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.
Implementing Stored-Data Encryption

Data security is top of mind for most businesses trying to respond to the constant barrage of news highlighting data theft, security breaches, and the resulting punitive costs. Combined with litigation risks, compliance issues and pending legislation, companies face a myriad of technologies and products that all claim to protect data-at-rest on storage devices. What is the right approach to encrypting stored data? The Trusted Computing Group, with the active participation of the drive industry, has standardized on the technology for self-encrypting drives (SED): the encryption is implemented directly in the drive hardware and electronics. Mature SED products are now available from all the major drive companies, both HDD (rotating media) and SSD (solid state) and both laptops and data center. SEDs provide a low-cost, transparent, performance-optimized solution for stored-data encryption. SEDs do not protect data in transit, upstream of the storage system.

For overall data protection, a layered encryption approach is advised. Sensitive data (eg, as identified by specific regulations: HIPAA, PCI DSS) may require encryption outside and upstream from storage, such as in selected applications or associated with database manipulations.

This tutorial will examine a ‘pyramid’ approach to encryption: selected, sensitive data encrypted at the higher logical levels, with full data encryption for all stored data provided by SEDs. The attendee should learn:

- The mechanics of SEDs, as well as application and database-level encryption
- The pros and cons of each encryption subsystem
- The overall design of a layered encryption approach
The Problem...

Since 2005, over 345,124,400 records containing sensitive personal information have been involved in security breaches.

In 2008, the average cost of a data breach was $6.65 million per affected corporation ($202 per record).

http://www.privacyrights.org/ar/ChronDataBreaches.htm
Since 2005, over 345,124,400 records containing sensitive personal information have been involved in security breaches.

- Legal
- Financial
- Reputation

In 2008, the average cost of a data breach was $6.65 million per affected corporation ($202 per record).

http://www.privacyrights.org/ar/ChronDataBreaches.htm
Example: California

... any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person…”

Encryption “safe harbor”
Why Encrypt Data-At-Rest?

**Threat scenario**: stored data leaves the owner’s control – lost, stolen, re-purposed, repaired, end-of-life, …

- **Compliance**
  - 46+ states have data privacy laws with encryption “safe harbors”, which exempt encrypted data from breach notification¹

- Data center and laptop drives are portable (HDD, SSD)

- Exposure of data loss is expensive ($6.65 Million on average per incident²)

- Obsolete, Failed, Stolen, Misplaced…
  - Nearly ALL drives leave the security of the data center
  - The vast majority of retired drives are still readable

---

Customers Need Encryption
End-Users are looking for a Compliance Strategy

- New & Emerging Regulations and Laws Impact Key Verticals
  - Encryption is a ‘Safe Harbor’ whereby encrypted data cannot be stolen as long as the thief doesn’t have the key
- Customers are struggling to avoid the cost of a security breach
  - $204 per lost record, $6.7 million per breach
- Customers “Getting By” with current approaches
  - 31% of End-Users use DB encryption
    - 25% of customers are planning to add more encryption
  - Disk shredding can cost millions per year
- Customers are overwhelmed with the complexity of compliance
  - Up to 20% of IT staff time
- Real Customers asking for help
  - F100 Companies, Healthcare, Retail
  - Federal, DoD, and other three letter agencies
- Customers are looking for a better solution

<table>
<thead>
<tr>
<th>Vertical</th>
<th>Encryption Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Sector</td>
<td>Encryption is required for FISMA, DoD, and DCID 6/3</td>
</tr>
<tr>
<td>Health Sector</td>
<td>HiTECH gives HIPAA teeth. Healthcare providers can be fined or prosecuted</td>
</tr>
<tr>
<td>Ecommerce or Ecommerce hosting</td>
<td>PCI-DSS Requirement 3 is mandatory for any company that handles credit cards</td>
</tr>
<tr>
<td>Retail</td>
<td>PCI-DSS mandates encryption for data at rest for credit card data</td>
</tr>
<tr>
<td>Service Providers</td>
<td>Need to provide service level support for HiTECH, PCI-DSS, GLBA, FFIEC</td>
</tr>
<tr>
<td>Financial Institutions</td>
<td>Basel II, FFIEC, and GLBA place strict requirements including encryption</td>
</tr>
<tr>
<td>Other</td>
<td>Massachusetts and Nevada Laws are mandating encryption for any company that does business in their state. Law firms are sending out Client Alerts on the requirement to encrypt data</td>
</tr>
</tbody>
</table>

