


Technology Paper

How to Protect Data and Reduce Drive Retirement Costs

Overview

This paper discusses the challenge of securing data on hard drives that will inevitably leave the owner's control. It introduces Self-Encrypting Drives (SED), which may be used in two ways: to provide instant secure erase (cryptographic erase or making the data no longer readable), and to enable auto-locking to secure active data if a drive is misplaced or stolen from a system while in use. Two appendices then follow: The first compares SEDs to other encryption technologies used to secure drive data. The second provides detailed analysis of instant secure erase and auto-lock SED technology, explaining how SEDs are used in servers, NAS and SAN arrays, virtualized environments, RAIDs, JBODs and discrete drives.

Introduction

When hard drives are retired and moved outside the physically protected data center into the hands of others, the data on those drives is put at significant risk. IT departments routinely retire drives for a variety of reasons, including:

- Returning drives for warranty, repair or expired lease agreements
- Removal and disposal of drives
- Repurposing drives for other storage duties

Nearly all drives eventually leave the data center and their owners' control; Seagate estimates that 50,000 drives are retired from data centers daily. Corporate data resides on such drives, and when most leave the data center, the data they contain is still readable. Even data that has been striped across many drives in a RAID array is vulnerable to data theft, because just a typical single stripe in today's high-capacity arrays is large enough to expose hundreds of names and social security numbers.

How to Protect Data and Reduce Drive Retirement Costs

Drive Control Headaches and Disposal Costs

In an effort to avoid data breaches and the ensuing customer notifications required by data privacy laws, corporations have tried a myriad of ways to erase the data on retired drives before they leave the premises and potentially fall into the wrong hands. Current retirement practices designed to make data unreadable rely on significant human involvement in the process, and are thus subject to both technical and human failure.

The drawbacks of today's drive retirement practices are both numerous and far-reaching:

- Overwriting drive data is expensive, tying up valuable system resources for days. No notification of completion is generated by the drive, and overwriting won't cover reallocated sectors, leaving that data exposed.
- Degaussing or physically shredding a drive are both costly. It's difficult to ensure the degauss strength is optimized for the drive type, potentially leaving readable data on the drive. Physically shredding the drive is environmentally hazardous, and neither practice allows the drive to be returned for warranty or expired lease.
- Some corporations have concluded the only way to securely retire drives is to keep them in their control, storing them indefinitely in warehouses. But this is not truly secure, as a large volume of drives coupled with human involvement inevitably leads to some drives being lost or stolen.
- Other companies choose to hire professional disposal services, an expensive option which entails the cost of reconciling the services as well as internal reports and auditing. More troubling, transporting a drive to the service puts the drive's data at risk. Just one lost drive could cost a company millions of dollars in remedies for the breached data.

With these shortcomings in mind, it's no surprise that an IBM study found that 90 percent of the drives returned to IBM were still readable. The key lesson here? It's not just the drive that's exiting the data center, it's also the data stored within.

Encryption

Every day, thousands of terabytes of data leave data centers as old systems are retired. But what if all those hard drives had been automatically and transparently encrypting that data, enabling it to be instantly and securely erased? A majority of U.S. states now have data privacy laws that exempt encrypted data from mandatory reports of data breaches. And make no mistake, the cost of data exposure is high—US$6.6 million on average[1].

Challenges with performance, scalability and complexity have led IT departments to push back against security policies that require the use of encryption. In addition, encryption has been viewed as risky by those unfamiliar with key management, a process for ensuring a company can always decrypt its own data. Self-Encrypting Drives comprehensively resolve these issues, making encryption for drive retirement both easy and affordable.

We'll discuss two security scenarios:

- SEDs that provide instant secure erase without the need to manage keys
- Auto-locking SEDs that help secure active data against theft with key lifecycle management

1 2008 Annual Study: Cost of a Data Breach, Ponemon Institute, February 2009

How to Protect Data and Reduce Drive Retirement Costs

Instant Secure Erase Without Managing Keys

The Self-Encrypting Drive provides instant data destruction via cryptographic erase. When the SED is in normal use, its owner need not maintain authentication keys (otherwise known as credentials or passwords) in order to access the drive's data. The SED will encrypt data being written to the drive and decrypt data being read from it, all without requiring an authentication key from the owner.

When it's time to retire or repurpose the drive, the owner sends a command to the drive to perform a cryptographic erase. Cryptographic erase simply replaces the encryption key inside the encrypted drive, making it impossible to ever decrypt the data encrypted with the deleted key. (A more detailed explanation of how secure erase works appears in Appendix A.)

Self-Encrypting Drives reduce IT operating expenses by freeing IT from both drive control headaches and disposal costs. The SED's government-grade data security helps ensure Safe Harbor for data privacy compliance without hindering IT efficiency. Furthermore, SEDs simplify decommissioning and preserve hardware value for returns and repurposing by:

- Eliminating the need to overwrite or destroy the drive
- Securing warranty and expired lease returns
- Enabling drives to be repurposed securely

Auto-Locking Self-Encrypting Drives With Key Lifecycle Management

Beyond using a Self-Encrypting Drive for instant secure erase at retirement, the drive owner may also choose to employ that same SED in the auto-lock mode to help secure active data against theft. Insider theft or misplacement is a growing concern for businesses of all sizes; in addition, managers of branch offices and small businesses without strong physical security face greater vulnerability to external theft.

