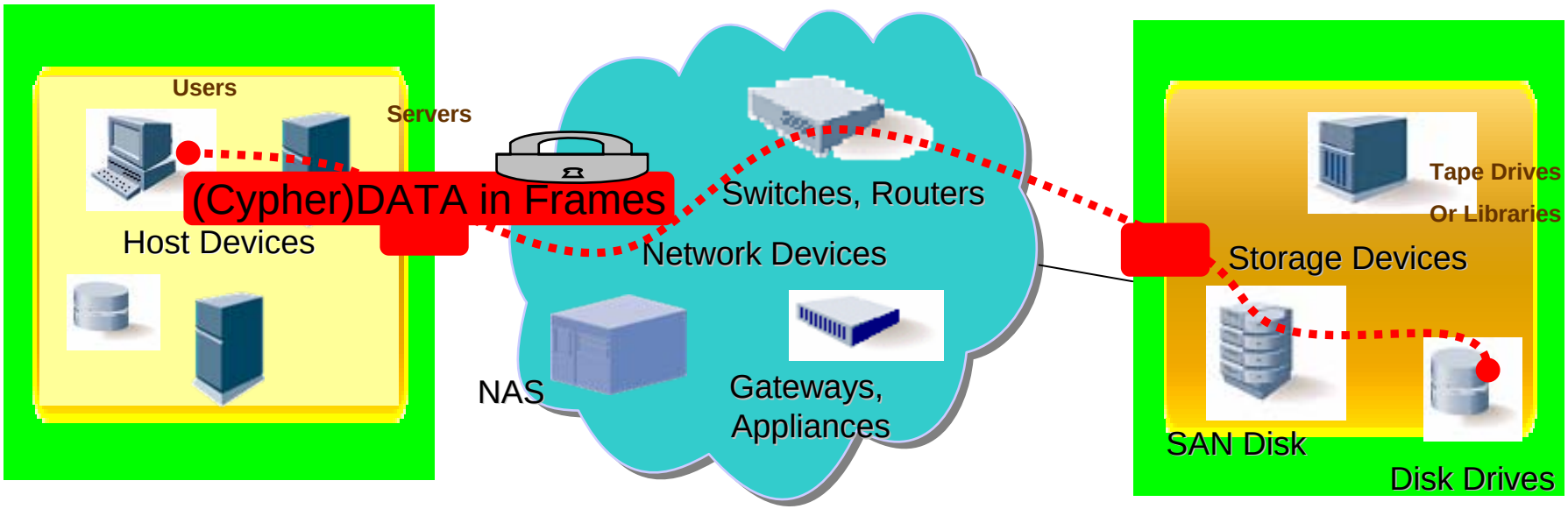
CONS:
May not address all in flight data risks

Various Data At Rest approaches

DAR Choices Overview

- Device Based
  - Tape Drives – IEEE P1619.1
  - Full encrypting Disk Drives – TCG
  - Encrypts SCSI I/O Commands Payloads or Data Files or Blocks and stores the data on the media, a la IEEE P1619.x.
- Network Based
  - NAS
  - Appliances or Switches – IEEE P1619 and P1619.1
- Host Based
  - Encrypting File Systems
  - IEEE P1619 and P1619.1 Supporting applications
- Many, many sub use cases and scenarios possible.
  - Acceleration
- The New Problem: Key Management

Data In-Flight Use Cases



Examples:
FC ESP_Header, IPSec, VPN's, Encrypts Transport Layer Frames, FC CT or IP Management Traffic w SSH, SNMPv3, SSL/TLS, at upper layers.

