Are You Using Full Disk Encryption Yet?

What You Need to Know for Safe Harbor Protection Under US Breach Notification Laws

Kenneth G. Hartman
www.KennethGHartman.com
www.self-encryptingdrives.com

Contents

Disclaimer

This document is not intended to be considered legal advice. Consult qualified lawyers regarding the specific legal requirements of your jurisdiction. This document discusses our understanding of what constitutes due care for full disk encryption from a technical perspective.

Background

Over the past decade, breach notification legislation has been an accelerating trend. Since California enacted the first breach notification law in 2002, at least forty-six states have passed legislation that requires notification of security breaches that involve personally identifiable information [1]. It seems that the barrage of disclosures in the public media is creating appropriate concern about the security practices of the organizations that collect and manage our personal information [2]. Much of the recent media attention has focused on breaches of personal health information. This is driven primarily by the *HITECH Breach Notification Interim Final Rule* which requires timely notification of affected individuals, and the notification of the media where the breach affects more than 500 individuals [3].

The U.S. Congress was explicit about their intent to use media notification as a significant motivator when they drafted HITECH: *"By imposing a duty on all covered entities to notify affected individuals of breaches of protected health information, the statute and the interim final regulation place a similar burden on all covered entities to notify affected individuals and* ***run the same risk of losing business as a result of notification****. Moreover, requiring breach notification* ***creates an incentive*** *on all covered entities to invest in data security improvements in efforts to minimize the possibility of reportable data breaches* [3]*."* Many expect the public policy work that is being done on the HITECH Breach Notification rule to serve as a template for a national breach notification to standardize how other data breaches are handled. In fact, the Obama administration just released a cyber-security policy proposal on May 12, 2011 outlining national guidelines for the consideration of Congress [4].

Encryption is considered a best practice safeguard against theft or loss of private data because encryption transforms the data info a format that is unreadable without expending considerable resources to break the encryption. Encryption is the scrambling of data, called 'plaintext' into unreadable 'ciphertext' using a well-known mathematical transformation and some secret information called a 'key.' The protection results from the fact that the transformation is irreversible without the key. Attempts to break the encryption generally focus on repeated attempts to guess the key because the algorithm has withstood the tests of time and public scrutiny.

Proper implementation of data encryption technology can provide safe harbor from both state and federal laws requiring public data breach disclosure in the event that a computer is stolen [5]. One estimate puts the cost of a typical breach at $200 per compromised record [6]. Besides regulations such as HIPAA, HITECH, Sarbanes-Oxley, and Graham-Leach-Bliley, compliance with PCI is becoming an ever increasing driver. PCI failures mean that an organization cannot process credit card transactions [7]. The Ponemon Institute's *2010 Annual Study: U.S. Enterprise Encryption Trends* report states that:

> "In past years, concerns about mitigating data breaches and protecting data itself drove encryption implementation. For the first time, companies' main reasons for deployment now focus on thwarting pre-breach attacks and avoiding post-breach legal noncompliance penalties [7]."

The Ponemon report also concluded that:

> "For these reasons and others, these organizations are starting to view encryption technologies as mission-critical strategic investments and are slowly dedicating more money toward implementing them. [7]"

And

> "The research reinforces best practices for encryption and arguments that those practices provide a positive return on investment [7]."

Why Full Disk Encryption?

Unless every hard drive that is connected to a computer is completely encrypted, there is no way to be absolutely certain that the protected information was stored in an encrypted state. Even if individual files are encrypted without encrypting all hard drives, the computer operating system may leave chunks of sensitive data in unencrypted system files that users are completely unaware of.

If the device is stolen, how completely certain can you be that all of the sensitive data was encrypted at the time of the theft unless all hard disks are encrypted with full disk encryption? [8] With full disk encryption all of the encryption occurs without user intervention, thus eliminating the dependence on human diligence.

Hard Drive Protection Methods

There are three common password protection mechanisms that should not be mistaken for encryption and in reality, provide only limited protection. These are using an operating system password, a BIOS[1] password, or a hard disk password.

Operating System Password

The operating system will only provide protection to data if the operating system is running. A common technique to circumvent this protection is to boot to an alternate operating system, such as from a LiveCD. [9]

BIOS Password

A BIOS password is a password that must be entered before the system will boot the operating system. However, these are very easy to circumvent. Many BIOS's have well-known backdoor passwords and some can be reset by simply removing the CMOS battery. Also, remember that an attacker can simply just remove the hard drive and attach it to another computer. [10]

[1] BIOS is an abbreviation for the Basic Input Output System. It is software that instructs the computer on how to do a variety of basic functions, including how to load the operating system and the power-on self-test (POST). Certain information used by the BIOS, such as the current time, is stored in CMOS. CMOS is a type of integrated circuit chip. This information is preserved by what is referred to as the "CMOS battery" and it looks like a battery used for hearing aids.