Over 10,000 rules and regulations for end-users to manage
Encryption can be done in a number of places...

- Host middleware
- Host HBA (h/w adapter)
- Application
- Switch
- “Bump in the wire” or proxy appliance
- Array controller
- Drive (HDD, SSD)
Encryption can be done in “layers”…

Host middleware

Host HBA (h/w adapter)

Application

Switch

“Bump in the wire” or proxy appliance

Array controller

Drive (HDD, SSD)
Key Management: Disparate, Proprietary Protocols

Implementing Stored-Data Encryption
© 2012 Storage Networking Industry Association. All Rights Reserved.
OASIS KMIP: Standardized Key Management
Host and HBA Based Encryption

Host based

```
Key Manager

Application

O/S

HBA

HBA

Switch/Router/Appliance

Storage Controller
```

HBA based

```
Key Manager

Application

O/S

HBA

HBA

Switch/Router/Appliance

Storage Controller
```
Switch or Appliance Based Encryption

Switch based

Application

O/S

HBA

HBA

Switch or Router

Storage Controller

Key Manager

Appliance based

Application

O/S

HBA

HBA

Network Appliance

Storage Controller

Key Manager
Storage Controller or Drive-Based Encryption

Storage Controller

Application

O/S

HBA

HBA

Switch/Router/Appliance

Storage Controller

Key Manager

Drive

Application

O/S

HBA

HBA

Switch/Router/Appliance

Storage Controller

Locking Key Manager

NO encryption key management needed
Encryption of Data At-Rest

*Step-by-step Checklist*

Version 2.0

September 9, 2009

(available @ [http://www.snia.org/forums/ssif/knowledge_center/white_papers/](http://www.snia.org/forums/ssif/knowledge_center/white_papers/))
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)
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
#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
#2 Classify Data Assets

- Can you afford to encrypt everything?
- Classify data assets to prioritize encryption
- Use coarse classifications to start
  - e.g. High Value to the Organization, Most Sensitive, Regulated
  - … and refine over time
- Determine confidentiality priorities & categories
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)
#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?
#5 Choose Points-Of-Encryption

- **Security Perspective:**
  - Encrypt as close to source as possible (& get more protection per $!)

- **Points of Encryption:**
  - **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”
#6 Design Encryption Solution

- 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
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?
- Audit controls
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
#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
#9 Activate Encryption

- Activate encryption? NO, not quite yet!
- First get management signoff
  - Outside evaluation/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
Encryption upstream can affect other processes

- Data Compression
- Data De-duplication
- Data Loss Prevention (DLP)

Stored Data
Self-Encrypting Drives

- Simplified Management
- Robust Security
- Compliance “Safe Harbor”
- Cuts Disposal Costs

- Scalable
- Interoperable
- Integrated
- Transparent

“Many organizations are considering drive-level security for its simplicity in helping secure sensitive data through the hardware lifecycle from initial setup, to upgrade transitions and disposal.”

Eric Ouellet
Research Vice President
Gartner
Client Security: Pre-Boot Authentication

- Transparency: Master boot record and OS are unmodified
- Protected from malicious software: Authentication occurs before OS (and any malicious software) is loaded
- The master boot record can’t be corrupted: The entire drive, including the master boot record, is encrypted

1. BIOS attempts MBR read; drive redirects to pre-boot area
2. Drive loads pre-boot OS
3. User enters authentication credentials for drive to verify
4. If authentication successful, drive loads original MBR
5. Normal operation commences
Implementing Stored-Data Encryption

© 2012 Storage Networking Industry Association. All Rights Reserved.

