ARCHITECT'S GUIDE:

DATA SECURITY USING TCG SELF-ENCRYPTING DRIVE TECHNOLOGY

April 2013

Trusted Computing Group
3855 SW 153rd Drive
Beaverton, OR 97006
Tel (503) 619-0562
Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

Executive Summary and Action Items

With increasing global regulations for data security and the increasing consequences of non-compliance from privacy protection and breach notification laws, enterprises must take the appropriate steps to protect the data entrusted to them by others as well as their own proprietary corporate information.

Self-encrypting drives (SEDs) provide protection for data in storage and meet compliance criteria established by government agencies in the United States and around the world. SEDs demonstrate compliance with exemptions from breach notification laws by providing encryption 'safe harbor' protection.

This architect's guide focuses on the deployment of available SED products in the enterprise (both laptops and the data center), highlighting best practices for implementation in a variety of case studies.

Critical strategies for architects include:

1. **Purchase** all new laptops and enterprise data storage with SED drives
2. **Retrofit** high-risk legacy machines with SED drives
3. **Restrict access** to stored sensitive data to machines with SED drives in early rollout
4. When adding more drives to an array or more arrays to the data center, **use SEDs** to avoid concerns for balancing encryption workloads
5. **Phase in** SEDs into the data center
6. **Avoid or minimize** the need for data classification
7. **Be aware of and accommodate** other data security contexts, as required by statute or due diligence (e.g., transport – SSL/TLS)

Introduction

Today, self-encrypting drives (SEDs) designed to standards developed by the Trusted Computing Group (TCG) and based on built-in encryption hardware (HW) can protect data at rest in mobile products or in fixed assets within the enterprise. The on-board HW encryption provides a proven and recommended solution to the problem of data breach caused by lost or stolen storage devices containing private customer information or corporate confidential and propriety information.

Compelling Reasons. In 2002, California passed the first data breach law in the U.S., CA SB 1386[1]. Since then, a total of forty-six states as well as the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information, according to the National Conference of State Legislatures "State Security Breach Notification Laws" webpage[2].

The United States also has several federal laws for privacy protection. Well-known U.S. statutes include the Privacy Act of 1974, the Computer Security Act of 1987, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Act of 1999 (GLB), and the Sarbanes-Oxley Act of 2002 (SOX). In fact, many governments around the world have legislation regarding privacy. Forrester has rated each country[3] for the strength of its laws.

The consequences from losing confidential data can be severe. For example, according to Ponemon Institute's "2011 Cost of Data Breach Study: United States[4]," data breach incidents cost U.S. companies $194 per compromised customer record in 2011 with the average total per-incident cost of $5.5 million. The Ponemon Institute also has cost data for other countries.

Since 2005, the Privacy Rights Clearinghouse[5] reports that 607,234,229 records have been breached from unencrypted drives that were lost, stolen or hacked (as of Feb. 24, 2013). In addition to extensive media coverage, this site and several others identify the companies that have fallen victim to data breaches, creating an ongoing public relations nightmare and serious damage to corporations.

Safe Harbor. The majority of U.S. states and the European Union have safe harbor provisions in their statutes for secured and encrypted data. As a result, SEDs are an alternative to costly reporting, remediation, and fines.

SEDs provide encryption security, including a feature called Crypto Erase (see Solutions Overview), that makes them ideal for rendering their data unreadable. This capability is identified and officially recommended in Draft NIST Special Publication 800-88[7] Guidelines for Media Sanitization Revision 1, Recommendations of the National Institute of Standards and Technology.

Other Issues. Now, SEDs are available as stand alone or embedded units in a variety of computer products. All the major hard drive and solid state drive manufacturers have SED options in their inventory, for both laptop and the data center.

Managing the authentication keys is frequently cited as a concern. However, in SEDs, key management for locking/unlocking the drive is performed by available software from suppliers that have client and enterprise versions. And, since the encryption key is generated on board the SED during manufacture and never leaves the drive, the user does not have to manage the encryption keys at all (authentication/locking keys are managed by IT administrators).

---

[1] SB1386: http://leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

[2] State Security Breach Notification Laws: http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

[3] Privacy and Data Protection By Country For Security & Risk Professionals: http://blogs.forrester.com/chenxi_wang/12-02-21-data_privacy_heat_map_highlights_challenges_of_navigating_global_privacy_legislations

[4] 2011 Cost of Data Breach Study: United States: http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide__CODB_US

[5] Privacy Rights Clearing House "Chronology of Data Breaches," http://www.privacyrights.org/data-breach

[7] Draft NIST Special Publication 800-88: Guidelines for Media Sanitization: http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf

Storage Networking Industry Association (SNIA), the organization for advancing storage and information technology, that consists of about 400 member companies from the global storage market, has developed a nine-step checklist[8] for deploying encryption. As shown in *Table 1,* the steps are considerably simplified when using SEDs.

