SNIA

Education

ABCs of Encryption

Roger Cummings, Symantec

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the 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.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

© 2009 Storage Networking Industry Association. All Rights Reserved.

Abstract

ABCs of Encryption

- Public disclosures of data "indiscretions" have become regular enough and embarrassing enough that many organizations are exploring encryption options to simply stay out of the headlines. Those who have ventured into this space quickly realize that there is no "magic crypto fairy dust" that will make the problems go completely away. However, with careful planning and judicious use of the right technologies, organizations can eliminate many of their exposures.

  This session focuses on the efforts required at the storage layer to create a successful encryption strategy. Major uses along with factors to consider are presented for protecting storage management, data in-flight, and data at-rest. The session provides expanded coverage on encrypting data at-rest, based on a step-by-step approach.

© 2009 Storage Networking Industry Association. All Rights Reserved.

Agenda

- Formal Definition of Important Terms
- BRIEF Encryption Background
- Storage-Related Encryption
- The SNIA Nine Step Checklist
  - How to implement encryption in YOUR organization
- To get involved….
- Best Practices
- Sources of additional information

© 2009 Storage Networking Industry Association. All Rights Reserved.

Important Terms

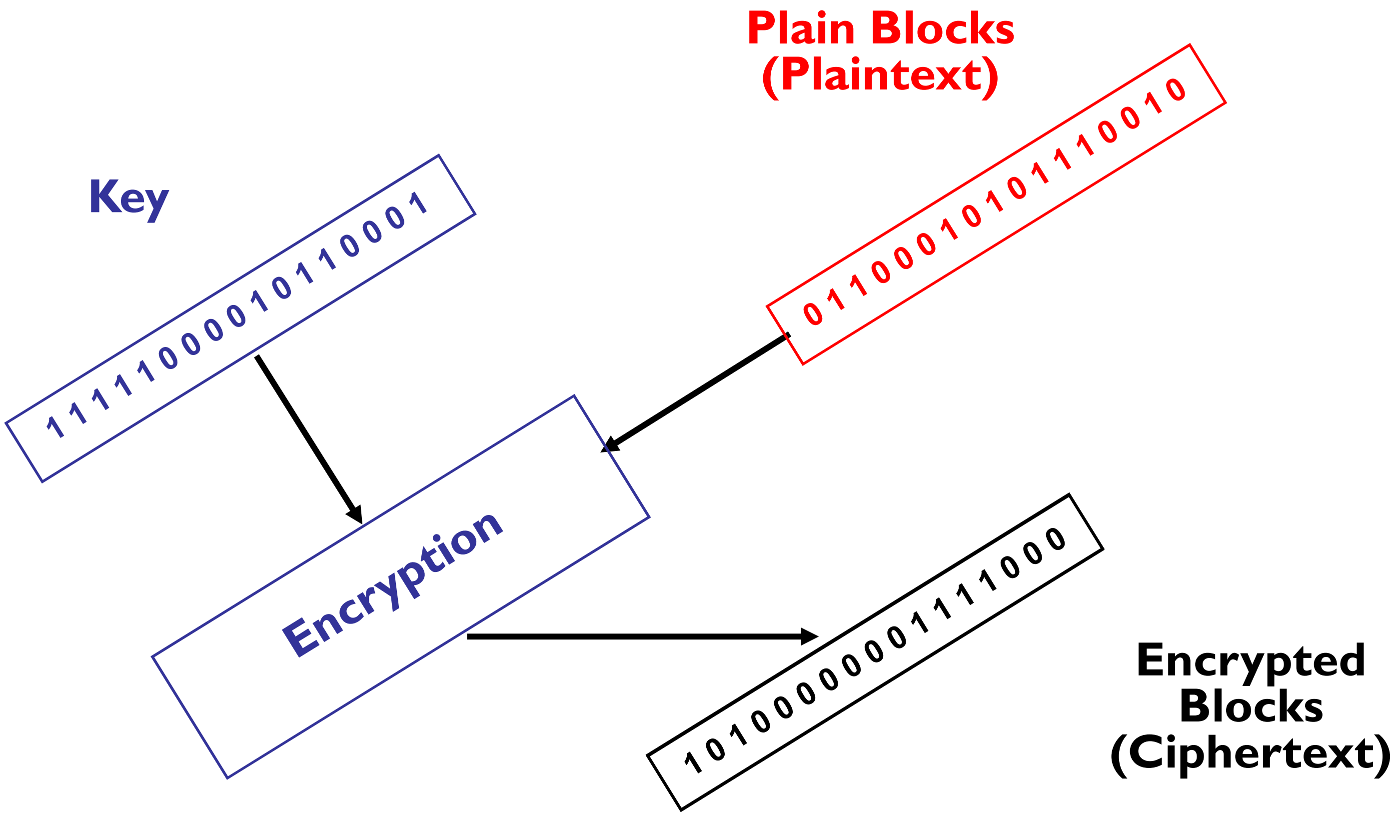
© 2009 Storage Networking Industry Association. All Rights Reserved.

