Stop Data Breaches Now: Self-encrypting Drives for Enterprises

July 16, 2014 1:00PM EDT
No Sound?
This is a streaming audio event. Make sure the sound on your PC is turned on.

Questions?
Type your questions using the Ask a Question Text Box
Dr. Michael Willett, Storage Security Strategist, Samsung

Recently, Dr. Willett was a Senior Director at Seagate Research, focusing on security functionality on hard drives, including self-encryption, related standardization, product rollout, patent development, and partner liaison. Currently, Dr. Willett serves as a consultant on the marketing of storage-based security. Presently, Dr. Willett is working with Samsung as a storage security strategist, helping to define their self-encryption strategy across Samsung’s portfolio of solid-state storage products.

Andy Avery, Senior Vice President, Global Business Development and Vice President, APAC Sales, Wave Systems Corp.

Andy is responsible for driving new business both with current partners and customers but also developing new markets for Wave’s SED management solution Embassy Remote Admiration Server (ERAS), Virtual Smart Card, Trusted Platform Modules and Security Solutions in a SaaS environment. Andy is also responsible for security development and partnerships within the Asia Pacific region. With more than 20 years in the Security as a Software industry, Andy has also served in executive business development roles at Absolute Software and Go America, Inc.

Patrick Bright, Senior Technical Sales Engineer, CISSP, CISA, CompTIA Security+, MCP, Wave Systems Corp.

Darren Leroux, Senior Director, Product Marketing, WinMagic Inc.

Darren manages all product related content, communications and analyst relations for SecureDoc data encryption and security software. In this role, he oversees the creation of product-related materials, communications, public and analyst relations, sales interactions, roadmaps, competitive evaluations and delivers external presentations about WinMagic and it’s go to market strategies. He is also the company’s lead blogger at http://blog.winmagic.com.

With more than 15 years experience in the IT industry, Darren previously worked for Hewlett-Packard (Canada) Co. and Hill & Knowlton in their Technology Communications Practice
Agenda

- Solving the Data Encryption Problem
- What Are SEDs?
- Why Enterprises Should Consider SEDs
- Management of SEDs
- Case Study Examples of SEDs in Action
- Deployment Tips
Solving the Data Protection Problem
Security Practices Leave an Open Back Door

- 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.

Front Door Closed  Back Door Open…
Breaches Are Numerous and Costly

2005-2013: over 864,108,052 records containing sensitive personal information have been involved in security breaches

In 2013, U.S. businesses paid an average cost of $5.4 million per data breach; that’s $188 per record

$5.4 Million Per Incident

http://www.privacyrights.org/ar/ChronDataBreaches.htm
Breach Notification Legislation

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”
IT Retires Drives Constantly – Making Data Vulnerable

- **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

Self-encrypting Drive (SED) Basics
This means:

- Encryption is always on
- Encryption is transparent to the system user
- The encryption keys never have to leave the drive
- Authentication is done independent of an operating system
- TCG has created industry standards with input from drive makers, PC and enterprise storage vendors and ISVs
Why Encrypt Data-At-Rest?

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

- Compliance
  - 48+ U.S. states have data privacy laws with encryption “safe harbors”, which exempt encrypted data from breach notification\(^1\)
  - EU: Data Protection Directive 95/46/EC (27 countries) replaced with European Data Protection Regulation \(^4\): requires breach notification \(^3\)

- Exposure of data loss is expensive ($6.65 Million on average per incident\(^2\))

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

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

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

3. **Custom logic for faster, more secure operations**
   - Inexpensive implementation of modern cryptographic functions
   - Complex security operations are feasible
Why Enterprises Should Consider SEDs
Why Hardware Self-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

**New hardware acquisition (part of normal replacement cycle)**
TPAL is a TCG-developed standard for managing SEDs

- It is a common set of criteria that SED drive manufacturers follow to ensure compatibility
- OPAL criteria outline how an SED encrypts data and how they are managed
- OPAL essentially offers an interface specification for SEDs that makes enterprise-class management of SEDs possible