Authentication in the Drive

1. Correct AK?
   - Yes: Clear AK decrypts DEK
   - No: Drive does NOT respond to Read or Write Reqs

Hash AK

2. Clear AK decrypts DEK

Unlock HDD

3. DEK encrypts and decrypts User Data

AK
Authentication Key

DEK
Data Encryption Key

Hashed AK

Encrypted DEK

Disc

Clear Data

Pre-boot Authentication

Drive Server

Storage Server

教育 SNIA
Cryptographic Erase

Description

- Cryptographic erase changes the drive encryption key.
- Data encrypted with previous key, unintelligible when **DEcrypted** with new key.

Benefits

- Instantaneous “rapid” erase for secure disposal or re-purposing.

Revision of U.S. NIST SP800-88: *Guidelines for Media Sanitization* under way to support Crypto Erase.
### ‘Hurdles’ to Implementing Encryption…

<table>
<thead>
<tr>
<th><strong>Key management / data loss</strong></th>
<th><strong>Complexity</strong></th>
<th><strong>Performance</strong></th>
<th><strong>Cost</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Tracking and managing encryption keys</td>
<td>- Data classification</td>
<td>- Performance degradation; scalability</td>
<td>- Initial acquisition costs</td>
</tr>
<tr>
<td>- Tracking and managing authentication keys (passwords for unlocking drives)</td>
<td>- Impact on OS, applications, databases</td>
<td></td>
<td>- Deployment costs</td>
</tr>
<tr>
<td>- Interoperability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
No Performance Degradation

Encryption engine speed
Matches
Port’s max speed

The encryption engine is in the drive electronics

Scales Linearly, Automatically

Network

Storage System

Storage System

All data will be encrypted, with no performance degradation
IT Retires Drives Constantly

- All Drives are Eventually Retired
  - End of Life
  - Returned for Expired Lease
  - Returned for Repair / Warranty
  - Repurposed

- 50,000 drives leave data centers daily

- Exposure of data is expensive - $6.65 million on average

- 90% of retired drives are still readable
  (IBM study¹)

Needed: A simple, efficient, secure way to make retired drive data unreadable

How the Drive Retirement Process Works

Retire Drive
• Replace
• Repair
• Repurpose

Remove ALL drives
Send even “dead” drives through
Queue in Secure Area
Transport Offsite
Queue in secure area

Retirement Options

Overwriting takes days and there is no notification of completion from drive

Hard to ensure degauss strength matched drive type

Shredding is environmentally hazardous

Not always as secure as shredding, but more fun

People make mistakes

“Because of the volume of information we handle and the fact people are involved, we have occasionally made mistakes.”

which lost a tape with 150,000 Social Security numbers stored at an Iron Mountain warehouse, October 2007


99% of Shuttle Columbia’s hard drive data recovered from crash site

Data recovery specialists at Kroll Ontrack Inc. retrieved 99% of the information stored on the charred Seagate hard drive’s platters over a two day period.

- May 7, 2008 (Computerworld)
How the Drive Retirement Process Works

Drive Retirement is:

- Expensive
- Time-consuming
- Error-prone

*which lost a tape with 150,000 Social Security numbers stored at an Iron Mountain warehouse, October 2007*

---

Drive Retirement: Self-Encrypting Drives

Power Off = Locked and Encrypted = Secure

- Reduces IT operating expense
  - Eliminates the need to overwrite or destroy drive
  - Secures warranty and expired lease returns
  - Enables drives to be repurposed securely
- Provides safe harbor for most data privacy laws
Encryption key never leaves the drive. No need to track or manage …
BUT, YOU STILL MANAGE THE AUTHENTICATION KEYS (drive locking),
to protect against loss or theft (for just crypto erase, no authentication key needed)