A Few Formal Definitions

- **Plaintext** – Original information (intelligible) that is used as input to an encryption algorithm (cipher).
- **Ciphertext** – The encrypted (unintelligible) output from an encryption algorithm.
- **Encryption** – The conversion of plaintext to encrypted text with the intent that it only be accessible to authorized users who have the appropriate decryption key.
- **Cipher** – A mathematical algorithm for performing encryption (and the reverse, decryption).
- **Key** – A piece of auxiliary information used by a cipher during the encryption operation.

© 2009 Storage Networking Industry Association. All Rights Reserved.

Encryption Scheme Concept



© 2009 Storage Networking Industry Association. All Rights Reserved.

Encryption Background

(Warning – uses analogies)

(Any cryptographers present might want to tune out for a while)

© 2009 Storage Networking Industry Association. All Rights Reserved.

Encryption is…..

- Exactly what we knew as “secret writing” when we were kids
  - Remember the “magic decoder rings” given away in the comics?
    - ABCDEFGHIJKLMNOPQRSTUVWXYZ
    - DEFGHIJKLMNOPQRSTUVWXYZABC
  - Replace the letter in top line by the one underneath (substitution)
  - Reverse the order of the letters in the message (transposition)
- The above scheme is known as the Caesar Cipher
  - Reputed 1st used by Julius Caesar during the Gallic wars
- Arguably there have only been two major advances since the time of Caesar
- Cryptography (Greek “cryptos" (hidden) + "graphia" (writing))

© 2009 Storage Networking Industry Association. All Rights Reserved.

Principles (or lack thereof)

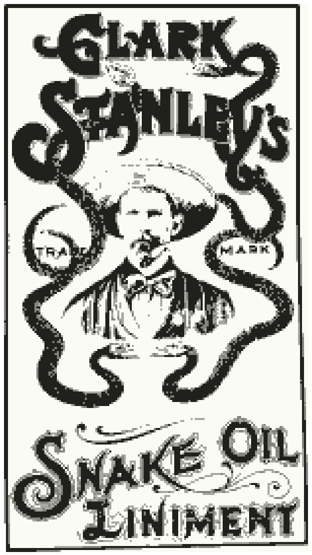
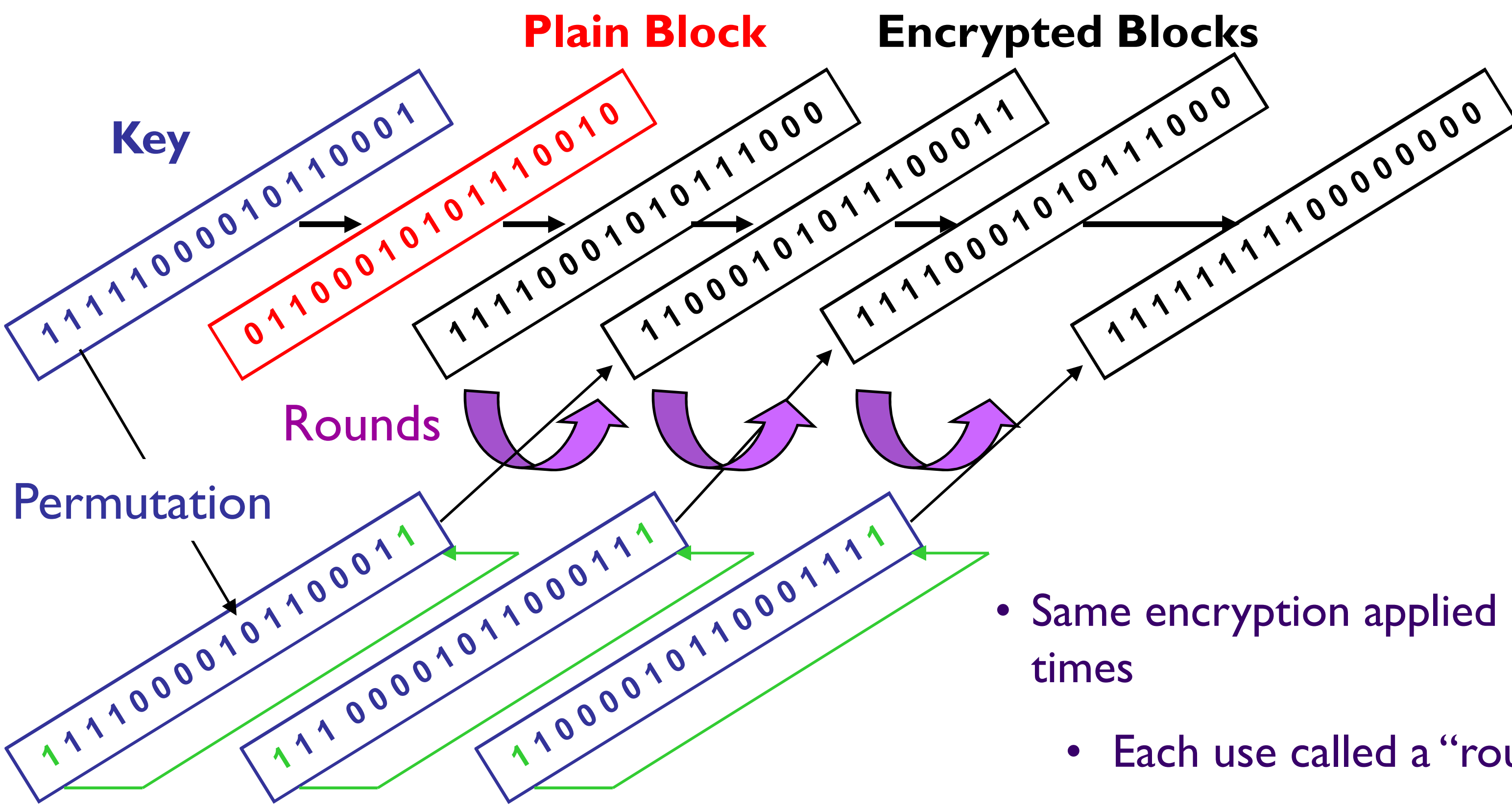


