SANS ANALYST PROGRAM

Sponsored by Seagate

Hardware versus Software

A Usability Comparison of Software-Based Encryption with Seagate DriveTrust™ Hardware-Based Encryption

A SANS Whitepaper – September 2007

Written by: J.D. Hietala

Introduction

Significant data breaches involving lost or stolen laptop computers have caused increased interest in encryption as a data protection mechanism. This paper explores the factors driving adoption of encryption in laptop and desktop systems and then compares two different approaches to providing encryption, software-based and hardware-based.

The results of a hands-on evaluation test of two products that are representative of the two approaches are also presented.

The evaluation explores setup and configuration, usability, performance, and system management characteristics of a system using a leading software-based encryption application, and of a system with hardware-based full disk encryption.

For its hardware-based example, this paper describes the types of cryptographic applications we're likely to see developed on top of the Seagate DriveTrust™ platform. Independent Software Vendors (ISVs) and laptop manufacturers are already creating security applications and management systems that leverage DriveTrust. Future support from software vendors in the identity and access management and single sign-on spaces can be expected, as the ability to securely store identity credentials is critical for these applications.

The Business Requirement for Disk Encryption

Now more than ever, businesses need to ensure that their information security controls extend to data stored on laptop and desktop computers. To anyone following the headlines on security breaches related to lost or stolen computers, the need for encryption of data at rest is obvious. Below is a matrix of just some of the publicly-disclosed security events involving missing or stolen computers containing personal information on customers, employees, or patients, which occurred April through June 2007:

Ohio Bureau of Workers Comp. (439 personal records)	**Concordia Hospital (3,000 patient records)**	**Pfizer (17,000 employee records)**
Bank of America (unknown number of names, SSNs)	**Northwestern University (unknown number of names, SSNs)**	**Highland Hospital (13,000 personal records compromised)**
Texas Commission on Law Enforcement (229,000 personal records)	**Louisiana State University (750 student records)**	**University of New Mexico (3,000 student records)**
Caterpillar (unknown number of employee names, SSNs)	**Baltimore County Dept. of Health (6,000 names and SSNs)**	**Ohio State University (14,000 names and SSNs)**

For a full years' list of recorded privacy exposures go to www.attrition.org

According to the 2006 CSI/FBI Computer Crime and Security Survey[i], laptop/mobile device theft is the second leading type of attack or misuse across all survey respondents, with 47% of respondents reporting losses in this category. The average loss per respondent was estimated at $30,057. The CSI/FBI survey notes that this average cost estimate likely only includes direct costs related to the loss of the hardware and does not include costs related to privacy breach notifications for personal data loss. The same survey ranked data protection (data classification, identification, and encryption) as the most critical computer security issue organizations are facing in the next two years.

While costs per data breach vary widely, a study by the Ponemon Institute found the total cost of data breaches to be $182 per compromised record last year, a 31% rise from 2005.[ii] This cost includes factors such as the cost to notify affected individuals, the cost to subscribe them to credit monitoring services, and other direct expenses.

If this data is not encrypted, the costs are higher. The Gramm-Leach-Bliley Act, HIPAA, and numerous state privacy laws and industry standards such as the Payment Card Industry Data Security Standard carry stiffer penalties for organizations that lose control of private consumer data if that data is not encrypted. If there is perceived exposure, and the data is not encrypted, a retail company loses its PCI compliance and pays dearly in higher rates for accepting credit transactions. If the data is encrypted at time of exposure, some states may not even require the company to report. Many organizations do report even if the data is encrypted because security executives would rather err on the side of caution in this time of changing data privacy rules. But in their notifications, they can at least add assurances that say, "Don't worry, your data is locked in an encrypted vault and we're the only ones with the key."

According to a recent study of over 700 C-level executives in mid- to large-sized US businesses, 95% of businesses suffering a data breach were required by a government regulation to notify data subjects whose information was lost or stolen. Of these, 97% were required to notify under state privacy statutes, and 58% were required to notify under federal privacy acts such as GLBA, HIPAA, and OCC regulations.[iii] Many of the recently enacted state privacy laws provide an "escape clause" that allows companies that lose control of data to avoid having to notify if that data is properly encrypted.

Against this backdrop, continuous protection for data at its source on desktop and laptop systems is gaining rapid acceptance. Full disk encryption can keep confidential data private, even if the systems are lost, stolen, or inadequately cleaned and disposed of.