• To recover data from a drive:
  • Only need the Authentication Key and the drive
  • Don’t need to escrow the encryption key to maintain data recoverability
  • Don’t need to track encryption key storage separate from data storage
  • Don’t need to be concerned with interoperability of encryption key storage and data
Hardware-Based Self-Encryption versus Software Encryption

- **Transparency:** SEDs come from factory with encryption key already generated

- **Ease of management:** No encrypting key to manage

- **Life-cycle costs:** The cost of an SED is pro-rated into the initial drive cost; software has continuing life cycle costs

- **Disposal or re-purposing cost:** With an SED, erase on-board encryption key

- **Re-encryption:** With SED, there is no need to ever re-encrypt the data

- **Performance:** No degradation in SED performance

- **Standardization:** Whole drive industry is building to the TCG/SED Specs

- **No interference** with upstream processes

**ISSUE:** Hardware acquisition (part of normal replacement cycle)
Performance Comparisons: HDD and SSD, software versus SED

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Startup</td>
<td>7.90</td>
<td>6.97</td>
<td>7.99</td>
<td>82.50</td>
<td>47.90</td>
<td>95.33</td>
</tr>
<tr>
<td>App Loading</td>
<td>7.03</td>
<td>5.77</td>
<td>5.71</td>
<td>48.33</td>
<td>30.77</td>
<td>60.37</td>
</tr>
<tr>
<td>Modest size file test</td>
<td>6.13</td>
<td>5.00</td>
<td>5.28</td>
<td>41.13</td>
<td>26.77</td>
<td>50.40</td>
</tr>
<tr>
<td>Large Scale Data Read</td>
<td>84.67</td>
<td>52.88</td>
<td>82.75</td>
<td>178.00</td>
<td>70.23</td>
<td>169.33</td>
</tr>
<tr>
<td>Large Scale Data Write</td>
<td>79.60</td>
<td>49.50</td>
<td>50.31</td>
<td>170.80</td>
<td>63.60</td>
<td>164.50</td>
</tr>
</tbody>
</table>

http://www.trustedstrategies.com/
### Addressing the Hurdles...

| Simplifies key management to prevent data loss | ✓ Encryption key does not leave the drive; it does not need to be escrowed, tracked, or managed |
| Simplifies Planning and Management | ✓ Standards-based for optimal manageability and interoperability  
✓ Transparent to application developers and database administrators. No change to OS, applications, databases  
✓ Data classification not needed to maintain performance |
| Solves Performance | ✓ No performance degradation  
✓ Automatically scales linearly  
✓ Can change keys without re-encrypting data |
| Reduces Cost | ✓ Standards enables competition and drive cost down  
✓ Compression and de-duplication maintained  
✓ Simplifies decommissioning and preserves hardware value for returns, repurposing |
The Future: Self-Encrypting Drives

- **Encryption everywhere!**
  - Data center/branch office to the USB drive

- **Standards-based**
  - Multiple vendors; interoperability

- **Unified key management**
  - Authentication key management handles all forms of storage

- **Simplified key management**
  - Encryption keys never leave the drive. No need to track or manage.

- **Transparent**
  - Transparent to OS, applications, application developers, databases, database administrators

- **Automatic performance scaling**
  - Granular data classification not needed
Layered Encryption

- Higher-level encryption
- Data context awareness
- Specific legislation requirements

- Encryption closer to storage
- Self-encrypting drives:
  - Encrypt everything!
  - Transparently
Thank You!
Check out...

- **SNIA Tutorials:**
  - Storage Security - The ISO/IEC Standard
  - Industry Perspective: Wikileaks: Are You the Next Target?
  - User Case Study: A holistic approach to Information security for Small and Medium Businesses
SNIA Security: Get Involved!

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](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](http://www.snia.org/forums/ssif)
Q&A / Feedback

Please send any questions or comments on this presentation to SNIA: tracktutorials@snia.org

Many thanks to the following individuals for their contributions to this tutorial.
- SNIA Education Committee

Roger Cummings
Gianna DaGiau
Eric Hibbard