Utilizing the SED in auto-lock mode simply requires securing the drive during its normal use with an authentication key. When secured in this manner, the drive's data encryption key is locked whenever the drive is powered down. In other words, the moment the SED is switched off or unplugged, it automatically locks down the drive's data.

When the SED is then powered back on, the SED requires authentication before being able to unlock its encryption key and read any data on the drive, thus protecting against misplacement and insider or external theft.

The lifecycle of authentication keys can be managed by the IBM Tivoli Key Lifecycle Manager (formerly Encryption Key Manager), which is a Java-based software program that centrally generates, protects, stores and backs up authentication keys. It is a unified key management service that will support the key management requirements for all forms of storage (as well as other security applications). IBM, LSI and Seagate will support the Key Management Interoperability Protocol submitted to OASIS for advancement through their open standards process. With its platform neutrality, IBM Tivoli Key Lifecycle Manager offers a simple and effective method for managing the growing number of encryption keys across the enterprise.

The auto-lock mode of Self-Encrypting Drives and IBM Tivoli Key Lifecycle Manager is discussed in detail in Appendix A.

The owner of a Self-Encrypting Drive is able to use the SED first in secure erase-only mode, and then later change that SED to auto-lock mode. Later, after performing an instant secure erase and repurposing the drive, the drive may then go back to being used in secure erase-only mode. So, initially, the drive owner may choose to leave the SED in secure erase only mode during normal operation, intending to just perform an instant secure erase when needed. Later, perhaps due to growing concerns over theft, the owner may elect to use the SED in auto-lock mode for the remainder of the owner's use of the drive, by simply creating an authentication key that wraps the existing encryption key. Subsequently, once the SED has been securely erased and repurposed, its new owner may decide to not put the drive in auto-lock mode and use the drive in secure erase-only mode to securely erase the drive at the end of its useful life.

How to Protect Data and Reduce Drive Retirement Costs

Using Self-Encrypting Drives merely for instant secure erase provides an extremely efficient and effective means to help securely retire a drive. But using SEDs in auto-lock mode provides even more advantages. In short, from the moment the drive or system is removed from the data center (with or without authorization), the drive is locked. No advance thought or action is required from the data center administrator to protect this data. This helps prevent a breach should the drive be mishandled and helps secure the data against the threat of insider or outside theft.

Comparing Technologies for Securing Data on Hard Drives

No single encryption technology can effectively and efficiently secure all data against all threats. Different technologies are used to protect against different threats. For example, Self-Encrypting Drives help secure data against threats when the drive eventually leaves the owner's control, but it cannot protect data from certain threats that take place within the data center. For example, if an attacker gains access to a server that can in turn access an unlocked drive, the attacker can read the clear text coming from the drive. Thus it's important to remember that SED encryption technology does not replace the data center's access controls, rather it complements them.

Securing data at rest also should be complementary, rather than a replacement, to securing data in motion. The vast majority of data in motion moving over the wire downstream of the file system, whether moving over Ethernet on the NAS or at the block level on a SAN, is physically under the IT storage administrator's control, and therefore is not considered a security risk. For the data in motion that is not physically under the administrator's control, the most widely accepted and established practice for encrypting this data is to use IPSec or FC over IP, which use ephemeral session encryption keys to encrypt small amounts of data. It may seem that, instead of using this session security technique, encrypting in the fabric to secure the data on the hard drive is a better solution: the data is encrypted not only on the hard drive, but also as it travels through the fabric. But this approach has an a fundamental flaw: Rather than increasing security, it actually decreases security and increases complexity by exposing encryption keys that are long-lived keys, while exposing large amounts of cipher text that were all encrypted with only a single encryption key. If encryption is needed for data in motion, it should be provided by IPSec or FC over IP. Encrypting data on the drive is best performed by the drive itself, for all of the reasons provided below.

Application, database, OS and file system encryption (see Figure 1) are all techniques that cover threats to drive data (whether from database, file or system administrators or from hackers) that arise within the data center. But due to the significant performance degradation and non-scalable changes required to the application, database, OS or file system that such encryption entails, it's impractical to encrypt more than just a limited portion of data. Administrators cope with this restriction by reserving encryption for only the most sensitive data.

This forces administrators to rely on data classification in order to identify and locate sensitive data; unfortunately, it's widely acknowledged that this process fails to identify all instances of sensitive data. Data classification is difficult, labor-intensive and challenging to maintain, especially when sensitive information can be copied from a protected source to an unprotected destination. Such problems result in too much unencrypted sensitive data being written to disk, data which will likely persist on the hard drive long after the drive's useful life has ended.

As such, it falls to encryption technologies downstream of the file system to provide full disk encryption and close the gap created when data classification fails to capture sensitive data. These technologies relieve data custodians from the responsibility of classifying the data's sensitivity upon leaving control of the data center, a task fraught with management headaches and extra cost. Encrypting in the fabric, RAID disk controller (in a server or storage subsystem controller) or hard drive are all possibilities. But where should this encryption take place?