Barriers to Widespread Adoption of Encryption

Encryption technologies have long been a part of the information security landscape. However adoption has been slow. Encryption products have historically had a reputation for being difficult to configure and implement, not to mention expensive, both in terms of direct cost and in system performance.

Performance has been a general issue for many encryption products and in particular for software-based products. The 2006 National Encryption Survey[iv] found the three most significant reasons given for not encrypting sensitive or confidential information to be:

- System performance (69%)
- Complexity (44%)
- Cost (25%)

Particularly for computing applications involving less technical end users, encryption products need to be almost invisible. The average end user has little desire or ability to understand the difference between encryption algorithms or between 40, 128, or 256- bit key lengths. In addition, fears about data being unrecoverable if encryption keys are lost have presented a barrier to adoption for many organizations.

To achieve widespread adoption in mobile business and consumer computing applications, encryption products must:

1. Provide high performance

2. Be simple to configure and operate

3. Be inexpensive

There are two primary approaches to encrypting data on personal computer disk drives. Software-based products use the main system microprocessor to perform encryption and decryption tasks. Hardware-based products use special chips to accelerate the encryption and decryption process. A hardware-based approach, DriveTrust, was developed and introduced by Seagate. DriveTrust utilizes firmware and hardware in the disk drive itself to perform encryption on all data being written to and read from the disk drive.

Software-Based Disk Encryption

Software-based encryption provides privacy for data residing on the computer systems disk by using the system CPU to perform encryption/decryption and related cryptographic operations. Software encryption products can provide for selective encryption of specific files or directories, or they can provide encryption of the entire disk by encrypting everything sent to the disk drive.

Software-based encryption can be used in a variety of applications, including encryption of files, directories, or entire disks in mobile or desktop PCs, and for communications security.

Encryption and data privacy products that are software-based have a number of advantages. The advantages of software-based encryption include the ability to use the software for multiple applications and purposes, including for messaging encryption and digital signature applications. Software-based products can also be easily extended to encrypt external disk drives and USB flash drives, providing protection for data stored on these removable and portable devices. Finally, keys that are used for encryption and decryption functions can be based upon unique passphrases, or they can be public/private keypairs that are also used for messaging security applications by the end user.

Important disadvantages that are common to most software-based encryption include performance, which is generally noticeably worse than on hardware encryption products. Configuration complexity and the amount of time needed to initially set up the software are also disadvantages.

Hardware-Based Disk Encryption

A relatively new approach to providing encryption of stored data – hardware-based encryption -- moves the encryption/decryption function inside the hard disk drive. Isolating the encryption functions and keys in the disk drive subsystem, where they are not accessible by the operating system, is advantageous because it protects these security components from rootkits and malware. In addition, utilizing dedicated hardware in the disk drive to perform the encryption and decryption offloads results in system performance that is closer to that of an unencrypted computer.

The DriveTrust platform is targeted at providing encryption and data privacy for laptop computer systems. Future applications on the DriveTrust platform will likely include providing encryption services in desktops, and SAN and NAS storage systems. Using the programming interface provided by Seagate, Independent Software Vendors (ISVs) are delivering pre-boot authentication and management solutions based upon DriveTrust. ISVs currently integrating DriveTrust into their security products include CryptoMill, Secude, Guardian Edge, and Wave Systems Corporation. It is worth noting that DriveTrust hard drives can be used without any 3rd-party software, using a BIOS level password to authenticate users to the drive. Seagate ships a single-user version of the enhanced pre-boot authentication and management 3rd-party software product with each DriveTrust hard disk. In addition, system builders and ISV's are expected to supply more fully featured enterprise versions of the authentication software to end user organizations.

Enhanced firmware and special purpose cryptographic hardware are built into DriveTrust hard disks. The firmware and hardware implement a cryptographic service provider that delivers common cryptographic functions, including encryption/ decryption, hashing, secure storage, digital signature, and random number generation. A trusted command set is also provided, delivering secure messaging capabilities for ATA and SCSI interface protocols.

DriveTrust has built-in secure partitions on the hard disk with strong conditional access controls. These secure disk partitions are used for storage of cryptographic keys. Computer applications with appropriate credentials can utilize this secure storage to store application code, passwords, system logs, or other sensitive information. Finally, DriveTrust includes an issuance protocol that determines which applications can access the secure disk partition. All access attempts by applications to the sensitive data stored in the secure drive partition use the issuance protocol to request access from the DriveTrust administrator function. The administrator function performs authentication on the application, activates the appropriate secure partition, and grants access from the application to the partition using the trusted send/receive command set. Figure 1 below depicts the four primary components of the DriveTrust architecture.