Hard Disk Passwords

The BIOS of most modern computers also allow a password to be set for each of the connected hard drives. This password is stored in the service area of the hard disk. Because of this, moving the password protected hard drive to a new computer does not allow access to the hard drive unless the password that was assigned to the hard drive is provided. [11] The *ATA Security Mode Feature Set* that is implemented in all modern hard drives actually provides for two passwords, a "Master Password" and a "User Password" [12] The User Password locks the hard drive and the Master Password is only used to allow an administrator to reset the user password. [13] The BIOS of many computers will not allow the master password for the hard drive to be changed from the default, so they rarely are. A quick search of Google.com for the specific model of hard drive with the phrase "ATA Master Password" will generally result in multiple web pages that contain the default master password. There is also an online service [14] that will reset a single hard drive password for under $50 using a downloadable software application. Hardware tools can recover, reset, or brute-force both the User and Master Passwords [15] [16].

Full Disk Encryption Methods

There are two major categories of full disk encryption (FDE)—software-based and hardware-based. Software-based encryption modifies the hard drive drivers and uses the CPU to encrypt all data as it is written to the drive and decrypt all data read from the hard drive. Hardware-based full disk encryption is built into the hard drive and is totally transparent to the user and does not impose a performance impact on the computer. [11]

Software-Based Full Disk Encryption

Wikipedia maintains a lengthy list of disk encryption software [17]. The two most popular FDE software implementations are TrueCrypt and BitLocker. BitLocker is included as a feature in the Ultimate and Enterprise editions of Microsoft Windows Vista and Windows 7, but has to be enabled and configured to provide protection. TrueCrypt [18] is free open source software that is ideal for individual users, but lacks management features that make it attractive to enterprise-wide deployment. [19]

Deployment of software-based full disk encryption in any organization with more than just a few computers requires careful consideration of how the encryption keys will be managed. Great encryption without proper key management is like locking the doors to your house and leaving the key under your doormat. One study on the usage of encryption states that 54 percent of respondents had experienced either stolen or unaccounted for encryption keys and that 78 percent experienced system downtime due to encryption failures in the past twelve months [20]. Full Disk Encryption solutions that are targeted at the enterprise typically offer integration with Microsoft's Active Directory or other LDAP directories for secure key management.

In 2008, security researchers created shockwaves by publishing a paper called *Lest We Remember: Cold Boot Attacks on Encryption Keys* [21]. This paper, and the accompanying YouTube video [22], demonstrate how Software-Based FDE can be circumvented by rebooting a computer that has been left in a locked-screen or sleep state. The attack exploits the fact that Dynamic Random Access Memory

(DRAM) may retain memory for up to a minute after the computer has powered down and that booting the computer into a software tool allows the residual data to be captured and analyzed. One of their more astounding discoveries is that the Trusted Platform Module (TPM), which is used by some FDE software such as BitLocker, may actually facilitate the attack if TPM is not configured to require the entry of a password or the insertion of a USB key at start up. The authors called their proof of concept software "BitUnLocker" and have posted the source code on their website. Now there is at least one commercially available forensic tool that automates this attack [23].

The security researchers recommend avoiding the use of sleep mode and maintaining physical control of the computer in the first few moments after the system has powered off. The computer can also be configured to perform a test of the RAM during the power-on self-test (POST) that occurs prior to booting to an operating system. This effectively clears the DRAM.

The cold boot attack vulnerability is sensational, but proper configuration of software-based full disk encryption in conjunction with user awareness provides for a very reliable level of security [24].

Hardware-Based Full Disk Encryption

Since the Trusted Computing Group released the specification commonly known as "Opal" [25] in 2009, many manufacturers are producing self-encrypting drives (SEDs). This includes Seagate, Toshiba, Samsung, Fujitsu, and Hitachi [26]. In a SED, the encryption logic is built into the drive electronics. SEDs scramble the data as it is being written to the drive and unscramble it as it is read using an AES encryption key. [27] The keys and encryption functions are isolated in the disk drive subsystem, protected from malware because they are not accessible by the operating system. A BIOS level password is used to authenticate the user to the SED. [28] A number of third party management software vendors have stepped up to provide enterprise deployment and central management tools for self-encrypted drives [29]. Typically pre-boot authentication software loads and can accept either the administrator or a user account to unlock the hard drives encryption keys before the operating system boots. The user credentials can be synched with Active Directory so that after the pre-boot authentication, the credentials are then passed to the operating system so that the user will not need to authenticate again [8].