How to Protect Data and Reduce Drive Retirement Costs

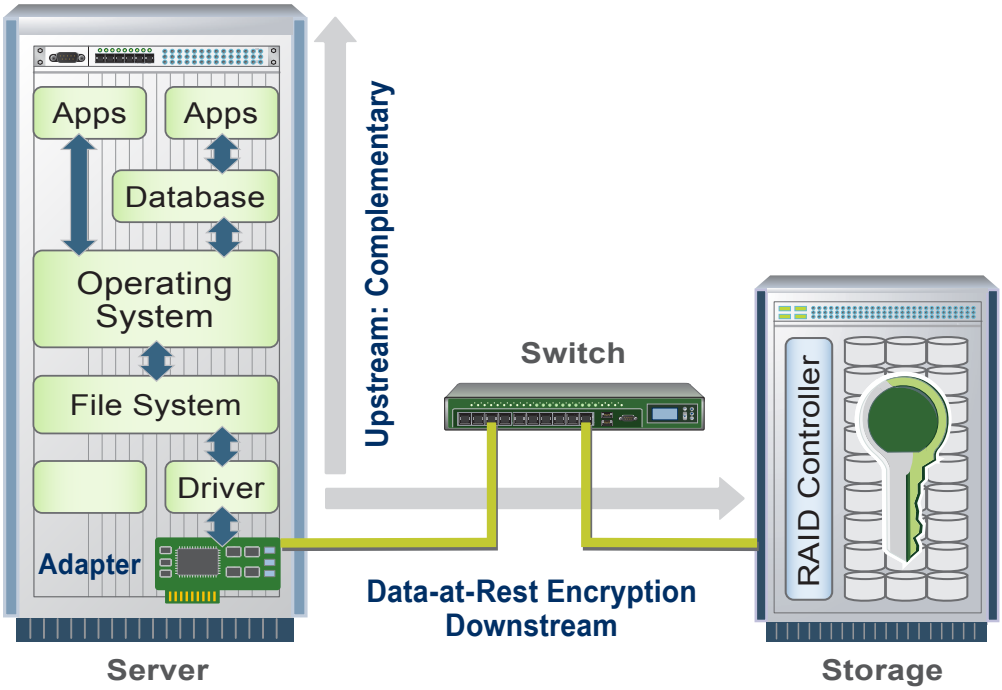

Figure 1.

Several years ago, before Seagate began working on drive encryption, the United States National Security Agency (NSA) analyzed the problem of data security and determined that the best place to perform encryption is in the hard drive. It's a well-known security maxim that guards should be placed as close to the jewels as possible. Similarly, encrypting within the hard drive is optimal because that's precisely where the data resides. SEDs boast superior technology to provide full disk encryption, lowering total cost of ownership for servers' direct-attached storage, SANs and NAS storage while delivering compelling advantages:

- **Simplified Key Management:** SED eliminates the need to track or manage a data encryption key; when used for secure erase only, there's no need to track or manage an authentication key either.
- **Reduced Costs via Standardized Technology:** Employing industry-standardized technology cuts costs and ensures common technology is used across SAN, NAS, server, desktop, notebook and portable storage platforms.
- **Optimum Storage Efficiency:** Unlike some encryption technologies, SED enables data compression and de-duplication to maximize value of disk storage capacity.
- **Increased Data Integrity:** SED enables Protection Information, the future of data integrity, and does not impact hard drive's reliability or warranty.
- **Maximum Performance and Scalability:** SED performs at full drive speed while also scaling linearly and automatically.
- **No Data Classification:** Expensive, time-consuming data classification is not needed to maintain peak performance.
- **Reduced Re-Encryption:** SED ensures there is less need to re-key and re-encrypt, because the data encryption key is never exposed.
- **Superior Security:** NSA qualified the first SED model. SED doesn't weaken security by needlessly encrypting the storage fabric, which exposes long-lived cipher text and keys. SED leaves over-the-wire encryption to technologies designed for securing data in motion

How to Protect Data and Reduce Drive Retirement Costs

Standardization of Self-Encrypting Drives promises lower acquisition costs as well. The world's top six hard drive vendors collaborated to develop the final enterprise specification published by the Trusted Computing Group (TCG). This specification, created to be the standard for developing and managing Self-Encrypting Drives, enables SEDs from different vendors to be interoperable. Such interoperability helps ensure greater market competition and lower prices for solution builders and end-users alike. Historically, the hard drive industry has repeatedly shown that industry-wide standards increase volume, which in turn lowers costs. These economies of scale help ensure incremental logic in the ASICs remains a small portion of drive material costs. (Appendix B provides a more detailed comparison of hard drive encryption technologies and explanation of the advantages of SEDs.)

Conclusion

Administrators of servers, SAN and NAS arrays have good reasons to want to encrypt their data. Self-Encrypting Drives address both those reasons and the concerns that have prevented some IT professionals from adopting data encryption until now.

The benefits of Self-Encrypting Drives are clear. Instant secure erase cuts IT operational expense for retiring drives without the need to manage keys. Further, it preserves the value of the retired drive by enabling the drive to be securely repurposed or returned for service, warranty or expired lease. Auto-locking SEDs automatically help secure the data against drive theft or misplacement the moment a drive is removed from the system. A drive may be compromised, but it will never expose its data.

Self-Encrypting Drives also offer compelling advantages. The encryption key doesn't need to be tracked or managed in order to recover data because the encryption key never leaves the drive, lessening concerns about being unable to decrypt one's own data. Only the authentication key must be tracked or managed, and it can be securely backed up, replicated and mirrored in disaster-recovery centers. And that key needn't be introduced and managed at all if an SED is used only for instant secure erase.