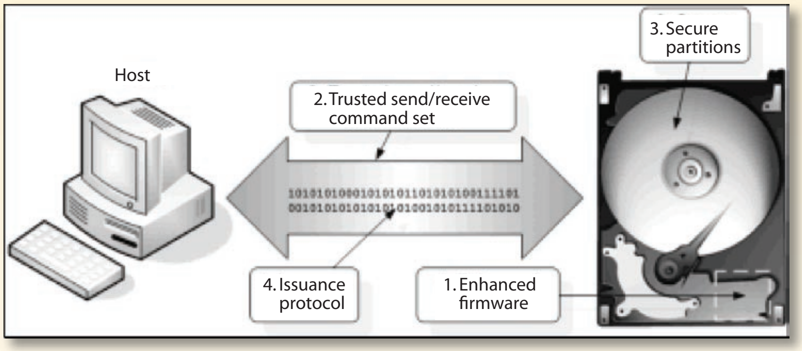

Figure 1: The DriveTrust technology includes four primary components.

Hardware-based encryption like DriveTrust transparently encrypts and protects data stored on computer hard drives. Performance of hardware-based encryption, as compared to software-based products, is a primary differentiator – disk encryption that is embedded in the hard drive provides performance that is very close to that of unencrypted disk drives. In addition, the user experience is really no different than using an unencrypted system. For mobile user populations where performance and transparency are important, using hardware-based disk encryption is a solid choice. Hardware-based encryption products also provide the ability to easily prepare drives for de-commissioning by simply changing the encryption key used to encrypt the drive's contents, thereby rendering the data stored on the disk drive unreadable and unrecoverable.

Disadvantages of disk-based encryption primarily relate to the lack of built-in management software. Vendors such as Seagate are collaborating with software vendors such as Secude, Wave Systems, CryptoMill, and Guardian Edge to leverage the strengths of the disk-based approach to create full-featured hardware and software encryption solutions. These will provide capabilities that large IT organizations will appreciate, including central management of distributed systems using DriveTrust drives.

Hands-on Evaluation

To better understand the differences between the two approaches, a hands-on evaluation was performed using a software-based encryption application, and a Seagate DriveTrust-enabled laptop as the hardware-based encryption application. The objective of the evaluation was to explore the differences between these two approaches in providing whole-disk encryption functionality. It should not be considered a head-to-head product comparison, as there are numerous additional functions provided by both products that do not allow for easy comparison. For example, DriveTrust is also envisioned as a component part in larger storage system applications, including Storage Area Networks and Network Attached Storage.

The evaluation used two identical Dell D620 laptops. Each system was configured with an Intel T2600 CPU running at 2.16GHz, with 1 GB RAM, and Windows XP Professional Service Pack 2 operating system. The only variance between the two test systems was the hard disk. In the case of the DriveTrust system, the hard disk was a 120GB Seagate drive. The system used to run software-based encryption software used a 150GB Seagate disk drive. Both disk drives are 2.5" drives, with 8MB buffers, operating at 5400 RPM. The second system was loaded with software-based encryption to test usability and performance.

Software-based Encryption: User Experience

The software-based encryption tested provided functionality to:

- Encrypt and secure e-mail messages
- Encrypt and secure instant messages
- Encrypt files and folders
- Create encrypted ZIP files
- Encrypt a disk or a partition, or encrypt a removable USB disk
- Delete and shred files, eliminating recovery concerns

Using the software encryption for the first time requires a number of steps to properly set up encryption functionality:

1. A setup wizard walks the user through a series of setup steps. To enable encryption for the entire disk drive, users must open the application and select the disk encryption module. Users can then choose whether to encrypt the entire disk or just a partition. Several options are provided. First, the user is given the choice of whether to use maximum CPU usage for encryption, which provides optimal performance for encryption. An option is also provided for power failure safety, which presumably provides protection in the event of power loss in the middle of encrypting data.

   Note: the software encryption tested uses a standard, non-changeable encryption algorithm, AES-128, and a standard hashing algorithm, SHA-1.