Primary Threats mitigated:

Sniffed or tampered data "on the wire"
Unauthorized disclosure of customer data in-flight

PROS:
Supports non-disclosure goals while data in motion.
Protects against malicious and non-malicious attacks

CONS:
Does not cover beyond point to point

In-flight point to point protection options

Data In-flight Choices

- FC Technology
  - FC ESP_Header w IKEv2
  - FC-SP
  - DH-CHAP or IKEv2 authentication
- IP Block Storage Technology
  - IPSec w ESP and IKE or IKEv2
  - IKE or IKEv2 authentication
  - iSCSI – CHAP authentication
  - FCIP – DH-CHAP authentication
- FC Management
  - FC CT Authentication and Confidentiality (Mgt and/or discovery)
  - Authentication on each message
- IP Management
  - SNMP3, SSH, TLS/SSL for Management traffic

NOTE: Authentication is critical to in-flight protection's usefulness!

You must know who/what you are talking to!

Is it Possible to Tie it all together?

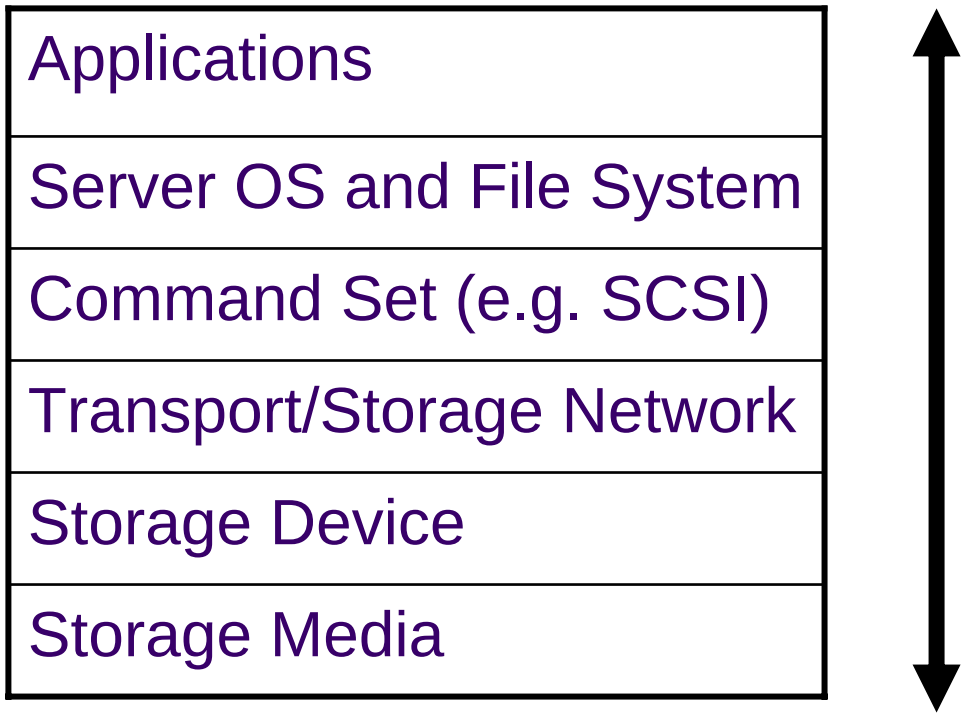
- Why would you use data integrity?
  - Your biggest concern is accidental corruption
  - Corruption has high impact, easy to relate to
  - Avoid bad publicity
- Why would you use data in-flight?
  - Your biggest concern is malicious attacks on the wire
  - Bad publicity and due diligence
- Why would you use data at rest?
  - Because everyone else is (just kidding)
  - Because theft of media is a real concern and attracts bad publicity
- Can I use them all together?
  - Today, fairly challenging to accomplish.
  - Much confusion on differences in technologies
  - Key management interoperability non-existent (DAR)
- Authentication is the foundation on which to build security!
  - RADIUS and AD are examples of how to centrally manage and tie in not only user authentication but also to prevent equipment spoofing.

Use Case Pros and Cons

Use Case	Pros and Cons
Host Based Data Integrity	Pros: End to End coverage. Cons: Generally protects against accidents only. May not cover Mgt traffic. (e.g. SCSI Prot.)
Host Based At Rest	Pros: Closest to data source. In-flight confidentiality. Supports non-disclosure. Cons: Large performance impact (software). Doesn't cover Mgt traffic.
Network Based At Rest	Pros: Closer to data source. Performance. Cons: Limited in-flight protection. Protects within the network only.
Device Based At Rest	Pros: Low scalability impact. Performance. Cons: No in-flight protection. No Mgt traffic.
Data In Flight	Pros: Malicious attack coverage. Performance (HW). End to End conf. and integrity coverage. Cons: End to End is Point to Point. Possible gaps.