SED encryption is automatic and transparent, avoiding costly changes to normal storage management, the OS, applications and databases. The significant cost savings of efficiently compressing and de-duplicating data in the storage system is fully maintained. In addition, performance scales linearly and automatically, and because all data can be encrypted without performance degradation, there's no need for costly and time-consuming data classification.

Self-Encrypting Drives are standards-based for optimal manageability, interoperability and cost-efficiency, and all major hard drive manufacturers participated in the standards development. Key management is also becoming interoperable, with major storage vendors committed to support the Key Management Interoperability Protocol from OASIS. SEDs are designed to be integrated into standard products, which are implemented per the typical storage upgrade schedule.

Simply put, encryption in the drive provides superior cost-effectiveness, performance, manageability and security when compared to other encrypting technologies. That's why many prominent analysts, system manufacturers and government agencies such as the NSA have concluded that encryption should be done in the drive. The bottom line: SEDs are a significant leap forward to improve security and lower the total cost of ownership in the world's servers, SANs and NAS arrays.

Given that SEDs lower drive retirement costs and reduce IT headaches, many corporations are considering the benefit of incorporating SEDs into their security policies. Security policy writers should consider updating their policies to specifically require that all future hard drive purchases be SEDs when available. IBM and LSI are leading the way in building Self-Encrypting Drives into their solutions, and Seagate is rapidly introducing SEDs across its entire portfolio of hard drives. Other hard drive vendors have introduced SEDs as well, and it won't be long until all hard drives will be Self-Encrypting Drives.

How to Protect Data and Reduce Drive Retirement Costs

Appendix A: Self-Encrypting Drive Technology

Newly-Acquired Self-Encrypting Drives

Each Self-Encrypting Drive (SED) randomly generates an encryption key in the factory that is embedded on the drive. The SED automatically performs full disk encryption; when a write is performed, clear text enters the drive and is first encrypted (using the encryption key embedded within the drive) before being written to the disk. When a read is performed, the encrypted data on the disk is decrypted before leaving the drive. During normal operation an SED is completely transparent to the system, appearing to be the same as a non-encrypting drive. The Self-Encrypting Drive is constantly encrypting—encryption cannot be accidentally turned off.

When the owner acquires the drive, this embedded encryption key is in clear text form and will remain so until the drive is put in auto-lock mode, where an authentication key is introduced. The drive will encrypt and decrypt all data that it writes to and reads from the disk; however, without establishing an authentication key, anyone can write and read the clear text data on the disk.

Setting up the system is quite simple. The owner must decide whether to use the SED in auto-lock mode or only for instant secure erase. Each use case is discussed below.

Instant Secure Erase Technology

If an owner wishes to use the drive for instant secure erase only, the owner will simply begin using the drive in normal operation. Secure erase-only mode means that the owner needs no authentication key or password to decrypt and read data. This eliminates the possibility of authentication key mismanagement and subsequent data loss.

SED technology greatly simplifies repurposing of the drive and disposal. An owner wishing to repurpose a drive simply performs a key erase to replace the encryption key. The drive deletes the encryption key and replaces it with a new encryption key generated randomly within the drive. After key erase, any data that had been written to the disk is unreadable—data that was encrypted with the previous key is unintelligible when decrypted with the new encryption key (see Figure 2). The drive is left as it was delivered from the factory, ready for a new owner to use it in secure erase only mode or put the drive in auto-lock mode.

Figure 2

How to Protect Data and Reduce Drive Retirement Costs

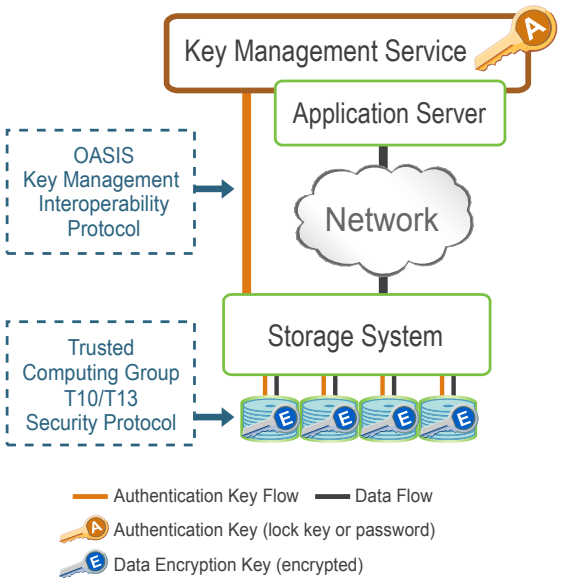

Figure 3

Key Management and Managing Auto-Locking Self-Encrypting Drives

When the SED is used in auto-lock mode, the SED requires an authentication key from an outside source before the drive will unlock for read/write operations. A data center containing auto-locking Self-Encrypting Drives utilizes a key-management service that stores, manages and serves authentication keys, and a storage system that passes these authentication keys to the correct drive (see Figure 3). Seagate, IBM and LSI have collaboratively worked to bring together technologies from their respective organizations and deliver complete self-encrypting solutions, such as in the IBM System Storage DS8000 and the IBM System Storage DS5000.

In addition to its traditional functions, the storage system also defines secure volume groups, obtains the authentication keys from the key management service and passes the key to the correct drive. The orange line in Figure 3 denotes this operation. In this way the storage system makes the encryption function transparent to the hosts, OS, databases and applications.