Image courtesy Wikipedia

- Kerckhoffs Principle (1883)
  - Only the key needs to be secret; there should be no secrecy in the algorithm
- Encryption is empirical science
  - We know a scheme is strong ONLY because it hasn't been broken yet…..
  - And have reasons for believing it's unlikely to be broken in a specific period using known or anticipated technology
- Use only published & proven schemes
  - And beware of snake oil!

© 2009 Storage Networking Industry Association. All Rights Reserved.

First Advance - Mechanization



- Same encryption applied multiple times
  - Each use called a "round"
  - Cryptographic "mode" defines how output of one round becomes input of another

To see the difference a mode can make, go to
http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

© 2009 Storage Networking Industry Association. All Rights Reserved.

Second Advance - Asymmetry

Education SNIA

- All previous encryption schemes were "symmetric"
  - Same key used to encrypt & decrypt
  - Thus key had to be distributed to both parties before communication could take place
- Major advance developed in the 1970s in area of key distribution
  - Based on "one way" mathematical functions
    - Not easy to determine the starting point from the result
  - Solved shared key "chicken & egg" problem
    - Now two parties that had never communicated before could do so securely
- First practical scheme was Diffie-Hellman Key Agreement
  - But it required a number of handshakes
    - Improved by RSA asymmetric cryptography

© 2009 Storage Networking Industry Association. All Rights Reserved.

Analogy

Education SNIA

- Chechen postal service said to be corrupt
  - Anything valuable sent in unlocked box is stolen
- How can Ramzan in Grozny send a valuable antique to Madina in Argun who he's never met?
  1. He puts the valuable antique in a box and sends it locked with his padlock
  2. She attaches a padlock of her own and sends it back
  3. He removes his padlock and sends the box back again
  4. She opens the box (had never been opened in public previously)
- Could be a single step process IF Ramzan could get a "Madina lock" i.e. a lock that can be opened with a key that Madina already has, from his local post office
  - Important question - how & why should Ramzan trust the post office to give him the right thing?

© 2009 Storage Networking Industry Association. All Rights Reserved.

Asymmetric Cryptography

- Two keys, one Public, one Private
- What one encrypts, the other can decrypt
  - And vice versa
- Cannot feasibly calculate one key given the other
- Also called Public Key Infrastructure (PKI) Cryptography
  - Because needs a TRUSTED infrastructure to distribute the public keys

© 2009 Storage Networking Industry Association. All Rights Reserved.

