Education

SNIA Storage Security Best Practices

Eric A. Hibbard, CISSP, CISA, ISSAP, ISSMP, ISSEP, SCSE
Hitachi Data Systems

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.

Abstract

SNIA Storage Security Best Practices

With the increasing importance and emphasis on security in mind, the Storage Networking Industry Association (SNIA) had developed and published a set of storage security best current practices (BCPs). This vendor neutral guidance has a broad scope, covering both storage systems and entire storage ecosystems. Specific elements include, but are not limited to, storage management, protocols, compliance, encryption, key management, and long-term archive. This session provides an introduction to the BCPs as well as information that that will help organizations exploit the BCPs in their own environments.

The Dilemma

- Organizational IT governance rarely extends to storage ecosystems
- Risk is often not appropriately factored into storage ecosystem decisions
- Storage ecosystems have emerged in isolation with a focus on data availability and resiliency
- Data traceability is challenging and rarely done
- Auditors and security professionals frequently treat storage ecosystems as nothing more than direct-attached storage

Why Does this Matter?

- Organizations live and die based on the availability and integrity of their data
- Mishandling of sensitive data can result in severe consequences
- Organized crime has discovered that cyber crime is more profitable (and safer) than drug trafficking
- Data is no longer safely tucked away behind servers; it may be readily available

Anatomy of Data Breaches

- Threat categories (% breaches / % records)
  - Hacking 64% / 94%
  - Malware 38% / 90%
  - Misuse 22% / 2%
  - Deceit 12% / 6%
  - Physical 9% / 2%
  - Error (cause) 1% / 0%
  - Environmental 0% / 0%

- Who is behind data breaches?
  - 74% resulted from external sources
  - 20% were caused by insiders
  - 32% implicated business partners
  - 39% involved multiple parties

91% of all compromised records were linked to organized criminal groups.

Errors contributed to or enabled 67% of all successful attacks.

Source: 2009 Data Breach Investigations Report

What is Storage Security?

- Technical controls, which may include integrity, confidentiality and availability controls, that protect storage resources and data from unauthorized users and uses.

  – SNIA Dictionary

- ***Convergence*** of the storage, networking, and security.

- Simply a part of ***Information Assurance***
  - Measures that protect and defend information and systems
  - Encompasses system reliability and strategic risk management
  - Provides for restoration of information systems using protection, detection, and reaction capabilities

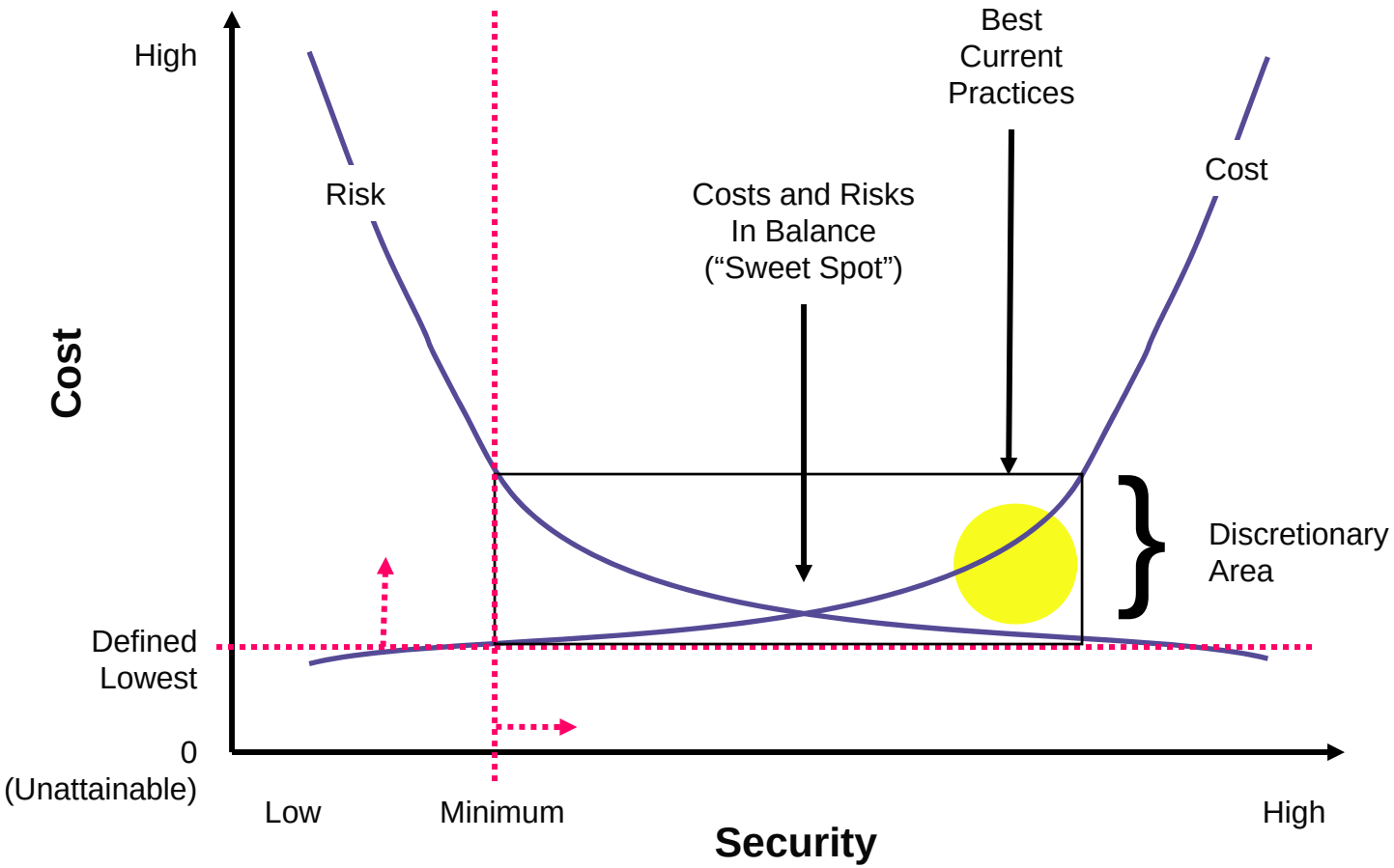
See Also: SNIA Technical Proposal, *Introduction to Storage Security, v2.0*, © 2009, http://www.snia.org/forums/ssif/knowledge_center/white_papers/