2. The system user must either create a unique passphrase for encryption, which is used to create the encryption keys that encrypt and decrypt the hard disk drive, or he can use his Windows login password. If the user opts to use his Windows password, a single sign-on capability within Windows is leveraged. This allows the user to present his credentials once at system login, and to have the login credentials used for Windows login and to encrypt/decrypt data. A third option exists to use public keys that have been previously established for use in encrypting/decrypting the hard disk drive. This is called "token-based public key." The software encryption tested additionally supports the use of user tokens for two-factor authentication.
3. Encrypting the hard disk is performed as an initial setup function by the end user or system administrator. Initially encrypting the disk takes a long time; on the 150GB disk, it took a little over three hours to fully encrypt the drive.

Logging in and using the software-based encryption was fairly straightforward. The software delivered a login screen pre-boot, and if the user has enabled the single sign-on capability, this is the only login prompt the user sees.

Seagate DriveTrust User Experience

DriveTrust ships 3rd-party software to provide the pre-boot authentication capability. Installation of the software was straightforward. The software uses the Windows login ID and password as the authentication credentials, and it provides a single sign-on capability by default. The passwords and authentication credentials are stored in a protected area on the disk drive and are never exposed to the operating system of the computer. The authentication software uses the GRUB bootloader and a hardened Linux system to authenticate users before allowing Windows to initialize. Once the user is properly authenticated, a soft reset is performed and Windows is started normally. The authentication software passes the user credentials to Windows to provide single sign-on.

From an end user perspective, using a system with DriveTrust and the accompanying pre-boot authentication software is simple. Once the user successfully authenticates, the encryption capability operates entirely in the background, and there is no perceptible difference in performance.

Usability Comparison

Once the initial configuration and setup of each system is performed, both systems operate transparently in the background.

Users logging on to systems protected by the software encryption are first presented with a login screen. The login prompt asks the user to input his Windows password or passphrase. After successfully entering the passphrase, Windows boots and the normal Windows login prompt is presented (for a non-single sign-on user). The software encryption is installed with a file shredding application, leaving an icon on the desktop for that purpose. This software application acts like an electronic version of a shredder, erasing any remnants of the file being disposed of.

The login for DriveTrust is similar in that it is provided pre-boot, before the operating system loads. Once the user has successfully authenticated, the DriveTrust technology operates in the background, encrypting and decrypting data on the hard drive. The authentication software actually provides the authentication login, and it uses a secure and hardened version of LINUX to perform the pre-boot authentication. The Windows operating system partition is hidden and is only accessed and booted after successful authentication. The authentication software can also support two-factor authentication including smart cards or USB tokens as the additional authentication factors. In this case X.509 certificates from the smart card or USB token are used as authentication credentials.

Strength of Security Comparison

Software encryption — the software tested uses the Advanced Encryption Standard (AES) encryption algorithm with 128-bit keys. Keys may be stored locally on the system hard disk, or on removable storage media or smartcards. There are no options to use other algorithms or different key lengths.

Seagate DriveTrust — the DriveTrust product also uses the AES encryption algorithm with 128-bit keys. There are no options to use other algorithms or key lengths. Keys are stored in protected and externally inaccessible sectors on the hard disk itself, and DriveTrust uses conditional access controls to grant key access to software applications.

The approaches used by each product are fundamentally different in one important respect that has implications for the security of each implementation. The software-based encryption relies on the security of an open system, the PC and operating system, for storage of passwords and keys and for generation of keys. By contrast, the DriveTrust product utilizes a closed system that is inaccessible to users or unauthorized users. This closed system stores all keys in a protected area. The closed system approach precludes the possibility that malware or rootkits can copy, observe, or otherwise compromise passwords and keys.

The software encryption and DriveTrust both operate similarly in terms of laptop hibernation. In both cases, closing the laptop and then re-opening it causes the system to display the Windows logon prompt, but not the pre-boot login prompt from the encryption pre-boot software.

Performance Comparison

To test and compare the performance of software-based versus hardware-based encryption, a series of tests were run using PCMark05[v], a popular performance test suite. The PCMark05 software provides various CPU performance tests, and it includes a hard disk drive test suite that tests and provides performance scores for common hard disk operations.

Three configurations were tested. First, the tests were run on a system using a Seagate DriveTrust drive with hardware-based encryption. Tests were also run on two systems with two different software-based encryption applications installed. For each configuration, two runs of each test were performed.