Hashing

- Hashing does not encrypt data, but provides transformation used to verify data integrity
  - Hash algorithm digests data and represents its bits and bit patterns by fixed-size equivalent - a Hash Value
    - Size of the value is fixed by the algorithm (SHA-1 is 20 bytes)
    - Algorithm is non-reversible: cannot reproduce data from hash
    - Single bit change in data may change half of the bits in hash
- Does not require the use of keys
  - But related construct called Message Authentication Code (MAC) uses a hash derived from both data & a secret key
    - HMAC is the best known – see IETF RFC 2104, FIPS PUB 198
- A hash may also be used in a "digital signature" scheme

© 2009 Storage Networking Industry Association. All Rights Reserved.

Summary

Education SNIA

- The basics of cryptography have been known since the time of the Greeks & Romans
  - Same basic mechanisms have been used throughout that time
  - History gives us a good basis for understanding what's practical today
- Modern block ciphers use large alphabets and keys
  - Mechanization provides multiple substitutions and transpositions in series to add strength
- Asymmetric cryptography is a truly revolutionary advance
  - Too compute-intensive for bulk data operations
  - But VERY useful for distributing keys

© 2009 Storage Networking Industry Association. All Rights Reserved.

Some people change when they see the light, others when they feel the heat.

Caroline Schoeder

© 2009 Storage Networking Industry Association. All Rights Reserved.

Storage-Related Encryption

© 2009 Storage Networking Industry Association. All Rights Reserved.

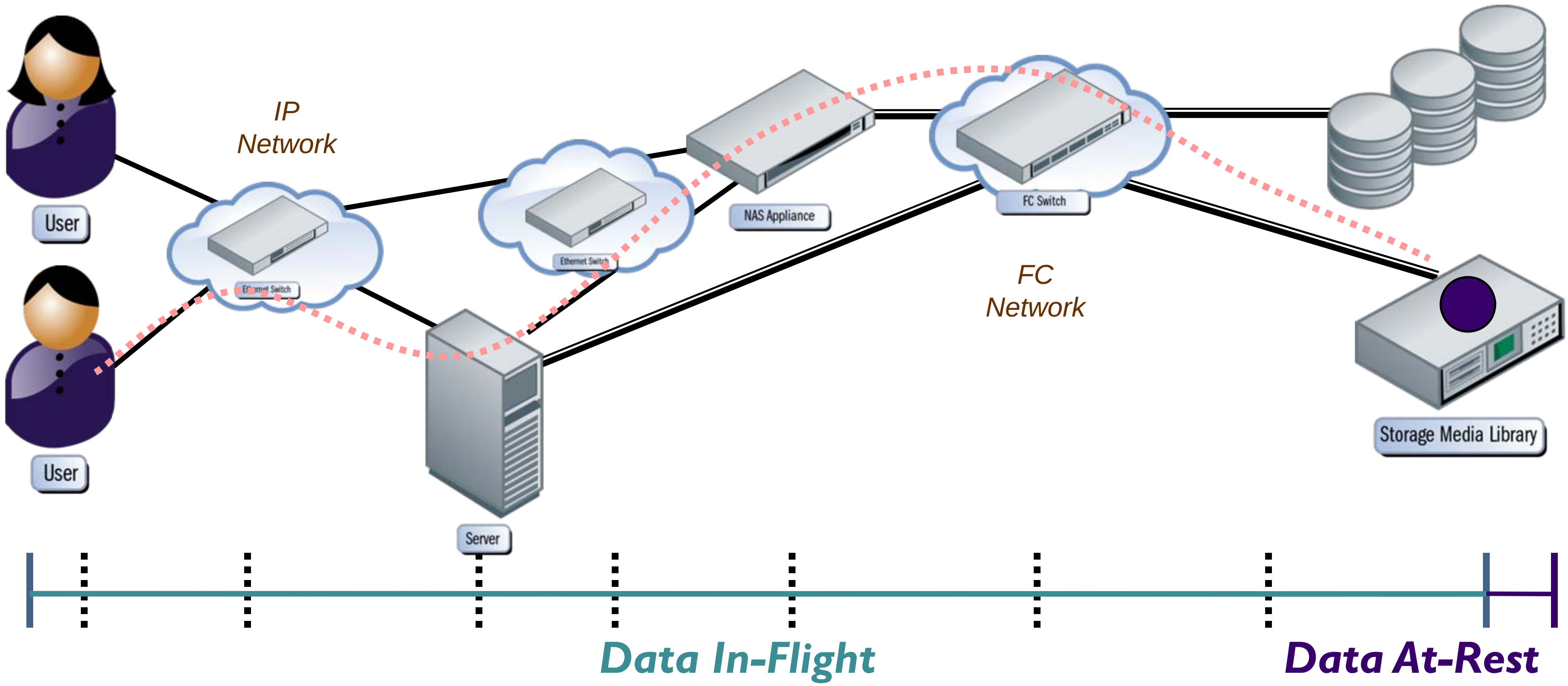
You will probably have read about….