While the ability to protect stored data with an industry standard approach based on SEDs has been in place for several years, some individuals and corporations have made the decision to postpone that implementation, and many have paid a high price when the data was lost or stolen and breach notification was required. Given the maturity of the technology, broader product availability, and a proven record of protection, users are deploying increasing numbers of SEDs through the normal asset replacement cycle.

The following provides a brief summary of the typical steps for successful decision making and implementation of SEDs in an enterprise.

1. Obtain executive buy-in by establishing the business case for stored-data encryption, including:
   - Research and review breach notification legislation (and penalties)
   - Understand the typical cost of breach notification (Ponemon studies)
   - Target both IT and corporate executives to address compliance issues
2. Perform Risk Analysis based on a summary of classified/sensitive data kept on company laptops
3. Evaluate/compare alternate solutions:
   - Review/summarize studies on software-based versus SED encryption
   - Research existing SED solutions: ISVs and HDD/SSD
4. Implement staged deployment:
   - Start with small test bed to obtain experience with independent software vendor (ISV) management, user training/questions
   - Expand with incremental, prioritized deployment including normal inventory upgrades
   - Use Crypto Erase for drive sanitization
   - Perform periodic risk assessment

SNIA'S 9-STEP CHECKLIST

STEP	CHECKLIST	SIMPLIFIED BY SELF-ENCRYPTING DRIVES
1	Understand Drivers	Breach Notification Laws; due diligence for data protection
2	Classify Data Assets	Not needed at the data level; may classify USERS (e.g., executives, road warriors, etc.) to prioritize SED rollout
3	Inventory Data Assets	See (2) above
4	Perform Data Flow Analysis	Not needed
5	Choose Points-of-Encryption	Laptops and data center drives
6	Design Encryption Solution	SEDs
7	Begin Data Re-Alignment	Not needed
8	Implement Solution	Staged rollout and replacement with SEDs
9	Activate Encryption	Happens automatically and transparently

Table 1: Simplifying SNIA's 9-step checklist with SEDs.

[8] Implementing Stored – Data Encryption:
http://www.snia.org/sites/default/education/tutorials/2012/spring/security/MichaelWillett_Implementing%20Stored-Data_Encryption_2.pdf

Solutions Overview

For self-encrypting drives, the Trusted Computer Group's Storage Work Group developed two related solutions, one for notebooks/portables and the other for enterprise drives. TCG Storage Security Subsystem Class: Opal[9] and TCG Storage Security Subsystem Class: Enterprise Specification[10], define the security subsystem class (SSC) requirements for each. Using an OPAL SED as an example, *Figure 1* shows the steps for an installed SED start-up are:

1. The BIOS attempts Master Boot Record (MBR) read, but the SED redirects to the pre-boot area in hidden memory
2. The drive loads the pre-boot OS, which requests authentication by the user
3. The user enters authentication credentials for the drive to verify
4. If authentication is successful, the drive loads the original MBR
5. Normal operation commences with complete transparency to the user, including in-line encrypt/decrypt

Crypto Erase. As identified and recommended in Draft NIST Special Publication 800-88[7] Guidelines for Media Sanitization Revision 1, Recommendations of the National Institute of Standards and Technology, crypto erase is uniquely supported by SEDs.

With SEDs, unified, standards-based key management takes place within the drive controller. Encryption algorithms are based on the NIST FIPS 197 Advanced Encryption Standard (AES) with both AES-128 and AES-256 permitted. The drive can be easily and quickly sanitized using crypto erase.

With software encryption, deleting the key does not ensure that the data is inaccessible because several copies of the key could have been distributed and their ownership is unknown. With SED encryption, the encryption keys never leave the drive. Since the encryption key (itself encrypted) is stored in a location known to the drive logic, simply deleting/replacing the onboard key permanently removes it, so the encrypted data is unreadable and the drive can be reformatted and used for other purposes. The drive is not destroyed. Current SCSI and SATA standards support a standard command for crypto erase.

Crypto erase can be used in conjunction with normal business processes like drive replacement, repair, de-commissioning, re-purposing, and end-of-life.

