SNIA™
Global Education

Intro to Encryption and Key Management: Why, What and Where?

Eric Hibbard / Hitachi Data Systems

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- 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

- Intro to Encryption and Key Management: Why, What and Where?
  - This Tutorial will explore the fundamental concepts of implementing secure enterprise storage using current technologies, and will focus on the implementation of a practical secure storage system. The high level requirements that drive the implementation of secure storage for the enterprise, including legal issues, key management, current available technologies, as well as fiscal considerations will be explored. There will also be implementation examples that will illustrate how these requirements are applied to actual system implementations.

Overview and Concepts

A Few Definitions (1)

- **Plaintext** – intelligible data; unencrypted data
- **Ciphertext** – data which has been transformed to hide its information content (unintelligible)
- **Cryptographic algorithm** – well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output
- **Key** – sequence of symbols that controls the operation of a cryptographic transformation (e.g., encryption, decryption)
- **Encryption** – operation by a cryptographic algorithm converting data into ciphertext
- **Decryption** – reversal of encryption by a cryptographic algorithm to produce a plaintext

A Few Definitions (2)

- **Key management** – administration and use of generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy
- **Data at rest** – data stored on stable non-volatile storage
- **Data in motion** – data being transferred from one location to another
- **Data breach** – compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed

Encryption Introduction

- Goals of Encryption
  - Make data unintelligible to unauthorized readers
  - Make it extremely difficult to decipher data without knowledge of the keying material
- Factors to consider:
  - Strength of encryption (algorithm, key size)
  - Sufficient randomness (entropy)
  - Quality of encryption (sufficiently reviewed by experts)
  - Speed of encryption (throughput)
  - Management of the persistent encryption keys
  - Auditability (proof of encryption)

Key Management Introduction

- Goals of Key Management (KM)
  - Protecting the confidentiality, integrity, and availability of keying material throughout their lifecycle in accordance with security policy
  - Handling of keys and other related security parameters during the entire life cycle of the keys in conformance with security policy
- Factors to consider:
  - Considered the ***most difficult aspect of cryptography*** because of the human element
  - Maintaining the security posture of the KM systems
  - Defining and enforcing cryptoperiods

Major Key Management Operations

- **Generation** – Creation of fully random keys
- **Distribution** – Keys have to be adequately protected (encrypted) when they are transmitted over networks
- **Storage** – Keys are encrypted wherever they are stored on some form of media; decryption of one key should not expose others in the process
- **Recovery** – Ability to restore (e.g., from backup or escrow service) a key that has been lost or corrupted
- **Destruction** – Ability to permanently destroy an encryption key, rendering the encrypted data unusable