Education SNIA

- A lot of storage security product announcements addressed at preventing repeats of past data "indiscretions"
  - Fueled by "lost tapes" & "lost laptop" scenarios
- A lot of confusion about data "in-flight" versus data "at-rest" security
- Issues with keys & related difficulties
  - Human involvement (e.g. policy creation, cross-group interaction) the source of much difficulty

© 2009 Storage Networking Industry Association. All Rights Reserved.

In-Flight versus 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
  - Plaintext to L, Ciphertext to R

Yes, the term is a misnomer because media moves!

© 2009 Storage Networking Industry Association. All Rights Reserved.

Data At-Rest

- Encryption/decryption built into tape drives
  - Encryption AFTER compression (to keep usual ratio)
  - Key not stored on the media or retrievable from drive
    - Key-associated data to help in “found tape” case
  - Tape-to-tape copy without decryption being worked
- Encryption/decryption built into disk drives
  - Data encrypted before storing on media, decrypted when read
  - Can probably be reset by extraordinary means in field
    - But will certainly wipe all existing data
  - Defined by Trusted Computing Group (TCG)
- Encryption/decryption built into SSD or Flash drives

Check out SNIA Tutorial:

Self-encrypting drives

© 2009 Storage Networking Industry Association. All Rights Reserved.

Data In-Flight

Education SNIA

- Technology differs by “transport”
  - Block-level IP protocols
    - IPsec for iSCSI, iFCP, FCIP
  - Block-level, FC protocols
    - FC-SP, ESP_Header, CT protection
  - File-level, IP protocols
    - IPsec for NFS & SMB/CIFS
    - SSL/TLS for WebDAV
  - Management protocols
    - SSL/TLS or SSH for SMI-S, SNMPv3, web-based mgmt
- IPsec & TLS largely proven
  - Widely deployed for VPNs, less so for traffic inside the corporate firewall
- SCSI Command Sets now also incorporate protection mechanisms (e.g. ESP-SCSI)

© 2009 Storage Networking Industry Association. All Rights Reserved.

Both In-Flight & At-Rest

- Host Bus Adapter- & Array Controller-based encryption
- Security appliances & switch-based encryption
  - Most also compress data before encryption (to keep historical efficiencies)
  - Also include key management functions
- Applications with encryption features
  - Many have been around for quite a while!
- New OS offerings & encrypting file systems
- New NAS & CIFS products will emphasize security
  - Some have purpose-designed cryptographic schemes
- Remember – all encryption points have to be authenticated & provisioned with keys

© 2009 Storage Networking Industry Association. All Rights Reserved.

Summary

- New storage products with data encryption are becoming available that address major users concerns
  - Based on industry standards, utilizing new features in SCSI and ATA interfaces and command sets
- Next we'll describe a Checklist defines the tasks you need to complete to best utilize these products in your organization
  - But also see the Best Practices for a more in-depth treatment of the situation

Check out SNIA Tutorial:

SNIA Storage Security Best Practices

© 2009 Storage Networking Industry Association. All Rights Reserved.

The SNIA Nine Step Checklist

(available @ http://www.snia.org/forums/ssif/knowledge_center/white_papers/)

© 2009 Storage Networking Industry Association. All Rights Reserved.

Introduction

- Step-by-step listing of tasks to be performed to effectively implement at-rest data encryption
  - Defines a process, not a single activity
  - Not all substeps will be needed in all cases, but they all merit consideration
- SNIA checklist document contains annexes with useful additional checklists related to security & encryption from:
  - Federal Financial Institutions Examination Council (FFIEC)
  - Information Systems Audit and Control Association (ISACA)
  - Payment Card Industry (PCI) Data Security Standard (DSS)

© 2009 Storage Networking Industry Association. All Rights Reserved.

The Steps

1. Understand Drivers
2. Classify Data Assets
3. Inventory Data Assets
4. Perform Data Flow Analysis
5. Choose Points-of-Encryption
6. Design Encryption Solution
7. Begin Data Re-Alignment
8. Implement Solution
9. Activate encryption

© 2009 Storage Networking Industry Association. All Rights Reserved.

#1 Understand Drivers

- Identify regulatory obligations (Sarbanes-Oxley, HIPAA, PCI DSS, EU Data Privacy etc.)
- Identify legal obligations
  - Review recent audits & any legal interactions
- Are there relevant "due care" mandates, national security concerns?
- Talk with executive management re concerns
  - Express everything in monetary impact
  - Real ones are the ones that get funded!
- Look @ corporate policies & IS/IT strategic plans

© 2009 Storage Networking Industry Association. All Rights Reserved.