The first test looked at the speed of system startup. In Figure 2 below, using the DriveTrust drive as a baseline, the system running software A performed system start-up at 79% of the speed of the DriveTrust system and the system running software B performed system start-up at 78% of the speed of the DriveTrust system.

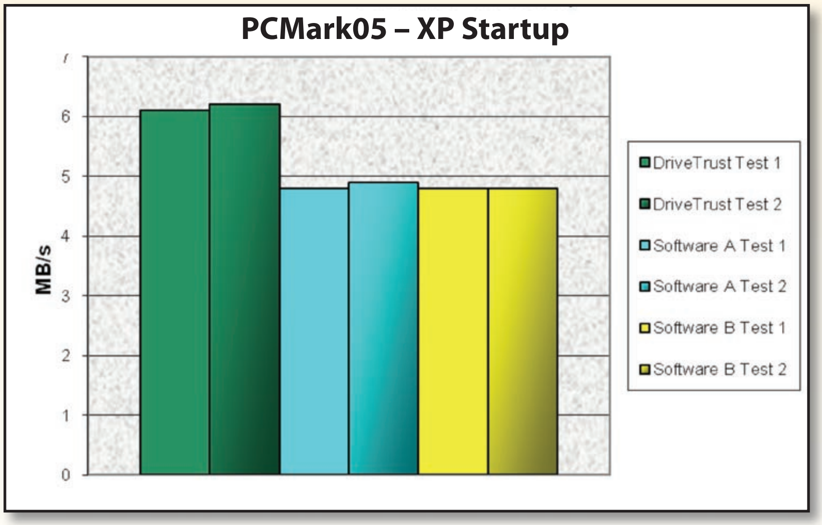

Figure 2: XP startup performance comparison.

A second test looked at the performance of each system when performing virus scans. Using the DriveTrust system as a baseline, the system running software A performed virus scans at 37% of the speed of the DriveTrust system, while the system running software B performed virus scans at 33% of the speed of the DriveTrust system. Figure 3 shows the results of this test.

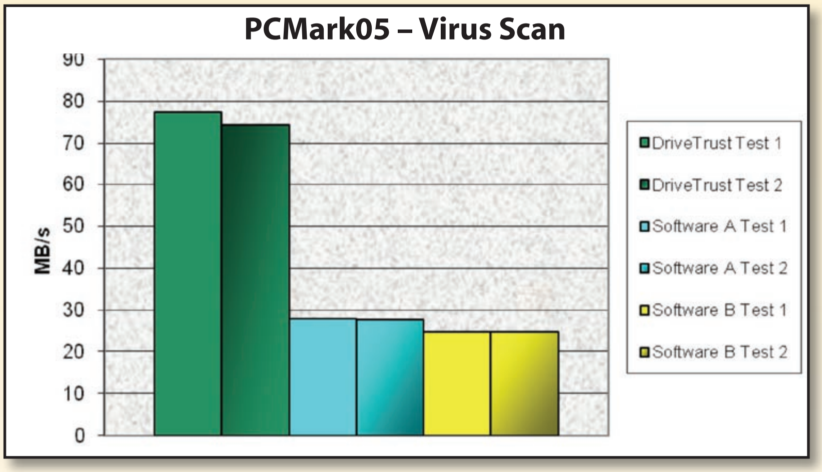

Figure 3: Virus scan performance.

The third test evaluated the performance of each system in loading applications. Using the DriveTrust system as a baseline, the system running software A performed application loading at 97% of the speed of the DriveTrust system, while the system running software B performed application loading at 96% of the speed of the DriveTrust system. Figure 4 depicts relative performance in application loading.

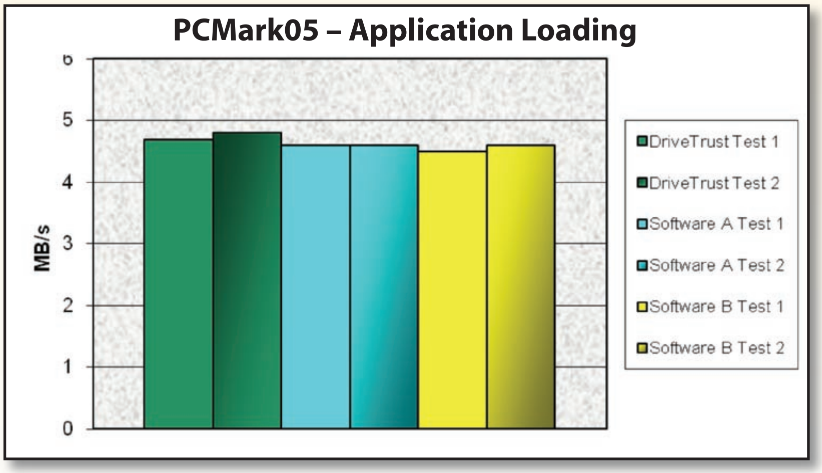

Figure 4: Application loading performance.

