SELF-ENCRYPTING DRIVES
Michael Willett, WillettWorks Technology
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

SELF-ENCYCRYPTING DRIVES

Data security is top of mind for most businesses trying to respond to the constant barrage of news highlighting data theft and security breaches. Combined with litigation risks, compliance issues and pending legislation, companies face a myriad of technology and products that all claim to protect data-at-rest on storage devices. However, these current solutions either fail to deliver or force compromise.

The disk drive industry has standardized and is now deploying innovative, simple and powerful technology intended to secure data where it lives – in storage. This presentation will give storage users and managers a look at emerging drive-level self-encryption technology (both HDD and SSD) from notebook PCs to the data center that will provide a more secure storage foundation.
IT Security Today

- Corporations spend millions to protect their networks, devices & data…
  - Physical security, firewalls, intrusion detection, etc…

- …But don’t always understand the risk posed by internal misplacement, re-purposing, and disposal processes.
The Problem...

Over 155,048,651 records containing sensitive personal information have been involved in security breaches in the US since 2005.

Reported Data Breaches Since February 2005 to Now

Source: Privacy Rights Clearinghouse

In another survey by the Ponemon Institute – corporations shelled out $14 million dollars on average to recover from a data breach.

$14 Million Per Incident
The Problem…

Over 155,048,651 records containing sensitive information have been involved in reported data breaches since February 2005.

Legal

Financial

Reputation

$14 Million Per Incident

Reported Data Breaches Since February 2005 to Now

# of reported breaches per month

Source: Privacy Rights Clearinghouse

Over 155,048,651 records containing sensitive information have been involved in reported data breaches since February 2005.
Problem: security for data-at-rest

Jan. 2, 2009
Merrill Lynch
Burglars took a computer, which had on it the names and Social Security numbers of current and former Financial Advisors and some applicants for employment.

Jan. 13, 2009
University of Oregon
A laptop computer containing data files for Youth Transition Program (YTP) participants was stolen. Those files contained names and social security numbers.

Jan. 13, 2009
Innodata Isogen, Inc. (Hackensack, NJ)
Laptop stolen from an employee’s car contained names, addresses, Social Security numbers of current and former employees.

Jan. 13, 2009
Seventh-Day Adventist Church (Silver Spring, MD)
A laptop stolen contained names and Social Security numbers.

Jan. 13, 2009
Continental Airlines (Newark, NJ)
A laptop containing fingerprints, Social Security numbers, names, addresses, was stolen from a locked Newark office.

Jan. 16, 2009
Southwestern Oregon Community College (Coos Bay, OR)
A laptop computer was stolen from the campus putting former and current students at risk.

Jan. 31, 2009
HoneyBaked Ham (Indianapolis, IN)
A computer server stocked with credit-card information was stolen from a store.

Feb. 3, 2009
Baystate Medical Center (Springfield, MA)
Several laptops were stolen with patient information on them.

The thefts and loss go on and on and...

Source: [http://www.privacyrights.org/ar/ChronDataBreaches.htm#2009](http://www.privacyrights.org/ar/ChronDataBreaches.htm#2009)
Who is demanding a solution...?

6 new bills on security breach, privacy, theft.

44+ states have passed laws on data privacy w/ encryption safe harbors

(Requires FIPS-140 Compliance)
Why Encrypt Data-At-Rest?

- Compliance
  - 44+ states have data privacy laws with encryption safe harbors
  - New data breach bills have explicit encryption safe harbors
- Exposure of data loss is expensive
- Data center and laptop drives are mobile (HDD, SSD)
- Exposure of data loss is expensive ($14 Million on average\(^1\))
- Obsolete, Failed, Stolen, Misplaced…
  - Nearly ALL drives leave the security of the data center
  - The vast majority of decommissioned drives are still readable

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

Encryption can be done in a number of places…

- Host middleware
- Host HBA (h/w adapter)
- Application
- Switch
- “Bump in the wire” appliance
- Array controller
- Drive (HDD, SSD)

Check out SNIA Tutorial: “ABCs of Encryption”
Encryption can be done in a number of places...

- Host middleware
- Host HBA (h/w adapter)
- Application
- Application Server
- Network Fabric
- Switch
- "Bump in the wire" appliance
- Array controller
- Drive (HDD, SSD)
3 Simple reasons

- **Storage for secrets with strong access control**
  - Inaccessible using traditional storage access
  - Arbitrarily large memory space
  - Gated by access control

- **Unobservable cryptographic processing of secrets**
  - Processing unit “welded” to storage unit
  - “Closed”, controlled environment

- **Custom logic for faster, more secure operations**
  - Inexpensive implementation of modern cryptographic functions
  - Complex security operations are feasible
Trusted Storage Standardization

Published Storage Specifications
Joint Work – T10 (SCSI) and T13 (ATA)

**TRUSTED SEND/IN**

(Protocol ID = xxxx .....)