#2 Classify Data Assets

- For the most part you cannot afford to encrypt everything
- Use coarse classifications to start
  - e.g. High Value to the Organization, Most Sensitive, Regulated
  - … and refine over time
- Determine confidentiality priorities & categories

© 2009 Storage Networking Industry Association. All Rights Reserved.

#3 Inventory Data Assets

Education SNIA

- For each category determine
  - Systems that transfer the data
  - Applications that process the data
  - Devices used to store the data
  - Networks used to transfer the data
    - Specifically those that leave the data center
  - Groups & people that own and are dependent on the data
- Perform risk analysis (unauthorized disclosure or deletion, loss of control etc.)

Check out SNIA Tutorial:

Securing the Cloud: Using Storage Services …

© 2009 Storage Networking Industry Association. All Rights Reserved.

#4 Perform Data Flow Analysis

- Look for temporary as well as permanent storage locations
  - And consider remote sites as well as the local one
- Don’t forget data protection schemes & archives
  - Where’s that device mirrored or replicated?
  - How are backups handled?
  - CDP or a DR/BC scheme to be considered? DLP?
- Also consider the impact of data reduction
  - Where is data compressed?
  - Where is deduplication performed?

© 2009 Storage Networking Industry Association. All Rights Reserved.

#5 Choose Points-Of-Encryption

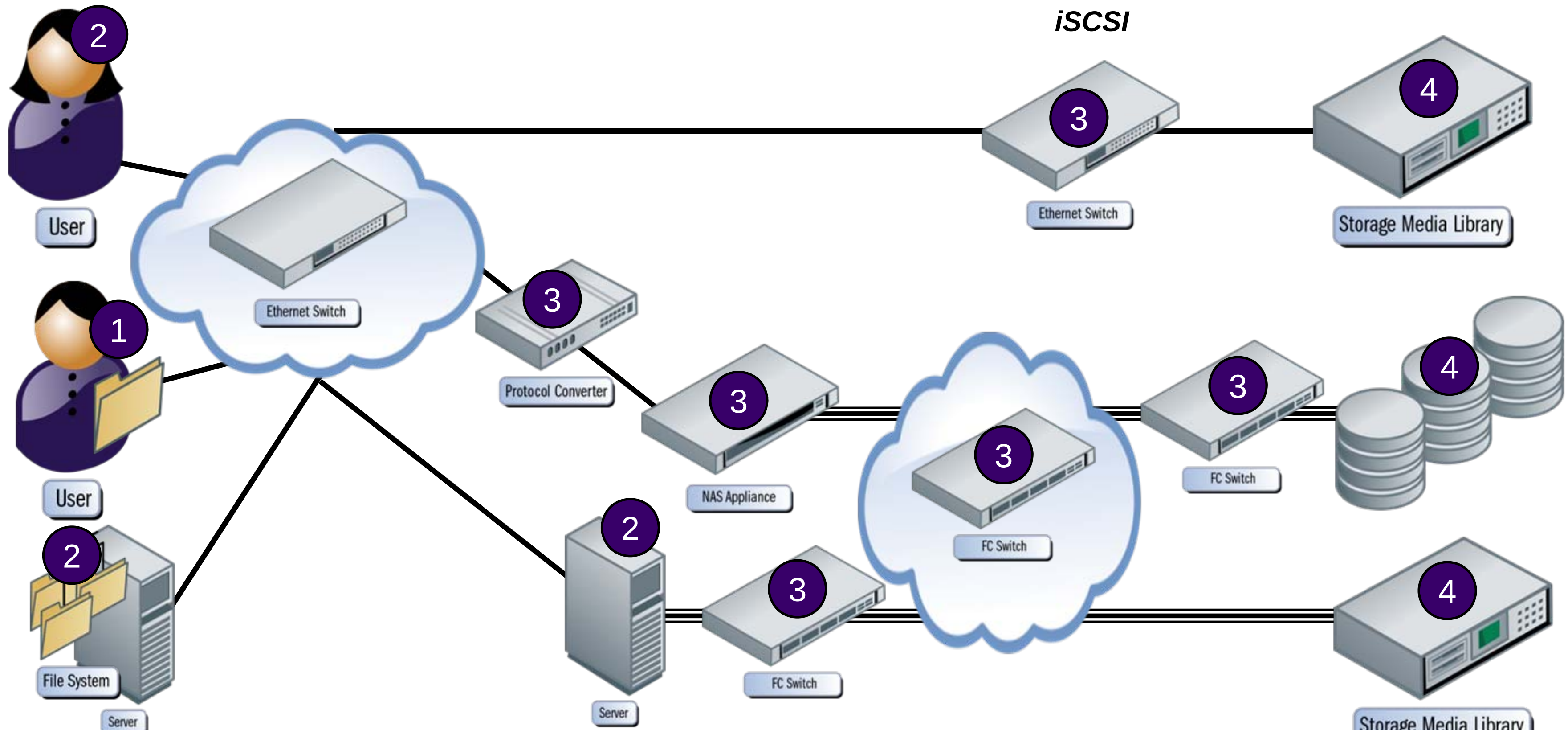
- Security Perspective:
  - Encrypt as close to source as possible (& get more protection per $!)
- Points of Encryption reprise:
  - Application-level – under the control of specific app or DB; finest granularity of control & max insight into data (type, users, sensitivity)
  - Filesystem-level – under the control of OS or OS-level app; control at file-level with insights into users
  - HBA-, Array Controller- or Switch-level – under control of the network
    - File-based (NAS) – control at share/filesystem-level (possibly file-level) with moderate insights into users
    - Block-based – control at logical volume level with limited or no insights in the "community of users"
  - Device-level – under the control of end-device; control at physical volume level with limited insights into "community of users"