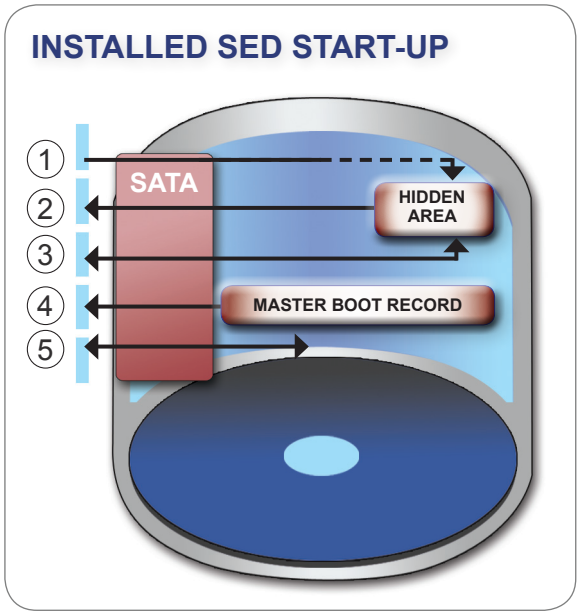

Figure 1: Pre-boot authentication of the SED user

Case Studies

SEDs have demonstrated their capability in numerous case studies. Documented studies in the healthcare industry, automotive operations, and engineering and consulting services provide examples of broad user acceptance.

Boston Medical Center one of New England's leading healthcare institutions and an early adopter of electronic medical records transitioned its fleet of 400 laptops to SEDs. After nearly 50 percent were upgraded, they already had found the SEDs:

- Quick to install
- Simple to administer and to remotely control security policies from a central location
- Virtually impossible to penetrate data security.

In addition, Saint Barnabas Health Care System, New Jersey's largest health delivery system, implemented SEDs in 700 laptops used by doctors, nurses, administrators, and executives in 25 facilities. They found:

- 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

[7] Draft NIST Special Publication 800-88: Guidelines for Media Sanitization: http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf

[9] TCG Storage Security Subsystem Class: Opal: https://www.trustedcomputinggroup.org/files/resource_files/B15F1F8F-1A4B-B294-D03F09D5122B21F6/Opal_SSC_2%2000_rev1%2000_final.pdf

[10] TCG Storage Security Subsystem Class: Enterprise Specification: https://www.trustedcomputinggroup.org/files/static_page_files/75FAE643-1A4B-B294-D061B8A67FBF525E/TCG_SWG_SSC_Enterprise-v1r3_Final.pdf

When Mazda North American Operations provided 200 laptops to its highly mobile field staff, it found that SEDs:

- Minimized time and expense to secure sensitive and confidential data on laptop computers
- Avoided help desk hassles with forgotten passwords
- Ensured centralized management of policy-based access controls and proof of compliance

VEGA Deutschland, a European engineering & consulting services firm, chose SEDs to secure confidential and classified information stored on 300 laptops distributed throughout Europe. It found that SEDs:

- Had lower cost to setup and maintain
- Avoided incompatibility with home-grown software
- Quick to install
- Simple to administer from a central location
- Virtually impossible to penetrate data security.

Solution Architecture

Today, SEDs are being implemented both in enterprises with Redundant Array of Independent Disks (RAID) controllers and servers in the data center as well as laptop/portable computers based on the two TCG specifications. Different scenarios exist for each.

OPAL SSC-based SEDs have a local management interface and preboot authentication, with local and centralized support through management software vendors. The Enterprise SSC-based SEDs operate in an automated environment, where the RAID controller performs the authentication automatically with centralized authentication key management (controller microcode has been modified to present the authentication keys to the SED) through products such as IBM's Tivoli and others.

Most major drive companies provide SEDs. For example, Seagate, Hitachi, Fujitsu, and Western Digital offer hard drive SEDs, while Samsung and Micron have solid-state SEDs, designed to TCG/OPAL. Such management software companies as Wave, WinMagic, Absolute, Credant, and McAfee manage TCG/OPAL SEDs. Seagate, Hitachi, and Fujitsu have Enterprise SSC-based SEDs for the data center.

