Education

Practical Storage Security With Key Management

Russ Fellows, Evaluator Group

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.

Storage Security Best Practices

- Best Practices are Dependent on Regulation
- What to Protect Depends on Context and Data
  - 'Joe Smith' is not covered by PCI in and credit card industry
  - 'Joe Smith' is covered by HIPAA and HIPAA HiTech for health information
- "Data Security" Does Not Always Imply Encryption
- Balance between security and ease of doing business

Types of Protected Information

- Many Types of Data Covered by Federal Laws:
  - Social Security Numbers (HIPAA, FERPA, others)
  - Credit Card #'s (PICS)
  - Date of Birth (HIPAA, others)
  - Student transcripts (FERPA)
  - Health records (HIPAA)
- Must be "Protected" from Release to any Unauthorized Individual

RISKS

Common Types Data Breach

- Loss of Physical Control
  - Theft or loss of tapes, disks, laptops, USB sticks, DVD's etc.
- External Access
  - Access by any unauthorized entity
  - Common Methods
    - "Hackers" – less common
    - Social Engineering – more common
      - Both "Overt" (e.g. talking with employees) and "Covert" (information harvesting)
      - Covert Social Engineering
        - Spyware, malware, "surveys", etc. Social media sites, etc.
  - Encryption of stored and displayed data may limit both

Data Breaches

- Costs can be Significant - Average cost $5.5 million*
  - * (2011 : 7th annual Ponemon study sponsored by Symantec)
    - Study includes 49 companies across 14 industries
- Costs Include:
  - Loss of credibility
  - Civil and Criminal liabilities
  - Internal costs (detecting, investigation, notification, disruption, and productivity losses)
- Likelihood
  - 37% - Malicious or criminal attacks
    - 50% malware, 33% Insider, 28% Theft, 17% Social Engineering
  - 39% - Negligence
  - 24% - 'System' Errors

End User Computing

- End User Devices - One of the Biggest Risk Factors
  - Proliferation of devices (tablets, smartphones, laptops)
  - BYOD adding further complications
- Issues with Protection:
  - Locking down access impacts business operations
  - Employees circumvent security to improve efficiency
- Virtual Desktops (VDI) can Enhance Security
  - Server-Based Storage of all Data

End User Recommendations

- Security Recommendations for End User Devices:
  - VDI can help with access to data
    - Centralized storage for all desktops / data
    - Apps, user data stored in any location
  - BYOD access to locked-down data
  - Secure all portable devices
    - Encrypt any stored data, login / password access
  - Encryption For All Locally Stored Data
    - Full disk encryption, volume, file or folder encryption
  - NIST Recommendations
    - Centralized management of encryption keys
    - Encryption keys stored securely, not with encrypted data

PRACTICAL DATA SECURITY TECHNOLOGIES

Encryption

- Regulatory Compliance
  - Often mandate FIPS-140-2, NIST, etc.
  - AES encryption, RSA public keys, etc.
- Business Best Practices
  - May require use of encryption
- Encryption relatively "low cost"
  - AES instructions now on x86 chips

Encryption Keys

- Key Management
  - Copy your keys
    - This includes electronic and/or printed copies of keys
    - No lock smith who can create a new key for you
  - Protect your keys
    - A physical vault is good
  - Manage them in standard formats
    - Standards now exist, implementations lagging
- KMS's can perform all of these functions
  - Key Management Servers
  - Electronically copy, protect and manage key interchange

Key Management

- OASIS KMIP – Coming … really
  - Over 10 companies demonstrating compatibility
  - KMIP (key mgmt.) and XACML (key access)
- SNIA SSIF
  - Storage Security Industry Forum
  - New SSIF Testing
    - KMIP interop testing, both clients & servers
    - Lab setup at Technology Lab in Co. Springs.