© 2009 Storage Networking Industry Association. All Rights Reserved.

Points-of-Encryption

Education SNIA

In-Flight vs At-Rest ??



1 Application-level	3 HBA-, Array Controller- or Switch-level
2 Filesystem-level	4 Device-level

© 2009 Storage Networking Industry Association. All Rights Reserved.

#6 Design Encryption Solution

Education SNIA

- Documentation is key here!
- What's the impact on performance and/or operational effectiveness?
  - Set the right expectations
- Define a framework
  - Address key management structure – particularly where managed, how communicated, who's responsible
    - Consider impact of import/export/re-export controls

Check out SNIA Tutorial:

Intro to Key Mgmt for Secure Storage

© 2009 Storage Networking Industry Association. All Rights Reserved.

#6 Design Encryption Solution

- Imagine having to demonstrate to an auditor (or prove to your legal department) that:
  - The media containing the information was correctly encrypted
  - You’ve been in complete control of the key used since the media was created.
- Do you collect the information necessary to do this?
  - Can you prove the authenticity & integrity of that information?

Check out SNIA Tutorial:

How E-Discovery Will Impact Your Life as a Storage Professional

© 2009 Storage Networking Industry Association. All Rights Reserved.

#7 Begin Data Re-Alignment

- Previous steps will probably require migration of data between devices and/or networks
  - Bandwidth & latency will change
    - Not everyone will be happy
  - May require infrastructure (& virtualization) changes to address issues
    - If so, do it now BEFORE going further
  - Don’t forget to change data protection schemes (& CDP, DLP, compression, deduplication etc.) as well
    - Frequencies may change
    - New platforms may need to be utilized

© 2009 Storage Networking Industry Association. All Rights Reserved.

#8 Implement Solution

- Determine approach to solution (outsourced, phased etc.)
- Create a rollback plan in parallel with determining the approach!
- Select technology & acquire components
- Deploy and integrate with key management
- Integrate with authentication, audit logging, directory services (access control)
  - Secure timestamp source very important

© 2009 Storage Networking Industry Association. All Rights Reserved.

#9 Activate Encryption

Education SNIA

- Activate encryption? NO, not quite yet!
- First get management signoff
  - Outside accreditation might be a good idea
- Complete final data realignment (if needed)
- Run some "point tests" to prove that the data can be processed & recovered & results can be audited
  - Makes sure the right keys are available & logs working
- Might need to encrypt existing data in background first
- Only THEN turn encryption on for all active data

© 2009 Storage Networking Industry Association. All Rights Reserved.

So you're done, right?

- Still need to perform regular point tests
  - Don't rely on users to detect problems for you
- Regularly audit the logs to ensure all relevant information being captured
  - When the external auditors are coming next week it's too late to find out that info hasn't been captured
- Start to consider the security of the "fixed" content separately

Check out SNIA Tutorial:

Retaining Info for 100 years

© 2009 Storage Networking Industry Association. All Rights Reserved.

Summary

- A number of secure storage products are now available
  - Based on industry standard definitions!
- Addressing major concerns by use of storage security becomes feasible for the first time
- Encryption within a SAN or a storage device is only one part of a total solution
  - You'll need multiple "layers" for fully effective protection i.e. defense in depth
  - You'll need a wider scope than just storage security to satisfy regulatory obligations (e.g. PCI DSS)
- This tutorial has:
  - Defined the terminology
  - Introduced the underlying protocols & approaches
  - Laid out a process to follow when fielding storage security products

© 2009 Storage Networking Industry Association. All Rights Reserved.