What are Best Practices?

- Best practice is an idea that asserts that there is a technique, method, process, activity, incentive or reward that is more effective at delivering a particular outcome than any other technique, method, process, etc. - Wikipedia

- For the purpose of the SNIA storage security best practices, they provide broad guidance to organizations seeking to secure their individual storage systems as well as their storage ecosystems.

Balancing Cost & Security



Source: Ray Kaplan, CISSP, *A Matter of Trust*, Information Security Management Handbook, 5th Edition. Tipton & Krause, editors.

SNIA Storage Security Best Current Practices (BCPs)

SOURCE: Storage Networking Industry Association Technical Proposal, *SNIA Storage Security – Best Current Practices (BCPs) Version 2.1.0*, © 2008 by SNIA, http://www.snia.org/forums/ssif/programs/best_practices/

Background

- Developed and maintained by the SNIA
- Vendor neutral guidance
- Written in layman terms – avoids techno babble
- Minimal assumptions
  - Some familiarity with either storage or security
  - Basic working knowledge of practices and concepts
- Target audience includes
  - Technologist – practitioners & IT architects
  - Management – IT managers & corporate executives

Introduction to the BCPs

- Cover storage systems & storage ecosystems
- Grouped into two categories:
  - ***Core BCPs***
    - apply to all storage systems/ecosystems
    - cover basic storage security elements
  - ***Technology Specific BCPs***
    - above and beyond the core BCPs
    - may or may not apply
    - multiple categories could apply for a given environment

Using the BCPs

- They are not a checklist
- They do not represent a minimum set of requirements to determine compliance
- Must strike a balance between
  - Mitigating risks and minimizing the impacts
  - Cost, complexity, throughput, availability, scalability, etc.
- Each organization must make its own trade-off decisions
  - Its unique situation (e.g., deployed infrastructure, legal and regulatory requirements, and due care expectations)
  - Importance of its data

Structure of BCPs

- Core:
  - General Storage Security (GEN)
  - Storage Systems Security (SSS)
  - Storage Management Security (SMS)
- Technology Specific:
  - Network Attached Storage (NAS)
  - Block-based IP Storage (IPS)
  - Fibre Channel Storage (FCS)
  - Encryption for Storage (ENC)
  - Key Management for Storage (KMS)
  - Long-term Information Security (ARC)

General Storage Security (GEN)

- GEN01 – Identify & Assess All Storage Interfaces
- GEN02 – Create Risk Domains
- GEN03 – Monitor & Control Physical Access
- GEN04 – Avoid Failures Due to Common Mistakes
- GEN05 – Address Data Security Compliance
- GEN06 – Implement Appropriate Service Continuity
- GEN07 – Align Storage and Policy

