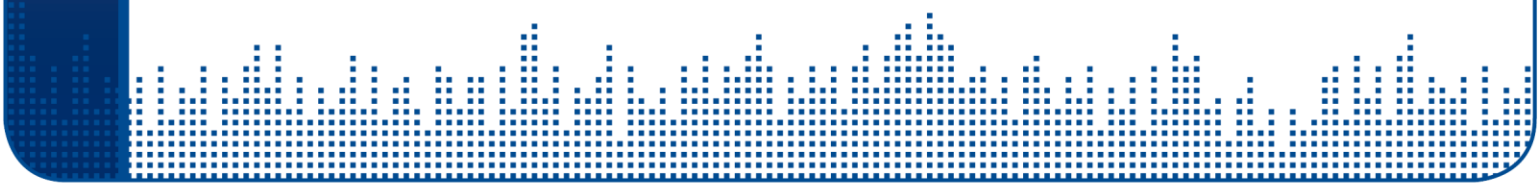
Solving the Data Security Dilemma with Self-Encrypting Drives

May 2010

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



Solving the Data Security Dilemma with Self-Encrypting Drives

As global regulations for data security increase in number and the consequences of non-compliance increase in severity, the ability to secure data has improved and actually become easier with the latest automatically implemented technology. Self-encrypting drives (SEDs) designed using an open industry standard developed by the Trusted Computing Group (TCG) provide protection for data at rest and in transit and meet criteria established by government agencies around the world. However, even with the latest regulations, loopholes exist that may allow users to comply with the regulations but not meet the intent of the laws resulting in inadequate data protection.

Existing Regulations and Compliance Issues

Today's laws that involve data security and breaches, such as the Federal Data Breach Notification Act introduced in January 2009[1], identify data encryption as a technique to avoid the fines and penalties associated with the loss of digital data. In the worst case, the encryption could be something very simplistic that does not prevent even an unsophisticated thief from decoding it. The regulations that have been written to provide more detail for improved solutions are also inadequate and filled with holes. Some suppliers can satisfy the regulations without actually fulfilling the intent of the law. Those entities taking the cheapest route may still be exposing their customers' data.

One of the complications of using NIST's globally-respected knowledge and processes involving cryptography fundamental to digital data encryption is two different specs that address cryptography. NIST initially developed the Federal Information Processing Standardization (FIPS) 140 that details the requirements of cryptographic modules, a module that can service cryptographic requests. A cryptographic module may be accessed through a specific key but it will not let a user know the key.

NIST was one of the contributors to Common Criteria for Information Technology Security Evaluation or Common Criteria (CC)[2] to handle those cases when the security device is not a cryptographic module, although it may perform a security or other type of cryptographic function. For example, software does not satisfy the requirements of a cryptographic module. The more general certification of Common Criteria applies when FIPS requirements are not applicable.

In either case, users need a federally certified product. A test suite on the NIST site, allows the certification of a particular piece of cryptography[3] for example, symmetric key AES (Advanced Encryption Standard), where an independent lab has confirmed the validity of the solution and provides a NIST certification. AES is widely available and source code can be easily downloaded from many web locations, so it provides a viable solution today. Users purchasing products without this lower level certification of individual cryptographic components could experience problems. Unfortunately, the recently enacted Health Information Technology for Economic and Clinical Health (HITECH) Act[4] allows approaches other than a federally certified one.

Globally, the U.S, and Japan are focused on the most recent FIPS version, FIPS 140-2[5], whereas the rest of the world has essentially chosen Common Criteria as a more flexible standard for cryptography. The difference is

---

[1] S139 Data Breach Notification Act http://www.govtrack.us/congress/bill.xpd?bill=s111-139

[2] Common Criteria http://www.commoncriteriaportal.org/

[3] Cryptographic Module Validation Program (CMVP) http://csrc.nist.gov/groups/STM/cmvp/

[4] Health Information Technology for Economic and Clinical Health (HITECH) Act http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

[5] FIPS 140-1 Security Requirements for Cryptographic Modules Standard http://www.itl.nist.gov/fipspubs/fip140-1.htm

that FIPS explains the threats, identifies the security objectives, and defines the requirements to meet those security objectives and thwart the threats.

Today, users can simply meet the standards or go beyond and have solid data protection. To address this conflict, the Aberdeen Group's recent report, "Full-Disk Encryption on the Rise"[6], recommends that to achieve Best-in-Class performance in endpoint encryption, companies "should adopt a risk-based rather than a regulation-based approach to IT security." The risk-based approach provides improved data protection choosing full-disk encryption that occurs automatically (i.e., a self-encrypting drive) as an integral part of centralized encryption management, over user-selected encryption and piecemeal-implemented alternatives.