Another test looked specifically at the performance of each system in writing files. In this test, the system running software A ran at 68% of the DriveTrust system, while the system running software B performed at 64% of the DriveTrust system. Figure 5 below shows the results for file write performance.

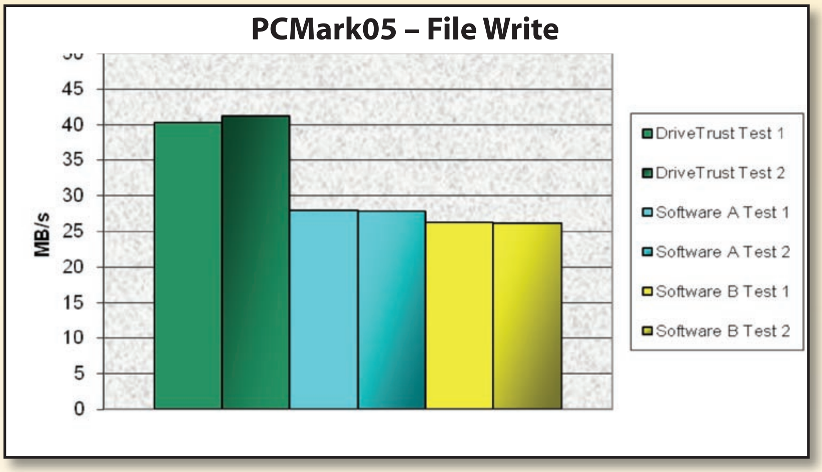

Figure 5: File write performance.

Finally, PCMark05 delivered a composite performance score for each system. On this test, the higher the score, the higher the overall performance of that system/drive combination. Using the DriveTrust system as the baseline, the system running software A performed at an overall level of 72% of the performance of the DriveTrust system as measured by PCMark05, while the system running software B performed at an overall level of 69%. Figure 6 depicts the overall performance results.

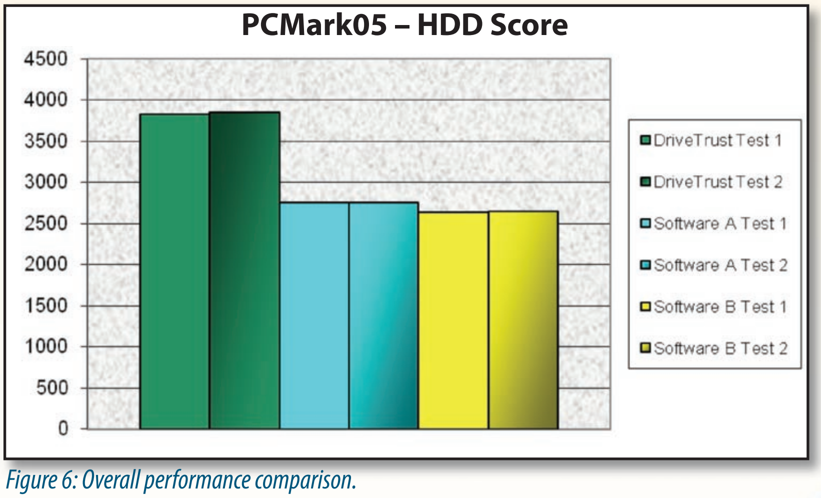

Figure 6: Overall performance comparison.

Overall, the performance tests revealed that those computing tasks that are heavily CPU-intensive were significantly faster on the hardware-based DriveTrust system as compared to the software-based approach.

System Management Comparison

One of the areas where further functionality is likely to be developed for both hardware-based and software-based products is central management of multiple systems. In large organizations with thousands of systems to administer, leaving the administration of each individual system to the end user is an unworkable solution. Providing a central administration capability allowing for recovery of data when users leave the organization is a desirable capability.