Once authentication is completed during power-up, encryption is fully transparent to the storage system, which can perform its traditional functions normally. In Figure 3, the dark gray line denotes the data flow that is clear text data. Storage systems are optimized for unencrypted data for data compression and de-duplication.

A key management service may employ software- or hardware-based key stores in order to create, assign and manage the relevant authentication and encryption keys across the enterprise. Effective key management should integrate well into an organization's existing security policies, to help ensure that both the service and the keys themselves are well protected from unauthorized access.

Moreover, an effective key management system should include backup, synchronization, life-cycle management, auditing and long-term retention capabilities. Deployment of a key management service is greatly simplified when it's possible to take advantage of an organization's existing high-availability and disaster-recovery solution.

The IBM Tivoli Key Lifecycle Manager (formerly Encryption Key Manager) is a Java-based software program that can generate, protect, store and maintain authentication keys that are used with IBM self-encrypting tape drives and with the IBM System Storage DS8000 with full disk encrypting drives. As a Java application, IBM Tivoli Key Lifecycle Manager operates on z/OS, i5/OS, AIX, Linux, HP-UX, Sun Solaris and Windows operating systems, and is designed to be a shared resource which can be deployed in several locations within an enterprise to help ensure the application is highly available.

With its platform neutrality and its ability to take advantage of the existing security policies and high-availability environment in an organization's most secure server platform, IBM Tivoli Key Lifecycle Manager offers a simple and effective method for managing the growing number of encryption keys across the enterprise.

How to Protect Data and Reduce Drive Retirement Costs

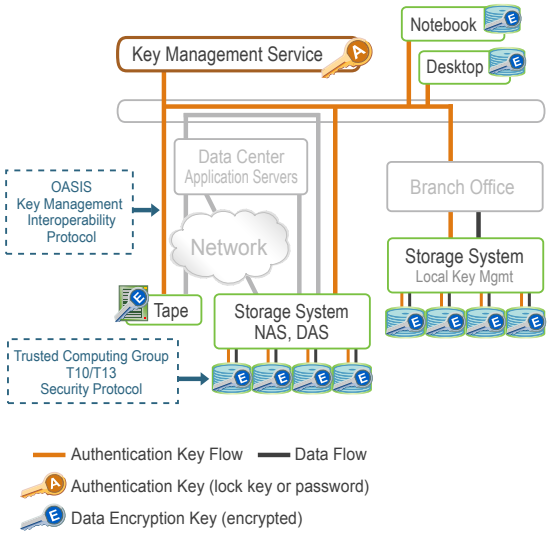

Figure 4

IBM Tivoli Key Lifecycle Manager serves keys at the time of use to allow for centralized storage of key material in a secure location, a unique approach that supports multiple protocols for key serving and manages certificates as well as symmetric and asymmetric keys. Users can also centrally create, import, distribute, back up, archive and manage the lifecycle of those keys and certificates using a customizable graphical user interface (GUI). In addition, IBM Tivoli Key Lifecycle Manager's transparent encryption implementation means that keys are generated and served from a centralized location and are never sent or stored "in the clear."

Ultimately this technology applies across the entire data center, as shown in Figure 4. Self-Encrypting Drives may be in storage arrays, on SANs, NAS and servers, and in data centers, branch offices and small businesses. A unified key management service will support the key management requirements for all forms of storage (as well as other security applications).

Auto-Locking Self-Encrypting Drive Technology

To put the Self-Encrypting Drive in auto-lock mode, the drive owner may wish to first change the encryption key for added security confidence, using secure erase on a new SED; this also protects the drive against a warehouse attack. The owner must then establish an authentication key by first entering the SID (Security ID, proof of ownership) from the drive's external label, then setting the authentication key, which is used by the drive to encrypt the encryption key. The SED is now in auto-lock mode. It is in a secured state; when the drive is powered down it will be locked, and when powered back up it will require authentication to become unlocked. In an auto-locking SED, an encryption key and an authentication key work together to enable access to the data stored on the drive.

An auto-locking SED, which is configured to use authentication, contains no secret that, if discovered, could reveal the encrypted data. A simple description of the unlock process explains why this is true. The unlock process is the part of the drive's power-on activity that enables access to the encrypted data. The drive expects a credential (authentication key) to be supplied to it, which it verifies as proof that the drive is being accessed by an authorized user.

How to Protect Data and Reduce Drive Retirement Costs

The following describes the steps that occur during the authentication process of a previously secured drive (see Figure 5):