Self-encrypting drives offer some attractive features. For example, the drive is automatically locked when it is removed from a system or powered down and the drive can be securely erased in a fraction of a second by the cryptographic erasure of the data encryption key [30]. But perhaps the most attractive feature to the average user is that the performance impact of a SED is negligible as compared to a similar hard drive. Contrast this with software-based full disk encryption, which can exact an average performance impact of 32% [31].

On May 4, 2011, the Ponemon Institute release a study called *Perceptions about Self-Encrypting Drives: A Study of IT Practitioners* that surveyed 517 experienced IT practitioners who were familiar with self-encrypting drive technology. A full 70 percent believe that SEDs "would have had an enormous and positive impact on the protection of sensitive and confidential data" with a majority of respondents believing that SED's provide a faster set-up time as well as enhanced scalability in multi-drive configurations. [27] Seagate expects their sales to continue to surge, having just shipped their one

millionth SED in February, 2001 [32]. This is corroborated by the Ponemon study of IT practitioners, which states in its conclusion, "As understanding and awareness about the capabilities of hardware-based encryption versus software-based encryption grows, we predict that there will be greater adoption of SEDs [27].

Conclusion

Breach notification laws as well as other regulations are driving the use of encryption technologies to protect data at rest. Operating system passwords, BIOS passwords, and Hard Disk Passwords are protection technologies that do not provide adequate data protection unless used in conjunction with FDE, and therefore do not afford safe harbor protection under US breach notification laws. Unless all drives attached to a computer system are encrypted using FDE and not just specific files or folders, security is weakened by residual data in the unprotected disk space that the user may not even be aware of. Software-based full disk encryption is a valid option for legacy systems that cannot be transitioned to the use of self-encrypting drives. However, users must be aware that they must maintain physical control over the computer while it is powered on and the sleep mode should not be used.

A growing consensus is considering self-encrypting drives to be a better option in terms of manageability and user experience. However, one should resist the temptation to consider SED a silver bullet. Full disk encryption should be considered only one component of a defense-in-depth security program along with awareness, physical security, minimal use, and file encryption among other countermeasures.

This article has delved into a variety of considerations for the implementation of full disk encryption, with an emphasis on protecting the confidentiality and integrity of information at rest. Security is also about availability. If an organization cannot recover the information on an encrypted laptop when the employee to whom it was issued is unavailable, that predicament is also a failure of the security program.

References and Resources

[1] National Conference of Legislatures. (2010, October) State Security Breach Notification Laws. [Online]. http://www.ncsl.org/Default.aspx?TabId=13489

[2] Samuelson Law, Technology & Public Policy Clinic. (2007, December) Security Breach Notification Laws: Views from Chief Security Officers. [Online]. http://www.law.berkeley.edu/files/cso_study.pdf

[3] United States Deptartment of Health and Human Services, "Breach Notification for Unsecured Protected Health Information; Interim Final Rule," *Federal Register*, pp. 42740-42770, August 2009.

[4] Elizabeth Montalbano. (2011, May) Information Week Government, "White House Seeks National Data-Breach Notification Law". [Online]. http://www.informationweek.com/news/government/policy/229500626

[5] Seagate. (2008, July) Seagate Solution Center, "Seagate Secure™ Technology Enables Robust Security Within the Hard Drive". [Online]. http://www.seagate.com/staticfiles/docs/pdf/security/Tech_Paper_Enables_Robust_Security.pdf

[6] Ponemon Institute, "2009 Annual Study: U.S. Cost of a Data Breach," January 2010.

[7] Ponemon Institute, "2010 Annual Study: U.S. Enterprise Encryption Trends," November 2010.