TCG also has created enterprise self-encrypting drive standards

- Vendors implement these standards
- Supported by many ISVs for management tools
SED Momentum

- Diminishing SED price differential
- Fast encryption and system performance
- Extremely secure and favored by Government
- Less susceptible to host hacking

SED Opportunity
Benefits of Opal SEDs

**Transparency**
- No need for kernel driver to encrypt
- No potential conflicts with other SW running on the machine
- No blue screens
- No conversion process – always encrypting

**Performance**
- Encrypt at full drive speed
- No CPU required to encrypt
- No draw on host computers resources
- No initial conversion required

**Security**
- Key never leaves the actual drive (no Cooled RAM attack)
- Read only Pre-boot authentication area (No Evil Maid Attack)
- Instant crypto erase for repurposing

**OPAL Standard supports wide range of Encryptions**
SED Management
Drives Need Management

As hardware-based encryption, and OS built-in encryption become more prevalent, there is a constant and definitive need for centralized management by a single management console.
• 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)
### 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 |
Case Study Examples of SEDs in Action
Barnabas Health Care System: SEDs in Action

• **Organization**
  - New Jersey’s largest integrated healthcare system
    - 25 functional facilities total
  - Provides treatment for >2M patients/year
  - 18,200 employees, 4,600 doctors

• **Environment**
  - 2,380 laptops, across 25 facilities
  - Adopted SED as standard for desktops this year (2011),
    - used by healthcare professionals and executives
    - distributed across 25 functional facilities
  - Protecting PII/PHI/diagnostic information
  - HP shop using Wave-managed Hitachi SEDs
BARNABAS HEALTH

- Encrypting 13,000 desktops used is the hospitals, via the asset lifecycle process in 4 years, 400 units expected to be done this year.

- **Key Findings:**
  - 24 hours faster deployment on average per user over previous software-based encryption
  - Negligible boot time versus up to 30 minutes to boot a PC with software encryption

- **Identify the data protection risks/requirements**
  - Regulatory requirement for data protection
  - Safe harbor exemption
  - Intellectual property/ Proprietary information protection

- **Build a business case**
  - Market place analysis
  - Embed into the asset lifecycle program to manage expense
Organization:

• The private, non-profit organization that manages the nation's organ transplant system
  • under contract with the federal government.
  • manages the national transplant waiting list
  • maintains database for all organ transplants in US
• 350 employees
Deployment environment:

- 200 laptops
- Regulated by Health Resources Services Administration
- 4 encryption projects over 5 years
  - Final project was SEDs
- Sensitive patient data to protect
Tips for Effective SED Deployment

- Understand the regulatory requirements for encryption
- Sell to upper management
- Review the many software versus SED encryption studies in the literature
- Identify the scope of stored sensitive data
- Review and select the best-fit management solution
- Roll out incrementally
- Analyze time/cost savings of the solution
The Future: Self-Encryption Everywhere

- **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

**Diagram:**
- Key Management Service
- Data Center Application Servers
- Storage System, NAS, DAS
- Network
- Trusted Computing Group T10/T13 Security Protocol
- OASIS KMIP
- Standard Key Mgmt Protocol
- Tape
- Storage System, Local Key Mgmt
- Notebook
- Desktop
- USB
- Authentication Key Flow
- Data Flow
- Authentication Key (lock key or password)
- Data Encryption Key (encrypted)
Questions?

Post your question now.
Data Security Architect’s Guide:
https://www.trustedcomputinggroup.org/resources/tcg_data_security_architects_guide

Case Studies:
  Boston Medical Center:
  https://www.trustedcomputinggroup.org/resources/wave_systems_case_sudy_boston_medical_center
  Mazda:
  https://www.trustedcomputinggroup.org/resources/mazda_north_american_operations

Storage Specifications:
http://www.trustedcomputinggroup.org/developers/storage/specifications

Interested in Getting Involved with TCG – Join Us:
http://www.trustedcomputinggroup.org/join_now