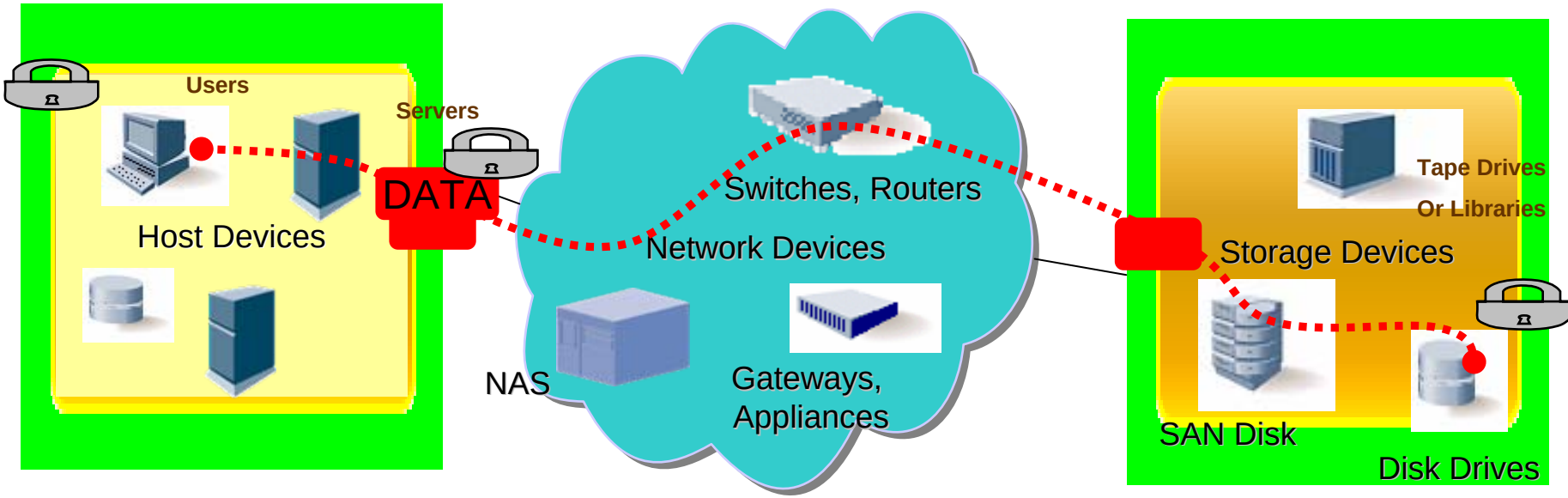
Goal:
End to End Comprehensive Security…

Ideally Would Like Coverage of All Layers



Is there anything today that completely covers all layers and all threats?
Unfortunately, no not really, but you can come close.
Layered protection still best practice.

Rationale for End to End Protection



- Remember the in-flight scenario?
- Let's back it up the stack a little… it becomes the data integrity scenario but… keep in mind the threat model.

End-to-End Data Protection Choices

- Where are the ends?
  - From Initiator source of information to Target end destination of information on writes
  - From target source of information to Initiator end destination of information on reads
  - **Application to Media - typically**
  - **Server to Storage Controller - typically**
  - Array
  - Gateways