---

**TRUSTED RECEIVE/OUT**

---

T10/T13 defined the “container commands”

TCG/Storage defining the “TCG payload”

Protocol IDs assigned to TCG, T10/T13, or reserved
TRUSTED STORAGE

- (Partitioned) Hidden Memory
- Security firmware/hardware
- Trusted Send/Receive Commands
- Assign Hidden Memory to Applications

Implementation Overview
Trusted Storage with Trusted Platform

Trusted Storage

Root Of Trust

Secure Communications

Trusted Platform

TPM

OR

Trusted Element

Life Cycle: Manufacture, Own, Enroll, PowerUp, Connect, Use, …
Trusted Storage with Trusted Platform

Trusted Storage

Manage Trusted Storage

Life Cycle: Manufacture, Own, Enroll, PowerUp, Connect, Use, …
TCG Storage Use Case Examples

Self-Encrypting Drive
- Laptop Loss or Theft
- Re-Purposing
- End of Life
- Rapid Erase

DriveLocking/DrivePairing

On-board Crypto Key Management

Forensic Logging

DRM Building Blocks

Personal Video Recorders

Self-Encrypting Drives
© 2009 Storage Networking Industry Association. All Rights Reserved.
SPs (Security Providers)
- Logical Groupings of Features
- SP = Tables + Methods + Access Controls

Tables
- Like “registers”, primitive storage and control

Methods
- Get, Set – Commands kept simple with many possible functions

Access Control over Methods on Tables
SPs (Security Providers)
- Logical Groupings of Features
- SP = Tables + Methods + Access Controls

Tables
- Like “registers” for primitive storage and control

Methods
- Get, Set – Commands kept simple with many possible functions

Access Control over Methods on Tables
Home Banking
(or Remote Medical, or … )

- Multi-factor authentication: password, biometrics, dongles
- Secure/hardware storage of credentials, confidential financial/medical data
- Trusted life cycle management of personal information
- Integrity-checking of application software
- Cryptographic functions for storage and communications security
- Trusted/secure computation of high-value functions (protection from viruses/etc)
Home Banking
(or Remote Medical, or … )

Breadth of Applications

Trusted Platform w/
Trusted Storage

- Multi-factor authentication: password, biometrics, dongles
- Secure/hardware storage of credentials, confidential financial/medical data
- Trusted life cycle management of personal information
- Integrity-checking of application software
- Cryptographic functions for storage and communications security
- Trusted/secure computation of high-value functions (protection from viruses/etc)
TCG Storage: Document Structure

**General Documents**

**Specific Documents**

**Auxiliary Documents**

Core Spec  
Interface

PC SSC (OPAL)  
Optical SSC  
Enterprise SSC

Compliance and Security Evaluation

SSC = Security Subsystem Class

Self-Encrypting Drives  
© 2009 Storage Networking Industry Association. All Rights Reserved.
Self-Encrypting Drives

© 2009 Storage Networking Industry Association. All Rights Reserved.

Separate control channel

- transparent
- compatible

- ease of use
- unobtrusive

CD/DVD

Self-Encryption
“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
Self-Encrypting Drives Solve...

Purpose

- Protect data from exposure due to equipment loss
- Enable instant, secure erase of HDD/SSD

Closed encryption device

- Dedicated engine for full interface speed encryption
- Key generated by true RNG\(^1\) in drive
- Encryption cannot be turned off
- Encryption Key never leaves the drive
- Drive exposes an open interface for management of encryption & credentials
- Only signed firmware can be loaded onto drive

2 Architectures

- Client (laptops, desktops) 3rd party software manages encryption
- Enterprise (arrays) Storage System manages encryption

\(^1\)Random Number Generator
- **Enterprise Server:**
  - Key generation and distribution
  - Key/Password archive, backup and recovery

- **Laptop (Application):**
  - Master/User passwords, multi-factor authentication, TPM support
  - Secure log-in, “Rapid Erase”

- **Trusted Drive (self-encrypting):**
  - Disk or sector encryption, sensitive credential store, drive locking
- Continuous protection against laptop loss and theft
- Facilitates easy re-purposing, end of life, and rapid erase
- Satisfies legislative/regulation compliance obligations
- No performance degradation (with hardware encryption)
- Considered more secure than software-based solutions
The National Security Agency (NSA) has approved a vendor laptop SED hard drive for protection of **sensitive and classified** information in computers deployed by U.S. government agencies and contractors for national security purposes.