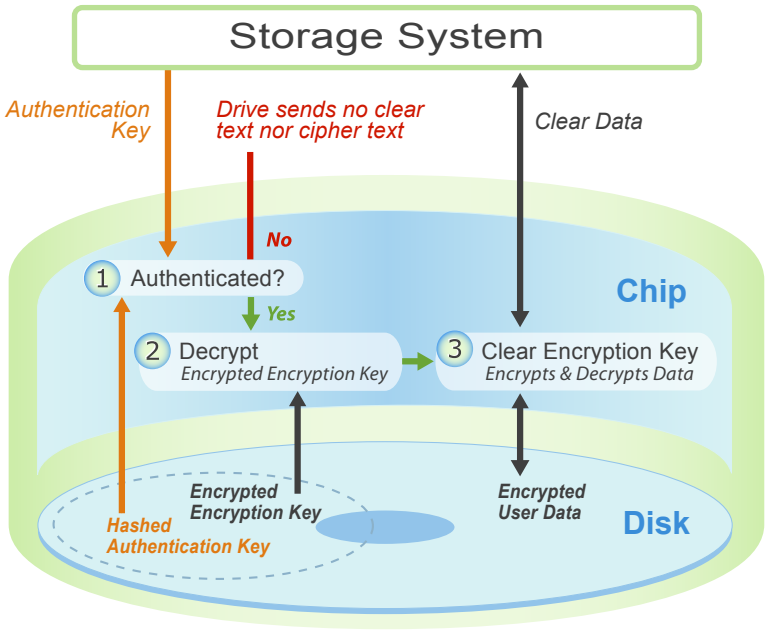

Figure 5

1. Authentication

- The storage system gets the authentication key from the key management service and sends it to the correct locked drive.
- The drive hashes the authentication key and compares the result with the hash of the authentication key that's stored in a secure area of the disk.
- If the two hashed authentication key values do not match, the authentication process ends, and the drive will not permit reading data from the disk. The drive remains locked. Note that the drive never sends cipher text from the drive.

2. Decrypt the encrypted encryption key

- If the two hashes match, the drive is then unlocked, and the drive uses the authentication key it received from the storage system to decrypt a copy of the encryption key (which was previously encrypted with the authentication key) that's stored in a secure area of the disk. Once the authentication process is successfully completed, the drive is unlocked until the next time it is powered down. Note that this authentication process only occurs when the drive is first powered on; it does not repeat with each read and write operation.

3. Clear encryption key encrypts and decrypts the data

- The clear-text encryption key is then used to encrypt data to be written to the disk and to decrypt data that's being read from the disk.
- The drive now works in standard fashion during data transfers, with encryption and decryption transparently occurring in the background.

Once the drive is put in auto-lock mode, it can be put back into secure erase-only mode only after a secure erase is performed. If an owner wishes to repurpose or retire the drive (i.e., change the drive from being in an auto-lock mode to a secure erase-only mode so that someone else can use the drive), the owner would simply perform a secure erase to replace the encryption key.

How to Protect Data and Reduce Drive Retirement Costs

Appendix B: Comparing Technologies for Securing Data on Hard Drives

There is no one comprehensive encryption approach that covers all threats to data at rest. There are cost, interoperability, performance and latency issues to consider with each approach, thus care must be taken when choosing where to encrypt. Data encryption options come in many forms, including:

- Host-based software
- Encryption hardware appliances
- Encryption ASICs that reside on the adapter, switch, RAID controller or hard drive

When evaluating how to protect and where to encrypt data at rest on the SAN, NAS or the server's direct attached storage, the best solution is to encrypt as close as possible to the storage—ideally, the hard drive.

Key Management and Interoperability Made Simple

SEDs greatly ease key management because the encryption key never leaves the drive, thus there's no need to track or manage the encryption key. In addition, the data center administrator needn't escrow the encryption key to maintain data recoverability, because the drive itself keeps encrypted copies of the encryption key in multiple locations on the drive.

Only SEDs eliminate the need for encryption key escrow, because if the drive loses all copies of its encryption key, it is likely the drive has failed, which makes its data unreadable in any event. More encryption keys are automatically added with data redundancy—each time the data is mirrored onto another Self-Encrypting Drive, that drive will have its own set of encrypted encryption keys. By contrast, fabric and controller encryption can present challenges in tracking, managing and escrowing encryption keys to enable the end points to read and write the data.

There are major challenges with hardware encryption that occurs at the switch or on the adapter. Separating the encryption from where the data is stored increases the solution complexity, increasing the chances for error. For example, the correct key may not be readily available

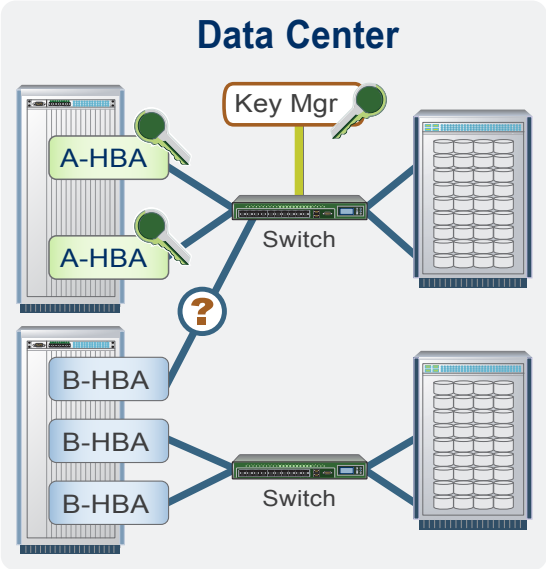

Figure 6

when needed to decrypt data in a virtualization environment. More shared equipment increases the number of entities that must share a given key, and tracking more keys moving across the fabric entails greater exposure, complexities and performance issues.

Adapters with on-board encryption ASICs entail interoperability challenges with multi-vendor adapters that do not support on-board encryption. Data encrypted by adapter-mounted hardware can only be read by the compatible hardware that uses the same encryption algorithm and that can access the same key management infrastructure. For example, in Figure 6 a blue HBA (Host Bus Adapter) in the bottom server cannot read data that's encrypted on the target or authenticate with the key manager or encryption switch, because either it can't access the key manager or it has incompatible encryption hardware.