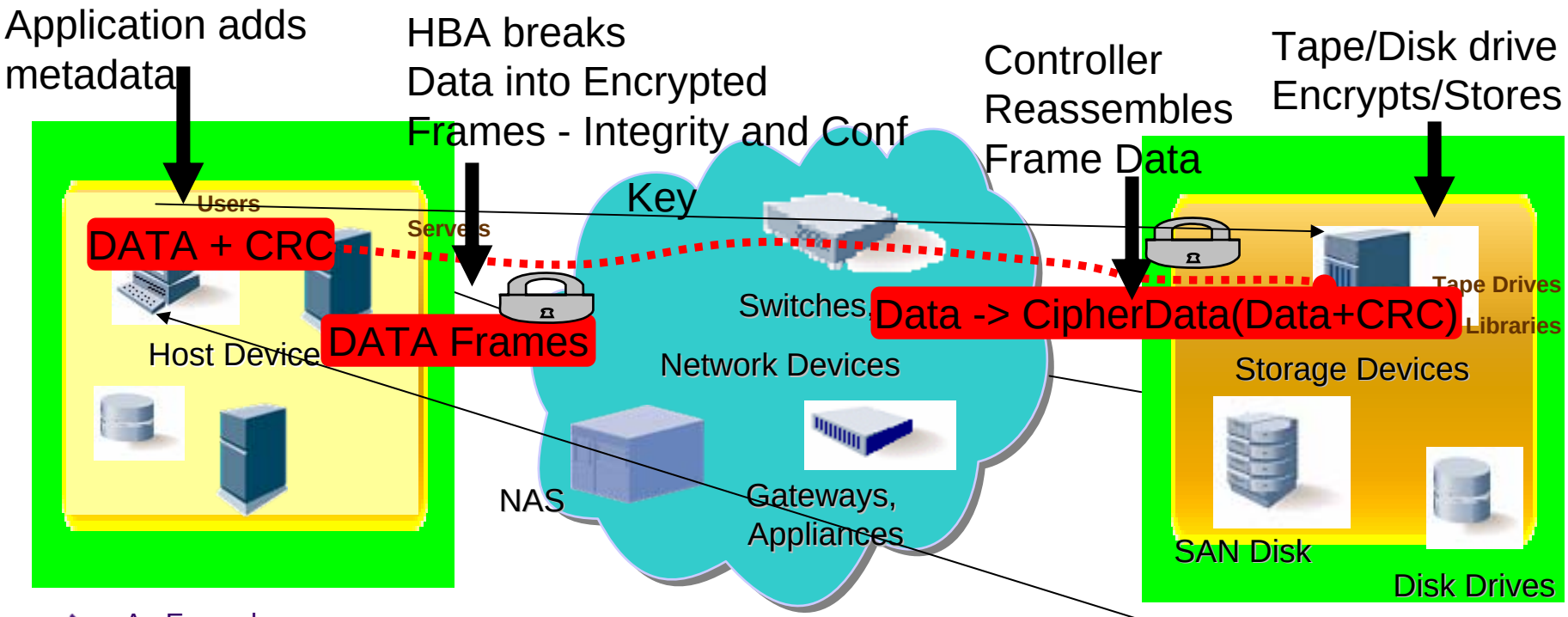
End to End Protection Support - Discussion

- Can you really trust the entire IP network or FC fabric?
  - Not the traditional security person's way of looking at network security
  - Physical security not always good enough
- Does the entire fabric or storage network fit inside the data center?
  - Not all the time (e.g. SSP's)
  - Topologies are many and varied
- What alternatives are there for distance or campus connections, of current primary concern?
  - FC, IP, iFCP, FCIP, ethernet
  - Distance Issues: Latency ~ 1msec/100km round trip, DWDM etc.
  - Security: IPSec, FC ESP_Header, FC CT_Auth, Ethernet layer protection
- Who is setting the company's in-flight storage data protection policy?
  - Varies: Storage Admin or Network Admin? Does the same person control the in-flight protection policy for the whole fabric? (e.g. virtual connections, virtual fabrics, multi-sites, multi-org)
  - Unlikely that one admin owns the entire infrastructure/topology
  - Virtual fabrics continuing to add to this separation of duties
  - Compliance driving orgs to minimal/separate knowledge of people
  - Unlikely to have consistent policies across management domains
- Is it easier to selectively protect end to end connections or protect an entire network ?
  - Entire fabric, versus, classifying/protecting only most important paths
- Should not rely solely on upper layers for security – defense in depth, etc.