**Other vendor SED drive qualifications expected to follow…**

*More information on NSTISSP #11 is available at [http://www.niap-ccevs.org/cc-scheme/faqs/nstissp-faqs.cfm#Question_1_5](http://www.niap-ccevs.org/cc-scheme/faqs/nstissp-faqs.cfm#Question_1_5).*
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

SATA
Hidden area
Master Boot Record
Self-Encrypting Drive Basics

The drive LOCKS automatically when powered OFF
The drive remains LOCKED when it is powered back ON
Authentication Key (Password) **Unlocks** the drive
Write and Read data normally while drive is unlocked

Data protected from loss, disclosure
Authentication in the Drive

Correct AK?

Hash AK

Clear AK decrypts DEK

Unlock HDD

DEK encrypts and decrypts User Data

Clear Data

Storage Server

Chip

Disc

Hashed AK

Encrypted DEK

Encrypted User Data

Self-Encrypting Drives
© 2009 Storage Networking Industry Association. All Rights Reserved.
**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
Client SED Deployment

Drive Manufacturer

Encryption key created
Encryption turned on
User password Not Initialized

System Manufacturer

Optional cryptographic erase (generate new encryption key)
Optionally integrate management software

Drive
Sold

System sold

SED Managers

Change master password(s)
Optional crypto erase before re-image
Set a default User password
Save new passwords

End User

User powers on, enters PWD
User changes PWD
Uses system normally

User returns system to IT for erase

IT department

Generate new encryption key to erase drive

Customer

System Delivered to end user

System Manufacturer

System sold
### ‘Hurdles’ to Implementing Encryption

<table>
<thead>
<tr>
<th>Key management / loss</th>
<th>Complexity</th>
<th>Performance</th>
<th>Cost</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>- Tracking and managing authentication keys (passwords for unlocking drives)</td>
<td>- Interoperability</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
- Data classification
- Impact on OS, applications, databases
- Interoperability

---

Self-Encrypting Drives
© 2009 Storage Networking Industry Association. All Rights Reserved.
No Performance Degradation

Encryption engine speed

Matches
Port’s max speed

The encryption engine is in the controller ASIC

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 - $14 million on average
- 90% of retired drives are still readable (IBM study)

Needed: A simple, efficient, secure way to make retired drive data unreadable
How the Drive Retirement Process Works

People make mistakes

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

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

- May 7, 2008 (Computerworld)


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

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**

Retirement Options:
- Overwriting takes days and there is no notification of completion from drive
- Shredding is environmentally hazardous
- Not always as secure as shredding, but more fun
- Hard to ensure degauss strength matched drive type
- Overwriting takes days and there is no notification of completion from drive

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)

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
Reducing Complexity for IT

Encrypting outside the drive

- Application Developers: May need to change applications
- OS: May change if encrypting in a driver
- Encryption engine: May need separate hardware
- Network: Heavyweight encryption can impact performance
- Key Manager: Installed on existing server
- Storage System: Data compression & de-duplication affected

Encrypting inside the drive

- Key Manager: Installed on existing server
- Storage System: Upgrade per schedule
At Initialization:
- Bring in new volume
- Set up Authentication Key

Power-up:
- Authenticate with the key source
- Pass key to the disk drive

After Power-up:
The storage system virtualizes the drives and provides:
- Data protection through RAID and copy services
- Availability through redundancy, failover drivers, robust error handling
- Capacity sharing through partitioning and network connectivity
- Management reporting
- Data compression and de-duplication best applied BEFORE encryption
Reducing Security Costs

- **Initial acquisition costs:**
  - Integrated into standard products
  - Implemented per standard storage upgrade schedule
  - Standards-based, and all drive vendors are participating in TCG
  - The drive industry has long demonstrated standards drive competition which drives cost
  - Economies of scale enable incremental logic in the ASICs to remain a small portion of drive material costs

- **Reduce drive decommissioning and insurance costs**

- **Maintain ability to compress and de-duplicate data**

- **Preserve drive hardware value**
  - Service, warranty, expired lease returns enabled
  - Drive repurposing enabled
## Addressing the Hurdles…

<table>
<thead>
<tr>
<th>Simplifies key management to prevent data loss</th>
<th>✓ Encryption key does not leave the drive; it does not need to be escrowed, tracked, or managed</th>
</tr>
</thead>
</table>
| **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 |
New IT policy: All future drive purchases to be self-encrypting drives when available

Beginning: SEDs for critical applications and routine storage upgrades
Ongoing: SEDs for ongoing routine storage upgrades
Eventually: All data, no matter where data resides, is stored securely

Eventually, ALL drives will be self-encrypting
The Future: Self-Encrypting Drives

- **Encryption everywhere!**
  - Ecosystem to extend from the 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
Thank You!
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

- Michael Willett
- Robert Thibadeau
- Eric Hibbard
- Gianna DaGiau
- Jason Cox
- All Storage Manufacturers (contributors)