Storage Encryption

Data Storage Encryption

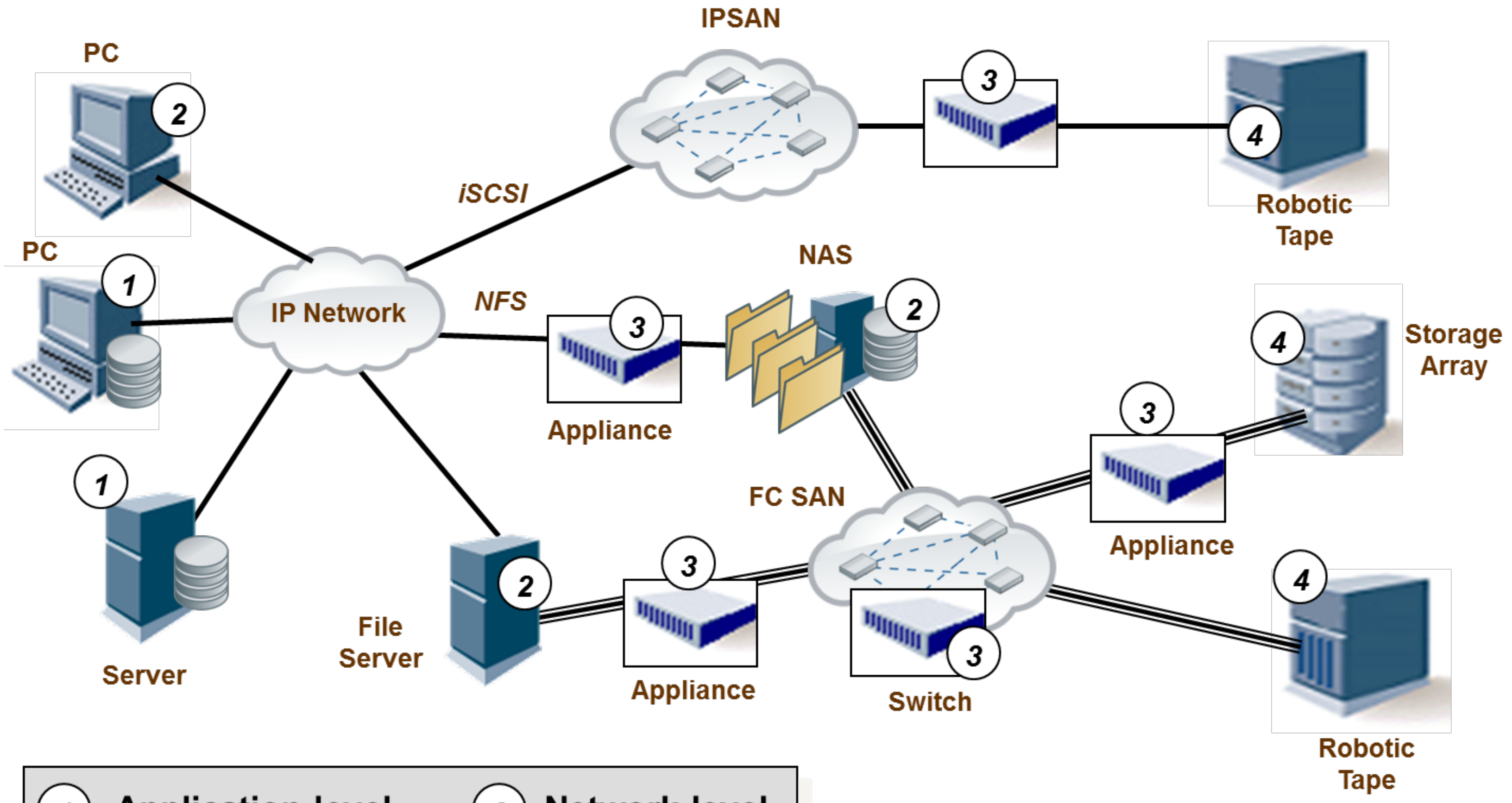
- **Data At Rest Encryption**
  - Encryption that protects data while it resides on the media
  - Multiple options for the placement on encryption/decryption points
- **Data In Motion Encryption**
  - Encryption that protects data while it is being transferred over a physical link between two communicating entities
  - Tends to be ephemeral

- **Encryption within storage ecosystems are typically focused on data at rest**

Location of Encryption & Decryption Points

- **Application-level**
  - Under the control of a specific application or database
- **Filesystem-level**
  - Under the control of the operating system or operating system-level application
- **Network-level:**
  - Under the control of the network devices, such as HBA, array controller, or switch
    - File/Object-based
    - Block-based
- **Device-level:**
  - Under the control of the end-device

Sample Points of Encryption



1	Application-level	3	Network-level
2	Filesystem-level	4	Device-level

Factors and Impacts to be Considered

- Usability
- Availability
- Infrastructure
- Performance/throughput
- Scalability
- In Motion Confidentiality
- Business Continuity/Disaster Recovery
- Proof of encryption
- Environmentals

ISO/IEC 27040:2015 (Storage security) Recommendations

Encryption Recommendations

- For block-based storage, encryption within the storage ecosystem should not be the primary form of encryption
- Encryption used should be a minimum of 112 bits of security strength (128 bits recommended)
- Encryption activities should generate appropriate audit log entries (proof of encryption)
- Compression and deduplication should be factored into the selection of the point of encryption
- Data retention requirements should be accommodated
- Cryptographic modules should be validated using recognized criteria