Likely in-flight Use Case Configurations

- Some links leave Data Center
  - Outside Building (Campus, e.g. < 10Km)
    - FC – 100Km capable
    - IP - WAN distances
  - To a distant site
    - Many possible configurations/technologies
    - MAN (e.g. < 100Km), WAN (e.g. > 100Km)
    - Varied technologies - Ethernet/Gig E, ATM, IP, POS, DS3, Sonet, or FC
  - Varied valid network topologies
    - Gateway to Gateway
    - Router to Router
    - Switch to Switch
    - Selective Links to be protected End to End

One Example, Putting it All Together



- An Example:
  - Data Integrity appended to data by application (SCSI layer)
  - DH-CHAP Authentication between HBA and fabric (optionally using RADIUS)
  - DH-CHAP Authentication between switches
  - DH-CHAP Authentication to tape (or disk) controller
  - DH-CHAP Authentication between HBA and Disk Controller
  - Data in flight implemented using FC ESP_Header or IPSec (Frame transport layer) using session keys
  - Backup application sends key to tape drive using SCSI commands (Command layer)
  - Tape Drive encrypts data and puts it on media using key (Storage Device layer)
  - Key Management – only required for DAR
- End to End protection achieved!

Key

KMA

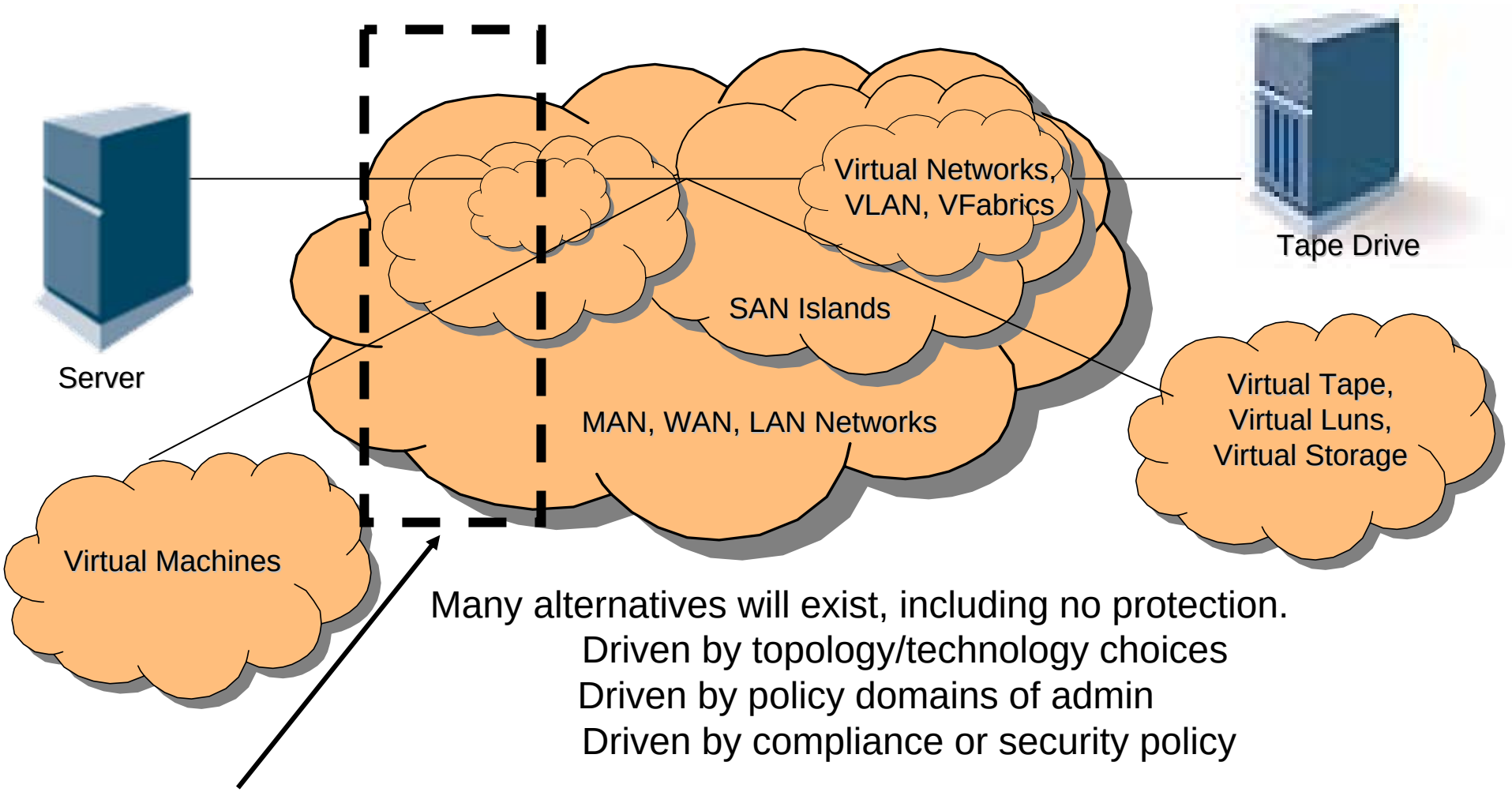
Key Produced By KM Server

Summary

Summary –

- There are many motivations for deploying data protection and privacy solutions
  - Many of which use cryptographic approaches
- There are many use cases to choose from
  - including multiple layers in the storage stack and
  - multiple locations in the topology
  - each with associated pros and cons
  - each addressing different threats
- The rationale for end to end data security shows it as a highly desirable approach to take
  - But not without its challenges (e.g. Knowing where the ends are, Virtualized environments)
- In the end, what really matters is that you've thought about the threats and why you are encrypting information and have a data protection and privacy strategy using encryption appropriately to help cover them.