Education SNIA

To Get Involved..

© 2009 Storage Networking Industry Association. All Rights Reserved.

SNIA Security

- 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
- Storage Security Industry Forum (SSIF)
  - Focus: Marketing collateral, educational materials, customer needs, whitepapers including the BCPs & Encryption of Data At-Rest (a Step-by-Step Checklist)
  - http://www.snia.org/forums/ssif

© 2009 Storage Networking Industry Association. All Rights Reserved.

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

Eric A. Hibbard, CISSP, CISA	**Jim Norton**
Andrew Nielsen, CISSP	**Richard Austin, CISSP**
Larry Hofer, CISSP PE	**Scott Kipp**
Blair Semple, CISSP-ISSEP	
Roger Cummings	
SNIA Security TWG	**SNIA SSIF**

© 2009 Storage Networking Industry Association. All Rights Reserved.

For More Information

© 2009 Storage Networking Industry Association. All Rights Reserved.

Storage Security Standards Orgs

Education SNIA

- ISO/IEC JTC1 SC27 – IT Security Techniques (www.iso.org/iso/iso_technical_committee?commid=45306)
  - US group is ANSI/INCITS CS1 (cs1.incits.org)
- NIST/CSD Computer Security Resource Center (csrc.nist.gov) – Security standards for US Government
- IEEE/P1619 (siswg.net) – Security in Storage Working Group
- ANSI/INCITS T10 (www.t10.org) – SCSI security, tape drive encryption control etc.
- ANSI/INCITS T11 (www.t11.org) – Fibre Channel security (FC-SP)
- IETF (www.ietf.org) – IP security (IPsec), Transport Layer Security (TLS)

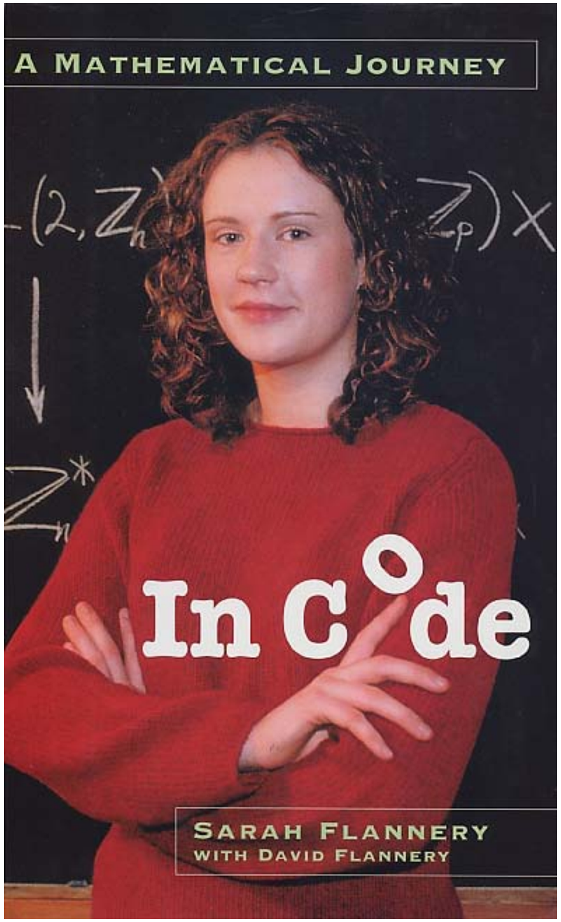
© 2009 Storage Networking Industry Association. All Rights Reserved.

Web Sources of Information

- The CERT® Coordination Center, http://www.cert.org
- The SANS (SysAdmin, Audit, Network, Security) Institute, http://www.sans.org
- The Center for Internet Security (CIS), http://www.cisecurity.org
- Information Systems Audit and Control Association (ISACA) – *IS Standards, Guidelines, and Procedures for Auditing and Control Professionals*, http://www.isaca.org/standards/
- Information Security Forum (ISF) – The Standard of Good Practice for Information Security, http://www.isfsecuritystandard.com/

© 2009 Storage Networking Industry Association. All Rights Reserved.

Maths Reference



ISBN 1-565123-77-8

- The story of an Irish schoolgirl's science project
  - That won Ireland's 1999 Young Scientist of the Year award!
  - An asymmetric cryptography scheme based on matrix multiplication
    - Turned out to be insecure, but so what!
- A simple introduction to the maths underlying cryptography
  - And a great story in general

© 2009 Storage Networking Industry Association. All Rights Reserved.