Focus Areas: Core - GEN

- Identify technology & data assets; do a basic classification
- Make sure storage participates in and complies with policy
- Use risk domains to limit access and damage (for example, management, data access, data protection)
- Make sure storage participates in the survivability measures
- Never underestimate the damage from incompetence or foolishness

Focus Areas: Core - GEN

- Limit physical access, which can be hazardous to data
- Ensure that virtualization doesn't create undesired risks to data
- Pay attention to compliance, privacy & legal requirements
  - Significant drivers for security programs
  - Accountability, traceability, risk management, retention & sanitization

Storage Systems Security (SSS)

- SSS01 – Understand the exposures
- SSS02 – Utilize Event Logging
- SSS03 – Secure Backups and Replication
- SSS04 – Use Trusted and Reliable Infrastructure

Focus Areas: Core - SSS

- Understand the security posture of your storage systems/ecosystems and adjust appropriately
- Ensure storage participates in the centralized audit logging and meets the evidentiary requirements
- Ensure that backups and replication don't become a source of unauthorized data access or disclosure
- Avoid attacks and failures because of inappropriate infrastructure dependencies

Storage Management Security (SMS)

- SMS01 – Secure the Management Interfaces
- SMS02 – Harden Management Applications
- SMS03 – Tightly Control Access and Privileges
- SMS04 – Restrict Remote Support
- SMS05 – Include Configuration Management

Focus Areas: Core - SMS

- Protect the management interfaces from unauthorized access and reconnaissance
- Control and monitor your vendor access to storage systems
- Implement least privilege controls and separation of duties for privileged users
- Ensure that remote support is performed securely and in compliance with policy
- Employ change controls and configuration management practices

Structure of BCPs

- Core:
  - General Storage Security (GEN)
  - Storage Systems Security (SSS)
  - Storage Management Security (SMS)
- Technology Specific:
  - Network Attached Storage (NAS)
  - Block-based IP Storage (IPS)
  - Fibre Channel Storage (FCS)
  - Encryption for Storage (ENC)
  - Key Management for Storage (KMS)
  - Long-term Information Security (ARC)

Network Attached Storage (NAS)

- NAS01 – Network File System (NFS)
  - NAS01.A Control NFS Network Access and Protocols
  - NAS01.B Apply Access Controls to NFS Exported Filesystems
  - NAS01.C Restrict NFS Client Behaviors
  - NAS01.D Secure Data on NFS Filer
- NAS02 – SMB/CIFS
  - NAS02.A Control SMB/CIFS Network Access and Protocols
  - NAS02.B Apply Access Controls to SMB/CIFS Exported Filesystems
  - NAS02.C Restrict SMB/CIFS Client Behaviors
  - NAS02.D Secure Data on SMB/CIFS Filer

Focus Areas: Tech - NAS

- Limit access to the network interfaces
- Secure the file access protocols (NFS, SMB, CIFS, HTTP, NCP)
- Employ user-level authentication whenever possible
- Avoid granting "root" or "administrator" unrestricted access to files on NAS or file server
- Only enable multi-protocol access to files for those users who actually need this functionality

Block-based IP Storage (IPS)

- IPS01 – Secure iSCSI
  - IPS01.A Control iSCSI Network Access and Protocols
  - IPS02.B Implement iSCSI Security Measures
- IPS02 – Secure FCIP
  - IPS01.A Control FCIP Network Access and Protocols
  - IPS02.B Implement FCIP Security Measures

Focus Areas: Tech - IPS

- CHAP authentication is available in all iSCSI implementations (initiators and targets), so use it
- Avoid connecting iSCSI and FCIP interfaces to general purpose LANs; segregate for security and performance
- Remember that VLANs are not the same as physically isolated LANs
- Use IPsec to secure the communication channel when sensitive data could be exposed
- Use discovery services cautiously

Fibre Channel Storage (FCS)

- FCS01 Secure FCP
  - FCS01.A Control FCP Node Access
  - FCS01.B Implement FCP Security Measures
- FCS02 Secure Fibre Channel Storage Networks
  - FCS02.A Implement Switch-based Controls
  - FCS02.B Interconnect Storage Networks Securely

Focus Areas: Tech - FCS

- Limit access to storage, using WWN-based access controls (LUN masking and zoning)
- Leverage ANSI 426–2007 FC-SP features (like authentication and in-flight encryption) for trusted in-band management and trusted storage networks
- Restrict switch interconnections (e.g., ACLs, binding lists, FC-SP policy)
- Configure switches, extenders, routers, and gateways with the least amount of access

Encryption for Storage (ENC)

- ENC01 – Protect Externalized Data
  - ENC01.A Secure Sensitive Data on Removable Media
  - ENC01.B Secure Sensitive Data Transferred Between Data Centers
  - ENC01.C Secure Sensitive Data in 3rd-party Data Centers
- ENC02 – Pedigree of Encryption
  - ENC02.A Encryption Algorithms
  - ENC02.B Symmetric Encryption Modes
  - ENC02.C Strength of Encryption

Check out SNIA Tutorial:

ABCs of Encryption

Encryption for Storage (ENC) cont.