Self-Encrypting Drives inherently provide manageability because the encryption key never leaves the drive. In addition, it's easy to add hard drives with different embedded encryption engines to an existing array. Thus the data center can have a wide variety of encryption engines in the same array, because the encryption algorithm is transparent to the system. As drive models

How to Protect Data and Reduce Drive Retirement Costs

change and newer encryption technologies are incorporated into hard drives, they can be intermixed with older drives in storage systems that support encryption without making any changes specific to the new drives' higher level of protection.

Key management is also becoming interoperable. IBM, LSI and Seagate will support the Key Management Interoperability Protocol submitted to OASIS for advancement through their open standards process.

Government-Grade Security

Self-Encrypting Drives provide superior security, making it less likely that the data security solution will need to be ripped out and replaced in the future due to more stringent regulations. As noted earlier, SEDs do not weaken security by needlessly encrypting the storage fabric and exposing long-lived cipher text and keys. SEDs also provide a host of other advantages that makes their security stronger than other full disk encryption technologies.

The United States National Security Agency (NSA) has approved the first Self-Encrypting Drive, the Momentus® 5400 FDE hard drive, for protection of information in computers deployed by U.S. government agencies and contractors for national security purposes. Also, the encryption algorithm implementation in this first model is NIST AES FIPS-197-compliant. Seagate is in the process of pursuing similar acceptance on its future SEDs.

Figure 7 depicts what potential attackers will have if they obtain a secured SED that was locked when powered down. The encryption key never leaves the drive; the key is unique to that drive alone, generated by the drive itself. What's more, a clear encryption key is nowhere to be found—only an encrypted version of the encryption key is kept in the drive. There are no clear text secrets anywhere on the drive, just a fingerprint (hash) of the authentication key. In addition, hard drives don't utilize the type of memory that is susceptible to a "cold-boot" attack.

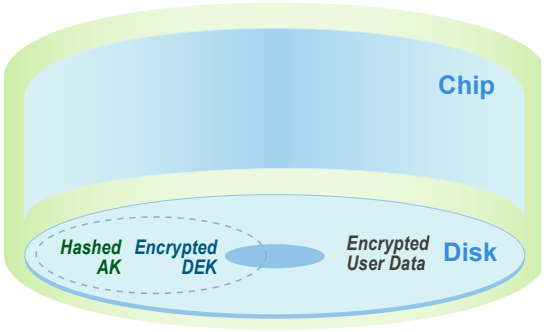

Figure 7

Both the data and the encryption key are encrypted using the AES 128 algorithm, the same encryption algorithm approved by the U.S. government for protecting secret-level classified information. When designing the drive, Seagate assumed an attacker could obtain complete knowledge of the drive's design and the location of any secrets held by the drive. Because there are no clues on the drive that could aid in deciphering the data, knowing the intricate details of the drive's design and construction cannot help hackers. Similarly, breaking one drive provides no secrets that would enable the attacker to break other drives more easily.

In general, exposing cipher text can aid an attacker. For example, if the file system on the drive is a well-known structure, a hacker might use the fact that certain sectors always contain known values to begin an attack on the encryption. Database structures are similarly well known. A significant benefit unique to Self-Encrypting Drives is that an SED does not send cipher text from itself, effectively thwarting this type of attack.

SEDs have the ability to essentially turn themselves into bricks, after a pre-determined number of authentication attempts have failed. By contrast, an attacker who has a non-SED that's been encrypted by some other method can attempt to authenticate indefinitely and the drive has no protection. In addition, the SED has protected firmware downloads; an attacker cannot insert modified firmware into the drive. Finally, to further minimize vulnerability to attack, Seagate has put no security back doors in the SED.

How to Protect Data and Reduce Drive Retirement Costs

Performance at Full Drive Speed; Less Need for Data Classification

The Self-Encrypting Drive has a dedicated engine for full interface speed encryption. Utilizing hardware-based encryption, the SED's encryption engine resides in the controller ASIC. Each drive port uses a dedicated encryption engine that matches the port's maximum speed. Simply put, encryption will not slow the system down.

SED performance also scales linearly and automatically. As more drives are added, encryption bandwidth commensurately increases. Data center administrators needn't worry about balancing encryption workloads when adding more drives to an array or more arrays to the data center.

Because data center administrators can encrypt all of the data they wish without performance degradation, there is far less need for data classification. As noted earlier, attempting to identify all instances of sensitive information is labor-intensive and time-consuming. Such data is also difficult to maintain and update, especially when it can be easily copied from a protected source to an unprotected destination. Reducing the need for data classification greatly simplifies the process of planning and managing encryption in the data center.

Compression and De-Duplication Efficiencies Fully Maintained

Storage system data compression and de-duplication present the opportunity to dramatically cut storage costs, but only when the data is not encrypted as storage systems are optimized for unencrypted data when performing data compression and de-duplication. With SEDs, the ability of the storage system to efficiently compress and de-duplicate data is fully maintained.