Highly Virtualized Environments



Many alternatives will exist, including no protection.
- Driven by topology/technology choices
- Driven by policy domains of admin
- Driven by compliance or security policy

Considering physical protection boundaries (the dashed line that varies)

How to get involved

- T11.3 FC-SP-2 Work Group
  - Focus: Fibre Channel Security Protocols
  - http://www.t11.org - look under draft standards
- SNIA Security Technical Work Group (TWG)
  - Focus: Requirements, architectures, interfaces, practices, technology, educational materials, and terminology for storage networking.
  - http://www.snia.org/tech_activities/workgroups/security/

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

Larry Hofer, CISSP
Bob Nixon
Rob Peglar
Eric Hibbard, CISSP
Richard Austin, CISSP

Bibliography

- Introduction to Storage Security SNIA white paper
  - http://www.snia.org/ssif/documents/Storage-Security-Intro.051014.pdf
  - http://www.snia.org/ssif/documents
- INCITS 426-2007, Fibre Channel Security Protocols, FC-SP
- INCITS 427-2007, Fibre Channel - Generic Services 5, FC-GS-5
- IEEE P1619 Drafts http://www.siswg.net
- FCIP, RFC 3821 http://www.t11.org
- iSCSI, RFC 3720
- Securing Block Storage Protocols over IP, RFC 3723 http://www.ietf.org
- www.snia.org Encryption of Data At Rest, Checklist
- ANSI INCITS 408-2005, SCSI Primary Commands – 3 (SPC-3)
- ANSI INCITS 405-2005, SCSI Block Commands – 2 (SBC-2)
- ANSI INCITS 350-2003, Fibre Channel Protocol for SCSI, Second Version (FCP-2)
- ANSI INCITS 400-2004, SCSI Object Based Storage commands

THANK YOU

BACKUP SLIDES

Encryption Modes

- Just when you thought it was safe…
- You realize not all modes are created equal!
  - E.g. ECB, CBC, GCM, XTS, CCM
- Questions to ask:
  - NIST approved?
  - Performance?
  - Strength?
  - What threats does it address?
    - E.g. Authentication (tamper resistant) and confidentiality (private) or just confidentiality
  - Cost effective?