Tokenization

- Replaces Protected Data with a "Token"
  - Random data - like cypher text
  - Tokens are a 1 way cypher
    - Cannot deduce the value from the token
  - Creates a "Code Book" with reference to actual value
- Features of Tokens
  - Security for Token Still Required
  - Tokens may be shared in the open
  - Tokens typically are the same length as original data
    - Allows them to "stand in" for fields in databases and other tools

INDUSTRY IMPACT

Regulations Dictate Security

- Regulations Effect Companies Across Industries
  - HIPAA: Companies with medical data
  - Sarb-Ox, C-SOX: Public Companies
  - PCI-DSS: Payment card processing
  - GLBA or BASEL III: Financial organizations
  - FISMA: US Govt. Regulations

HIPAA - Covered Entities

- Who Must Comply with HIPAA?
  - Companies with health plans that receive identifiable claims data (most plans with > 100 members)
  - Companies with Self Insured plans are typically 'Covered Entities'
- Encrypt any Media not under Physical Control
  - Includes vaults, DR sites or any other locations
  - PHI – Protected Health Information must be encrypted
  - Encrypt any e-mail that contains PHI
  - Laptop, tablet, smart-phones, etc.

HIPAA HiTech

- Extends Encryption Requirements
  - Encrypt Media, Including vaults, DR sites, etc.
- Encrypt any e-Mail that Contains ePHI
  - Email encryption:
    - Encrypt in the client or encrypted web based email service
- Encrypt the Storage of all ePHI
  - Even laptops that are protected with strong "boot passwords" are vulnerable
- Transport must Use Encryption
  - TLS, SSL, IPSec or similar technologies