Data Integrity's Protection Information Standard Fully Maintained

SED enables the future of data integrity, PI (Protection Information, also known as Data Integrity Feature), which is a T-10 SCSI-based end-to-end data protection specification. The implementation of this SCSI protocol standard in SAS and Fibre Channel systems allows each element in the data's path to inspect the data and verify that no corruption has occurred. This is performed using a special appendix to the data, but it cannot be performed if the data passing through the element has been encrypted.

Because SED performs encryption at the end of the data's path, (i.e., at the drive where the data is stored), SED is the only solution that supports Protection Information throughout the data path. And while facilitating this superior data integrity, SED does not impact the hard drive's reliability, availability or serviceability/warranty.

Standardized Technology Lowers Costs

The world's top six hard drive vendors (Fujitsu, Hitachi, Samsung, Seagate, Toshiba and Western Digital) collaborated to develop the final enterprise specification recently published by the Trusted Computing Group (TCG). This specification, created to be the standard for developing and managing Self-Encrypting Drives, enables SEDs from different vendors to be interoperable. Such interoperability helps ensure greater market competition and lower prices for solution builders and end-users alike.

Eventually all drives shipping from all vendors will be Self-Encrypting Drives (half of these vendors are already shipping SEDs today). This promises an end to the risk of data breaches when hard drives leave their owner's control.

How to Protect Data and Reduce Drive Retirement Costs

As a result, self-encrypting storage is expected to be available across all end points, including such diverse devices as:

- Servers, SANs, NAS arrays (virtualized or not), RAIDs, JBODs or individual drives
- Tape drives
- Solid state disks
- Desktop drives
- Notebook drives
- Portable drives

Less Need to Re-Encrypt

Separation of authentication and encryption keys provides several management benefits for drive owners. Because the encryption key itself is encrypted and doesn't leave the drive, the data center administrator doesn't need to change the encryption key periodically, the way a user may periodically change his/her password for security reasons. That eliminates the chore of decrypting and re-encrypting the data, a highly resource-intensive process.

The authentication key can be changed as often as desired, such as when an administrator leaves the company, without requiring re-encryption. When storage administrators depart or new operators arrive, their rights to access the storage device can be incorporated without affecting the encrypted data.

By contrast, controller- and fabric-based encryption move data encryption keys between the key manager for safe storage and the point of encryption, and they require key escrow. Their data encryption keys are no more secure than their authentication keys, and thus should be periodically re-keyed, which requires re-encryption of data—a huge performance drain.

Data-in-Motion Secured Physically or with Session Encryption

The vast majority of data in motion moving over the wire downstream of the file system, whether moving over Ethernet on the NAS or at the block level on a SAN, is physically under the IT storage administrator's control, and therefore is not considered a security risk.

For data in-motion over the wire downstream of the file system that is not physically under the IT storage administrator's control, the most widely accepted and established practice for encrypting data transmitted over the wire is to use an ephemeral session encryption key. A single transmission can be encrypted by a session key that will be discarded immediately after the transmission—any subsequent transmission will be protected by a new, different session key. These very short-duration keys minimize data vulnerability, unlike the long-lived keys used to encrypt data stored on a hard drive.

Here are three scenarios of session encryption that may be used:

Scenario One

There are potential risks with Fibre Channel fabric links that leave the data center and extend the SAN to remote offices, other campuses or to remote locations for disaster recovery. In those cases, security is addressed by using FC links over Internet Protocol (IP) and protecting the data with IP security.

Scenario Two

Routers and switches use technologies such as IPSec to protect and link SANs over WANs. To specifically address this type of security threat, host/adapter-based encryption is not required as long as the switches and routers support IPSec data encryption. Fibre Channel technology can only reach a distance of about 10km, but IT managers need to share, protect and move data much farther than that—sometimes across geographic borders. QLogic provides routers and switches that enable SAN traffic to move over IP, linking SANs over WANs.

How to Protect Data and Reduce Drive Retirement Costs

Scenario Three

When IP extends the SAN over the Internet or dedicated lines, IPSec security is used on these remote links to protect valuable in-motion data over long distances and to support data replication, SAN data device sharing and ensure backup and business continuity. Secure Sockets Layer (SSL) sessions are used for the WAN links (with ephemeral keys) to help ensure that the link remains secure and that keys are not exposed for long periods of time.

Regardless of whether there is physical security protection for the fabric, there is still the need to secure the hard drive's data once the drive leaves the owner's control. Instead of using the session security techniques described above, it may seem that encrypting in the fabric to secure the data on the hard drive is a good long-term solution: the data is encrypted not only on the hard drive, but also as it travels through the fabric. But this approach has a fundamental flaw: Rather than increasing security, it actually decreases security and increases complexity by exposing encryption keys that are long-lived keys, while exposing large amounts of cipher text that were all encrypted with only a single encryption key.

If encryption is needed for data in motion, it should be provided by IPSec or FC over IP. Encrypting data on the drive is best performed by the drive itself, for all of the reasons provided by the above sections.

Additional Information

Additional information about storage security can be found at the Trusted Computing Group: www.trustedcomputinggroup.org

and at the Storage Networking Industry Association (SNIA) Storage Security Industry Forum (SSIF): www.snia.org/forums/ssif/knowledge_center

AMERICAS Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, United States, 831-438-6550
ASIA/PACIFIC Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
EUROPE, MIDDLE EAST AND AFRICA Seagate Technology SAS 16–18 rue du Dôme, 92100 Boulogne-Billancourt, France, 33 1-4186 10 00