[8] Greg Shipley. (2009, September) Information Week, "Full Disk Encryption Evolves". [Online]. http://www.informationweek.com/news/security/encryption/220200076

[9] BackTrack Linux. [Online]. http://www.backtrack-linux.org/

[10] Tech-FAQ, "How to Reset a BIOS Password". [Online]. http://www.tech-faq.com/reset-bios-password.html

[11] Bill Bosen. (2007, September) Computer Technology Review, "Hard Drive Passwords Easily Defeated; the Truth about Data Protection". [Online]. http://www.wwpi.com/index.php?option=com_content&view=article&id=2669:hard-drive-passwords-easily-defeated-the-truth-about-data-protection&catid=125&Itemid=2700162

[12] The X3T13 Technical Committee. (1997, January) AT Attachment-3 Interface (ATA-3). [Online]. http://www.t13.org/documents/UploadedDocuments/project/d2008r7b-ATA-3.pdf

[13] Harald Bogeholz. (2005, April) Free Republic, "How ATA security functions jeopardize your HD data". [Online]. http://www.freerepublic.com/focus/f-chat/1376364/posts

[14] AFF Repair Station. [Online]. http://hdd-tools.com/products/rrs/drives/

[15] Storage Heaven. Shinobi Password Remover. [Online]. http://store.storageheaven.com/shinobipasswordremover.aspx

[16] Atola Technology. Atola Insight. [Online]. http://atola.com/products/insight/

[17] Wikipedia. Comparison of disk encryption software. [Online]. http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software

[18] TrueCrypt. [Online]. http://www.truecrypt.org/

[19] Serdar Yegulalp. (2009, December) Information Week, "Getting Started With Full Disk Encryption". [Online]. http://www.informationweek.com/news/infrastructure/reviews/222001071

[20] Venafi. 2011 Enterprise Encryption Key and Digital Certificate Management Market Outlook. [Online]. http://www.venafi.com/collateral_library/2011-Enterprise-Key-and-Certificate-Management-Market-Survey-Outlook-Venafi.pdf

[21] Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten J. Alex Halderman, "Lest We Remember: Cold Boot Attacks on Encryption Keys," in *Proc. 2008 USENIX Security Symposium*, February 2008. [Online]. http://citp.princeton.edu/pub/coldboot.pdf

[22] Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. J. Alex Halderman. YouTube. [Online]. http://www.youtube.com/watch?v=JDaicPIgn9U

[23] Passware. Passware Kit Forensic 10.5. [Online]. http://www.lostpassword.com/kit-forensic.htm

[24] Secude. (2009) "Don't Panic–Cold Boot Reality Check, Understanding DRAM Attacks". [Online]. http://www.secude.com/html/fileadmin/files/pdfs/WPs/SECUDE_WhitePaper_DRAMAttacks_EN_090521.pdf

[25] Trusted Computing Group. (2009, January) TCG Storage Security Subsystem Class: Opal. [Online]. http://www.trustedcomputinggroup.org/files/static_page_files/9FE14508-1D09-3519-AD7D21A695E9B8EE/Opal_SSC_1.00_rev3.00-Final.pdf

[26] Aly Sidi. (2011, April) Security Director News, "SED 101: What security practitioners need to know about self-encrypting hard drives". [Online]. http://www.securitydirectornews.com/blogsi/?p=1105

[27] Ponemon Institute. (2011, April) Trusted Computing Group, "Perceptions about Self-Encrypting Drives: A Study of IT Practitioners". [Online]. http://www.trustedcomputinggroup.org/files/static_page_files/B759606E-1A4B-B294-D0A0450F23FC8836/TCG%20Executive%20Summary.pdf

[28] J.D. Hietala. (2007, September) Hardware versus Software, A Usability Comparison of Software-Based Encryption with Seagate Secure™ Hardware-Based Encryption. [Online]. http://www.seagate.com/docs/pdf/whitepaper/Seagate-crypto-bakeoff.pdf

[29] Trusted Computing Group. "Self-Encrypting Drives Take off for Strong Data Protection". [Online]. http://www.trustedcomputinggroup.org/community/2010/03/selfencrypting_drives_take_off_for_strong_data_protection

[30] Seagate. "Protect your data with Seagate Secure™ Self-Encrypting Drives". [Online]. http://www.seagate.com/www/en-us/products/self-encrypting-drives/

[31] Seclude. "Closing the Legacy Gap". [Online]. http://www.secude.com/html/index.php?id=migration-hardware-fde&L=0

[32] Seagate. "Seagate Tops 1 Million Mark In Shipments Of Self-Encrypting Hard Drives For Laptop PC's And Data Center Servers". [Online]. http://www.seagate.com/ww/v/index.jsp?locale=en-US&name=1-million-self-encrypting-drives-shipped-seagate-pr&vgnextoid=aaa1e1cf2a11e210VgnVCM1000001a48090aRCRD