Key Management Recommendations

- Use keys randomly selected from the entire key space
- Avoid the use of weak keys and check for them
- Data encryption keys should be limited to a finite cryptoperiod (typically no more than 2 years) or to a maximum amount of data processed
- Enforce strict access controls for key generation, change, and distribution
- Use a centralized, interoperable key management infrastructure
- OASIS KMIP-compliant servers and clients should be used to manage keys
- Key management should be fully automated

Implementation Issues & Drivers

Compliance and Encryption

- **Payment Card Industry Data Security Standard (PCI DSS)** – stored credit card data needs to be rendered unreadable
- **Privacy Regulations** – PII needs to be protected against data breaches
- **HIPAA/HITECH** – requires encryption of electronic protected health information
- **GLBA/FFIEC** – ensure the security and confidentiality of customer financial information

- Proper use of encryption often serves as a “safe harbor”

Common Implementation Approaches

- Self encrypting drives (SED)
- Storage array encryption
- Full disk encryption (FDE)
- File-level Encryption (FLE)

Cryptographic Erase

- Approved method of sanitization
  - ISO/IEC 27040:2015
  - NIST Special Publication 800-88 Rev 1 (Dec-2014)
  - May be the only way of sanitizing certain types of media (e.g. flash)
- Predicated on the encryption being active before data is recorded
- Can be used for secure and rapid de-provisioning
- Accomplished by sanitization of the target data’s encryption key (all copies), leaving only the ciphertext on the media
- Both proof of encryption and proof of sanitization are needed

Enterprise Key Management

- Storage systems that include encryption technology often include integrated key management
- To guard against catastrophic loss of the keys used by storage systems, regular backups of the keys are necessary (e.g., drive replacements)
- In large installations, these backups can represent a significant operational consideration
- Centralized key management can be a mitigation strategy
  - Leveraging OASIS Key Management Interoperability Protocol (KMIP) for storage systems (clients)

Additional Issues

- Key compromise recovery plan
- Business continuity management (disaster recovery)
- Interactions with data reduction techniques
  - Compression and deduplication must be performed before encryption
  - Encryption can render these technology ineffective
- Import/Export (or transfer) of encryption technology
  - Severe penalties for unauthorized actions

Final Thoughts

Remember…

- Determining the primary driver for encryption is critical
- Classification of the organizational data can significantly improve the effectiveness of most encryption solutions
- Know (or be able to discover) where the data resides
- The “need” for encryption, combined with insufficient budget, often results in impacts to business processing
- Key management complexities are almost always overlooked, but they are critical success factors for the encryption solution
- Interoperability is not guaranteed, so attention to detail is important
- For all that encryption offers, it does not come for free
- If you can’t prove encryption is operational, why bother

Useful Resources

- Standards:
  - ISO/IEC 27040, ISO/IEC 11770, ISO/IEC 18033, ISO/IEC 17970
  - NIST FIPS 140-2, NIST FIPS 197NIST SP 800-57, NIST SP 800-88
  - OASIS KMIP
  - IEEE Std 1619 (XTS-AES)
  - TCG Storage Opal SSC, TCG Storage Enterprise SSC
- Industry Resources
  - SNIA Tutorials: http://www.snia.org/education/tutorials/security
  - SNIA Whitepapers:
    - Encryption and Key Management
    - Sanitization
    - http://www.snia.org/securitytwg

SNIA Security Organizations

- 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: Educational materials, customer needs, whitepapers, and best practices for storage security.
  - http://www.snia.org/ssif

Attribution & Feedback

SNIA Global Education

The SNIA Education Committee thanks the following Individuals for their contributions to this Tutorial.

Authorship History

Eric A. Hibbard – May 2016

Updates:
N/A

Additional Contributors

Richard Austin
Walt Hubis
Tim Hudson
Thomas Rivera

Please send any questions or comments regarding this SNIA Tutorial to ***tracktutorials@snia.org***