Since the encryption engine in an SED is in the controller hardware, the port's maximum speed can be achieved without incurring any performance degradation (see sidebar: Hardware vs. Software-Implemented Encryption)

Key Management. Managing the authentication keys (or passwords) is one of the major issues that potential users had raised in the early availability of SEDs and one of the more important aspects of TCG's specification, since the authentication key unlocks the self-encrypting drive. However, multiple management vendors now provide easy-to-use solutions for flexible management of these keys. On the other hand, the encryption keys for the SED are established in manufacture by on-board random number generators (producing true randomness). The drive only stores the hash value of the authentication key for comparison during authentication. Encrypted under the authentication key and stored on the drive, the encryption key is never stored in the clear and never leaves the drive. The encryption key is decrypted every time the drive is unlocked, for use in the AES-based hardware.

Figure 2 shows key management for traditional encryption solutions outside the drive versus inside the drive using SEDs. With off-drive encryption option (A), the encryption keys are managed off-drive and encrypted data for different encrypting applications could be 'striped' across multiple drives. With on-drive encryption (B), no upstream encryption key management is needed.

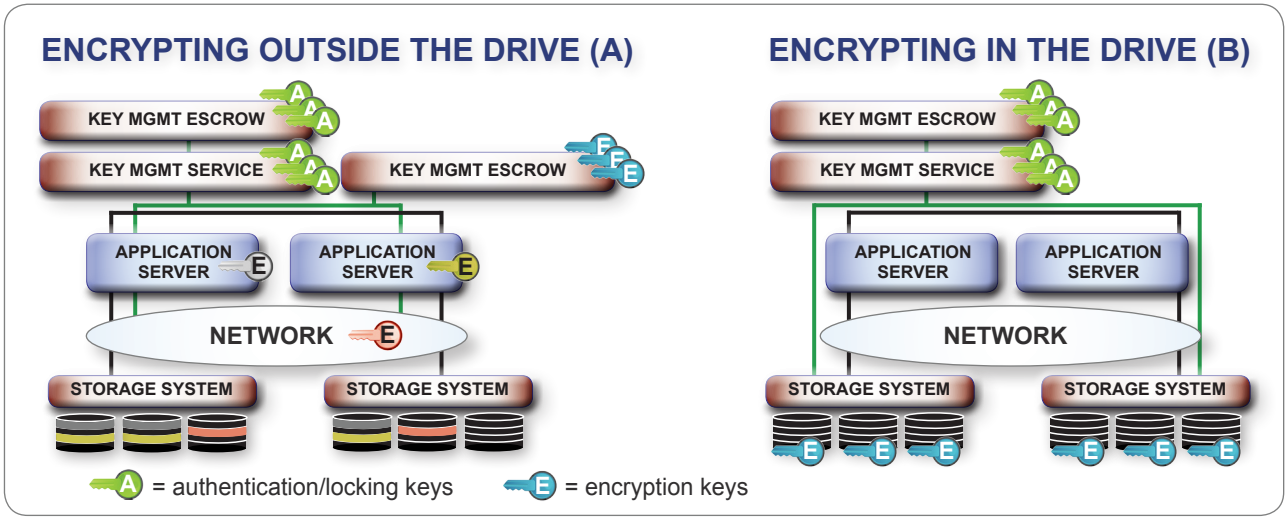

Figure 2: Encrypting outside of the drive versus simplified key management using SEDs

Future

The numerous advantages of SEDs for encrypting and protecting data and the increasing availability in drives and computers from several suppliers have industry experts extremely optimistic for SED market acceptance. A 2011 market analysis for SEDs from Coughlin Associates[11] projected that:

- By 2017, all hard drives will be SED capable with encryption integration into the controller (As a reference point, over 25 percent were SED enabled in 2011)
- By 2013[12], 80 percent of SSDs will be SED capable and by 2014, penetration will near 100 percent

In the future, some analysts expect that all enterprise drives will be self-encrypting based on requirements from industry organizations. *Figure 3* shows the vision for self-encrypting storage in the enterprise.