Encryption Techniques and Applications

Most of the established encryption techniques for enterprise computers are based solely on software. However, the Trusted Computing Group has developed several open standards to protect data based on hardware. Hardware-based solutions are more robust and immune to external software attacks. Comprised of technology experts from member companies, TCG's first standard was the Trusted Platform Module or TPM[7] [7]. The TPM provides a hardware basis, usually through an application specific integrated circuit (ASIC), for protecting computers. The TPM's capabilities include trusted cryptography, protected storage, integrity management, and attestation through natively supporting public key infrastructure (PKI) authentication. The TPM has been installed in over 200 million desktop and portable computers and is an integral part of essentially every enterprise level computer being shipped today.

Since it performs cryptography as a service, a TPM is a cryptographic module. In addition, the many TPM's are certified to at least an augmented Evaluation Assurance Level (EAL) 4 against the international Common Criteria certification standards. In 2010, the TPM 1.2 also became an International Organization for Standardization (ISO) standard, ISO/IEC standard 11889.

More recently, TCG's Trusted Storage work group developed and announced specifications for Trusted Storage. The TCG Storage Security Subsystem Class (OPAL) Specification released in 2009[8] [8] details the requirements for self-encrypting drives. SEDs automatically encrypt all data in the drive, preventing attackers from accessing the data through the operating system. These drives can be coupled with TPMs to add strong machine authentication through the TPM's binding and authentication capabilities.

Besides being more vulnerable than hardware-based encryption techniques, software-only encryption can significantly slow the operation of the computer. A recent white paper[9] [9] evaluated the difference between hardware and software for full-drive encryption, comparing three different software products to an SED and a regular drive. One of the conclusions of the report was that unlike software encryption, the performance of SEDs was comparable to standard drives in all cases so "there is simply no incentive for users to remove or bypass the encryption, even if it were possible." This performance level makes SEDs suitable for all of the well-known applications for protecting sensitive data such as health care, financial institutions, and governments as well as corporations and any entity with a need for secure data.

Managing Encrypted Drives and Their Data

---

[6] Brink, Derek, September 2009, "Full-Disk Encryption on the Rise," Aberdeen Group report, http://www.aberdeen.com/summary/report/benchmark/6190-RA-full-disk-encryption.asp

[7] Trusted Platform Module http://www.trustedcomputinggroup.org/developers/trusted_platform_module

[8] Trusted Computing Group Storage Security Subsystem Class (OPAL) Specification http://www.trustedcomputinggroup.org/developers/storage

[9] Bosen, Bill, Feb. 9, 2010, "FDE Performance Comparison: *Hardware Versus Software Full Drive Encryption,"* Trusted Strategies white paper http://www.trustedstrategies.com/papers/comparing_hardware_and_software_fde.pdf

Simply having encryption software and/or hardware on a portable product is insufficient evidence to avoid the penalties of a data breach. To meet the terms of the current laws, the owner must prove that the laptop was encrypting at the time of the data breach. This requires enterprise data logs to verify that the laptop was encrypting all the data on the disk drive the last time it touched the enterprise network.

Software, such as Wave System's Embassy Remote Administration Server, can provide the required data logs for encrypting drives. This software allows organizations of any size to centrally manage numerous remote computers and maintain logs that can prove that the laptops were currently being managed for encryption to avoid a data breach notification issue.

Other companies offer enterprise management software for encryption. At least one supplier's management tool keeps logs and others may as well. In the event of a stolen, lost or misplaced laptop, the central management software must provide a data log.

Recommendations for Securing Data

While laws exist around the world for data protection, and encryption has been defined as the means of avoiding data breach notification penalties, the situation is far from being clear. Companies can comply with regulations and meet the laws but not necessarily fulfill the intent of the laws. New laws and regulations have been written and finalized/approved within the last year that could impact a company's data protection efforts. In addition, there are ongoing efforts for improving future regulations.

Self-encrypting drives have the ability to go above and beyond the regulations without reducing processing performance or experiencing the vulnerability of software-only encryption schemes. At least one FIPS-approved SED has been certified to meet the Federal Law and, soon, other FIPS-approved drives will be available to meet the laws and provide a high level of data protection.

For more information, go to www.trustedcomputinggroup.org