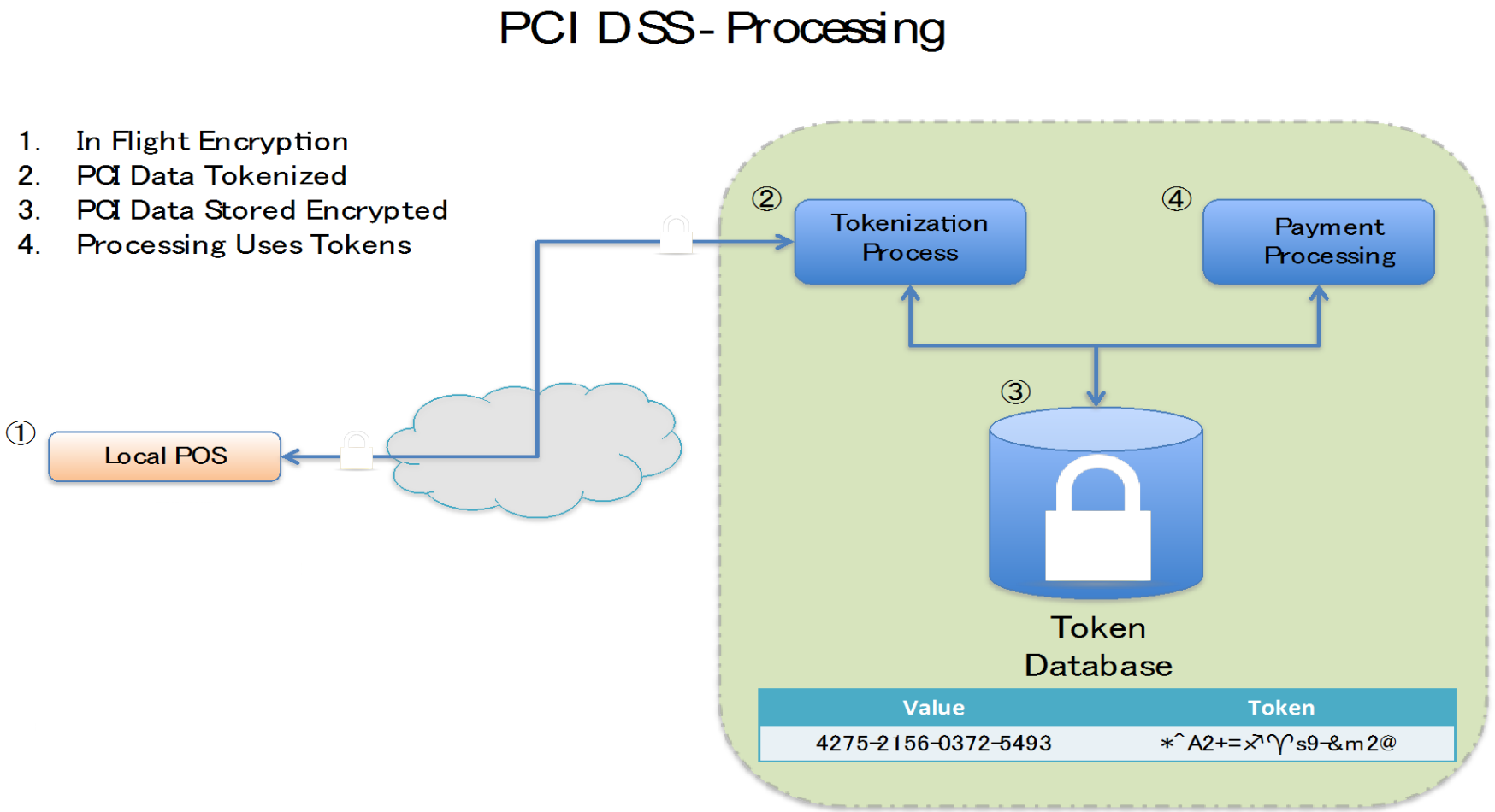
GLBA

- Gramm Leach Bliley Act
- Requires Financial Institutions to:
  - Maintain "The security and confidentiality of customer records and information" and
  - "Protecting against unauthorized access to information"

PCI DSS

- Payment Card Industry – Data Security Standard
- Who is Covered
  - Any company that holds, retains or processes credit card information must comply
- There are 12 Requirements
  - Requirement 3 mandates business to ensure payment card data is stored in a highly secure manner
  - Practically this means physical security and encryption
- "Tokenization" is the hot trend for PCI encryption

Using Tokens



Tokenization – Magic Bullet ?

- Pro's:
  - Protected information is centralized and encrypted
  - Works well for short, well defined data types (SSN, Credit Card, etc.)
- Con's:
  - Applications must be designed to utilize tokens
  - Does not work well for generally sensitive data
    - Email detailing health conditions, treatment, etc.
  - Centralized token-store is critical to business
    - Loss of token-store means loss of all protected fields

SECURITY BEST PRACTICES

The 4 "A's" of Security

- **Authentication** – Verifies the identity of a person or entity
- **Authorization** – Provides access to protected resources for authorized entities
- **Access** – Restricts access refers to resources
  - May be achieved through limited physical access
  - Or restriction via encryption
- **Audit** – Records and log authentication, authorization and access including all actions

Best Practices from NSA

- The NSA created 20 items ranked in order of importance for mitigating loss of data
  - Details on NSA or SANS websites
- In Essence, Attackers try to:
  - Probe for weaknesses
  - Obtain access to a system
  - Remain on system by hiding
  - Exploit their existence

Reduce Exposure to Data Breach

- Technical Areas
  - Encrypt only what is necessary
  - Limit internal access to un-encrypted information
    - Tokenization, Displays that blank out fields, etc.
- Process Areas
  - Appoint a CSO (Chief Security Officer) to coordinate
  - Classify Data
    - Identify what is, and is not covered
  - "Delete" is your friend
    - If there is no legal or business reason to retain data, it should be deleted
    - Some regulations mandate time length for retention

Best Practices

- Overall Plan for Security
  - Classification is the first step
  - Do not start with encryption
    - Can lead to gaps in security and impact operations
  - Remember the four "A's" of security
    - Authentication – who are you?
    - Authorization – do you have permission?
    - Access – limited to what you need
    - Audit – record who you are, and what you do
  - Implement Key Management

To Do List for Practical Security

1. Appoint a CSO
2. Document Applicable Regulations
3. Review Applications and Data Impacted by Regs.
4. Classify Data
5. Create Storage Security Policy
6. Review four "A's" of Security
7. Reduce Exposure to Data Breaches
8. Choose and Implement a KMS
9. Encrypt Required Data
10. Monitor Compliance

Attribution & Feedback

The SNIA Education Committee would like to thank the following individuals for their contributions to this Tutorial.

Authorship History

Russ Fellows

Additional Contributors

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