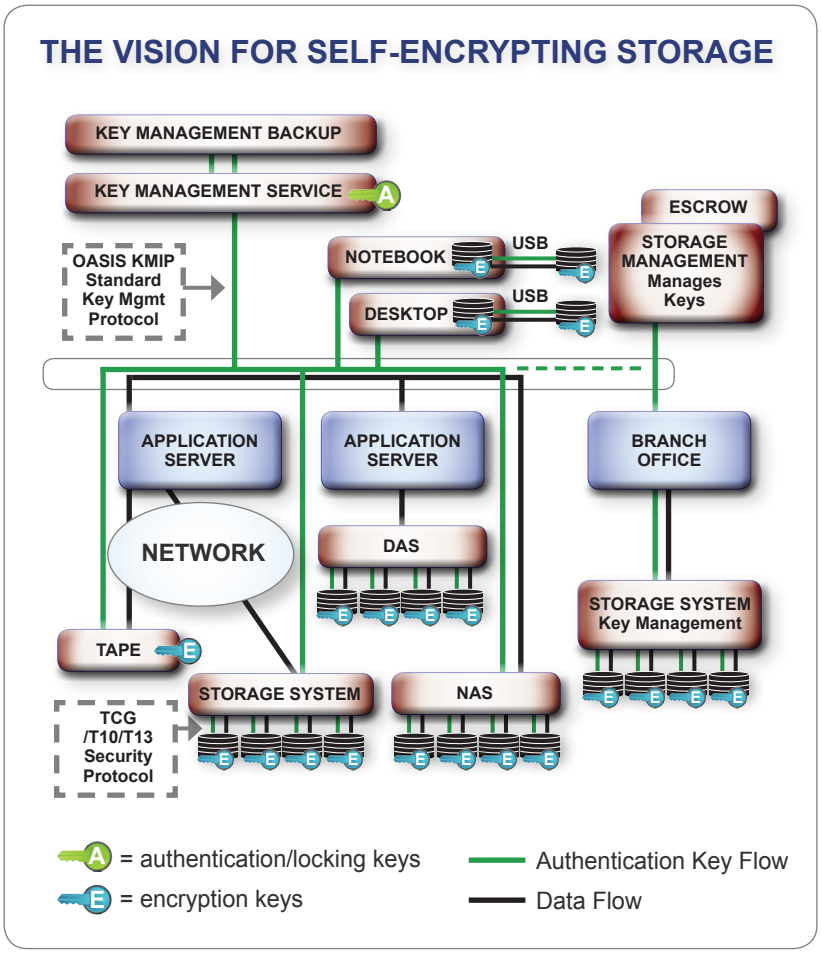

Figure 3: The vision for self-encrypting storage is protection for all data stored in the enterprise

[11] Coughlin, Tom, "Self-Encrypting Drive Market and Technology Report": Coughlin Associates, August 2011,http://www.trustedcomputinggroup.org/files/resource_files/8CA99975-1A4B-B294-D0D425207CA04BAA/Self-Encrypting_Drive_Market_and_Technology_Analysis.pdf

[12] Solid Security: The Rise of Self-Encrypting Solid State Drives: http://www.snia.org/sites/default/files/Solid%20Security%20012412.pdf

Conclusions

To cope with global requirements for data privacy and avoid the resulting penalties for data breaches, all electronically stored data needs to be encrypted. With the demonstrated advantages of hardware-based encryption over software-based implementations, SEDs status as a maturing technology and availability from numerous industry leading sources make them the preferred solution for encrypting stored data.

The bottom line is that enterprises need to implement a hardware-based SED solution to encrypt their data now. Waiting rather than taking action could result in a company's name and public exposure being added to the corporate data breach lists and could cost millions of dollars.

Hardware vs. Software-Implemented Encryption

Self-encrypting drives solve the major problems that plague software encryption solutions, such as complexity, interoperability, scalability, non-transparency, decreased system performance, and fear of lost keys.

Regarding the performance advantages, encryption performed in SED hardware matches the drive port's maximum speed, avoiding performance degradation common with software approaches. Since the encryption technology is built into the drive, it is transparent, and scales linearly and automatically. For greater system simplicity, no changes are required in applications, databases or the operating system (OS). In addition, unlike software that has continuing life cycle costs, the cost of an SED is pro-rated into the initial drive cost.

An independent comparison[13, 14] of hardware versus software encryption has shown that hard-drive SEDs delivered 115 percent higher read throughput than the average of the SW encryption products and 43 percent higher write throughput.

Solid-state (SS) SEDs provide an even more dramatic comparison of software versus hardware encryption. Tests have shown that large-scale data read increases from 70.23 to 169.33 megabytes/sec (MB/s) when a solid-state drive uses hardware-based SED technology instead of software. Large-scale data write increases from 63.60 to 164.50 MB/s. This is an improvement of 2.4 times for read and 2.6 for write performance.

[13] Bosen, Bill, "FDE Performance Comparison: Hardware Versus Software Full Drive Encryption," http://www.trustedstrategies.com/papers/comparing_hardware_and_software_fde.pdf

[14] "Full Drive Encryption with Samsung Solid State Drives: A performance and general review of Samsung's new self-encrypting solid state drives," Trusted Strategies white paper: http://www.trustedstrategies.com/papers/fde_samsung_ssd.pdf