DriveTrust allows for the distribution of the authentication software as an MSI installation file (.MSI file extension). This allows it to be distributed and installed from a central management system running Windows Installer using Windows group policies. Upon first booting a newly installed DriveTrust system, the boot process proceeds to the point of the Windows login prompt, and after receiving the username and password, the software synchronizes them with the secure key storage on the hard drive.

After this initial boot and key synchronization, the authentication software performs all subsequent login credential capture and authentication. To facilitate configuration changes, a separate utility called Windows Credential Management is provided. This utility allows administrators to create scripts that can be used to replace lost keys and to recover data. The utility also provides remote administration capabilities for administrators.

The software encryption tested delivers similar management capabilities via a separate management software component.

Other Factors

The DriveTrust technology provides a simple way to dispose of or re-provision disk drives. Changing the encryption key renders all data on the drive unreadable. This simplifies end-of-life disposal of systems, or re-purposing of systems from user to user. The software encryption application tested does not address repurposing or disposal of disk drives. It does, however, provide a file shredder application that operates as an add-on to the operating system to provide for secure and complete deletion of individual files and folders. This capability ensures that no data remnants from shredded files are left on the drive.

The success of DriveTrust depends on adoption by security-focused Independent Software Vendors (ISVs) and by laptop manufacturers. ISVs are needed to create compelling security applications and management systems that leverage DriveTrust. To date, several ISVs including Secude, CryptoMill, GuardianEdge, and Wave have all announced or are shipping security software compatible with incorporating DriveTrust. Among laptop manufacturers, Dell and ASI are shipping laptop models incorporating DriveTrust hard drives.

Future support from software vendors in the identity and access management and single sign-on (SSO) spaces can be expected as the ability to securely store identity credentials is critical to these products. SSO software is convenient for users, however storing login credentials and access strings for multiple applications and systems on PC's gives cause for concern. Allowing this sensitive information to be securely stored in a closed subsystem that is inaccessible to malware would add measurably to the security of a single sign-on system.

Conclusions/Summary

Data encryption is no longer a luxury. It's a necessity. Organizations and users with sensitive data in use on laptops and desktops have no choice but to secure data on disk drives in a manner that is reasonable to regulators.

Software-based encryption products address the basic need for encrypting data on computer systems where performance is not the primary concern or where disk encryption is a part of a larger set of data privacy requirements. Examples of this include communications and messaging encryption requirements. Software-based products can also provide encryption at the file and folder level, as well as for removable storage devices.

Hardware-based encryption overcomes the two most significant barriers to widespread adoption of encryption technology — ease of use and system performance. Encryption built into the hard disk eliminates much of the setup and configuration complexity. DriveTrust isolates the encryption functions and stores the encryption keys in the hard drive itself, providing an added security benefit of blocking rootkits and other malware from accessing keys and other sensitive information from the operating system. In addition, hardware encryption performance is very close to that of a non-encrypted drive with minimal impact on computing operations, far superior to software-based encryption. Hardware-based encryption is well-suited to mobile user populations where performance and ease of implementation and use are concerns.

About the Author

Jim Hietala, SANS GSEC, GCFW and CISSP, is the principal of Compliance Marketing Group, providing consulting services in the areas of compliance, risk management, and IT security. He developed and launched the industry's first remote access VPN service and encrypting ISDN router, and brought a compliance and risk management software start-up to market. An industry veteran, he has held leadership roles at ControlPath, Avail Networks, Alternative Technologies, eSoft, Qwest, Concentric Network, and Digital Pathway. A frequent speaker at industry conferences, he has also published numerous articles on information security and compliance topics. He holds a B.S. in Marketing from Southern Illinois University.

Works Cited

[i] 2006 CSI/FBI Computer Crime and Security Survey, www.gocsi.com/press/20060712.jhtml

[ii] 2006 Annual Study: Cost of a Data Breach, http://www.ponemon.org/press/Ponemon_2006%20Data%20Breach%20Cost_FINAL.pdf

[iii] The Business Impact of Data Breach, Scott & Scott LLP and Ponemon Institute, http://www.ponemon.org/press/Ponemon_Survey_Results_Scott_and_Scott_FINAL1.pdf

[iv] National Encryption Survey results, http://www.csoonline.com/read/020106/ponemon.html, The Ponemon Institute, http://www.ponemon.org

[v] http://www.futuremark.com/products/pcmark05/

Additional information on DriveTrust: www.seagate.com/security

SANS would like to thank the sponsor

Seagate