- ENC03 – Risk Assessment in Use of Encryption
  - ENC03.A Identify and Classify Sensitive Data
  - ENC03.B Analyze Risks and Protection Options
  - ENC03.C Mitigate Risks with Encryption
- ENC04 – Encryption Issues
  - ENC04.A Point of Encryption
  - ENC04.B Align with Data Reduction Services
  - ENC04.C Proof of Encryption

See Also: SNIA Technical Proposal, *Data At-rest Encryption: A Step-by-step Checklist, v2.0*, © 2009, http://www.snia.org/forums/ssif/knowledge_center/white_papers/

Check out SNIA Tutorial:

Self Encrypting Drives

Focus Areas: Tech - ENC

- SNIA position on encryption (for sensitive/regulated data):
  - Off-site backup tapes and other removable media must be encrypted when leaving the organization's control
  - Data transmitted to/between trusted, but remote datacenters must be encrypted in-flight
  - Data transmitted and stored in third-party datacenters must be protected both in-flight and at-rest, using encryption
  - For primary data, treat encryption as a measure of last resort
- Ensure the pedigree of the encryption is up to the job
- Ensure that encryption is driven by appropriate risk analysis and business needs
- Avoid huge challenges by identifying the appropriate point of encryption, aligning the encryption with data reduction mechanisms, and creating appropriate audit trails

Key Management (KMS)

- KMS01 – Key Management Principles
  - KMS01.A Observe Important Properties of Keys
  - KMS01.B Implement and Use Key Management Safely
- KMS02 – Key Management Functions
  - KMS02.A Establish Keys Securely
  - KMS02.B Ensure Proper Operational Use
  - KMS02.C Key Disposition
- KMS03 – Key Management Issues
  - KMS03.A Comply with Import/Export Controls
  - KMS03.B Plan for Problems

Check out SNIA Tutorial:

Introduction to Key Management for Secure Storage

Focus Areas: Tech – KMS

- Recognize that key management is the more difficult aspect of cryptograph and standards continue to lag
- Adhere to basic principles associated with keying material as well as implementing key management
- Understand and obey government ***import*** and ***export*** regulations associated with encryption and key management
- Consider escrowing keying material used to protect business/mission critical information

Long-term Security (ARC)

- ARC01 – On-line Fixed Content
  - ARC01.A Secure the On-line Fixed Content
  - ARC01.B Provide Governance and Compliance Functionality
- ARC02 – Off-line Fixed Content
  - ARC02.A Establish Off-line Fixed Content Policy
  - ARC02.B Maintain Off-line Fixed Content Security

Focus Areas: Tech – ARC

- Establish and enforce data retention requirements, including Legal Hold requirements (e.g., e-Discovery)
- Preserve the evidentiary nature of the data through the careful use of authenticity, integrity, and chain of custody mechanisms
- Identify the types of data to be accepted as well as the preservation period
- Ensure that the cryptographic assurances of confidentiality and authenticity are maintained

Final Thoughts

Summary

- Due to the increased activities of organized crime groups and government entities, external threats are a more likely source of data breaches
- A significant number of breach could have been avoided if simple or intermediate security controls had been in place at the time of the incident.
- Protect critical/sensitive/regulated data when it leaves your control
- Manage the risks or mitigate with the consequences
- Have a plan to deal with data security incidents

Last Words

- Security is basically a people problem… computers don't just wake up and start attacking their neighbors on their own…at least not yet!
- The attackers are adapting to our current protection strategies and inventing new ways to attain the data they value.
- It is not a matter of IF you will be attacked, but rather WHEN and if you will KNOW that you have been attacked.

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
Larry Hofer, CISSP, PE
Roger Cummings
Richard Austin, CISSP
Andrew Nielsen, CISSP, CISA
Ray Kaplan, CISSP

SNIA Security TWG

For More Information

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/security/
- Storage Security Industry Forum (SSIF)
  - Focus: Marketing collateral, educational materials, customer needs, whitepapers, and best practices for storage security.
  - http://www.snia.org/ssif