Data Security Features for SSDs

Micron® self-encrypting SSDs are easy-to-use, cost-effective solutions that protect important stored data from intrusion or loss.

Introduction

Realizing that data security was fast becoming one of the most pressing issues facing the information technology industry, Micron was among the first manufacturers to bring full drive encryption capability to solid state drives with our self-encrypting drives (SEDs). Micron has now shipped several generations of SSDs that feature hardware encryption.

This paper covers the basics of encryption — a key tool in data storage security — including discussions about:

- Different data storage encryption schemes, such as file/folder encryption and full-drive encryption (FDE).
- SEDs as data protection tools, covering methods to manage encryption and SEDs, including management of these security features in concert with software on the host computer.
- Industry and government protocols that ensure consistency and conformity of data security systems. These include protocols from the Trusted Computing Group (TCG) and requirements of the Federal Information Protection Standard (FIPS).

Encryption Explained

Put simply, encryption is an arithmetic tool used to keep data private between the sender and intended recipient. It uses mathematical algorithms and randomly derived keys to convert data from its original "clear text" to unreadable "cipher text." Cipher text can only be read using the same key and reverse-deciphering algorithm. Methods of encrypting data range from the simple (for example, ROT13), to the complex (ENIGMA), to the extremely complex and robust (AES).

Simple Encryption Example: ROT13

One of the simplest (and oldest) encryption mechanisms is rotation. In rotation encryptions, values in the original, unencrypted message (plain text) are substituted for new values to create the encrypted message (cipher text). The substitution follows fixed rules that are known to the recipient of the cipher text so that the message can be decrypted.

ROT13 is a classic example of a rotation encryption scheme. In ROT13, each letter in the plain text is substituted with a corresponding letter 13 places further ahead in the alphabet, rotating through Z to A when necessary. Of course, the value 13 is arbitrary and could be any value between 1 and 25 for English capital letters. When only the sender and receiver know the rotation value of 13, the message is secure. It could be made even more secure by including upper and lower case letters and perhaps numerals and other characters from the ASCII set. However, even when increasing the complexity in this way, an unauthorized reader could easily and quickly calculate 13 as the correct value.

Therefore, while easy to implement, this algorithm is extremely insecure in light of modern, sophisticated computer attacks. Today's proven encryption mechanisms still operate in an analogous manner to this simple ROT13 cipher. However, modern computing power enables us to add layers of mathematical complexity to reduce an attacker's odds of deciphering the message.

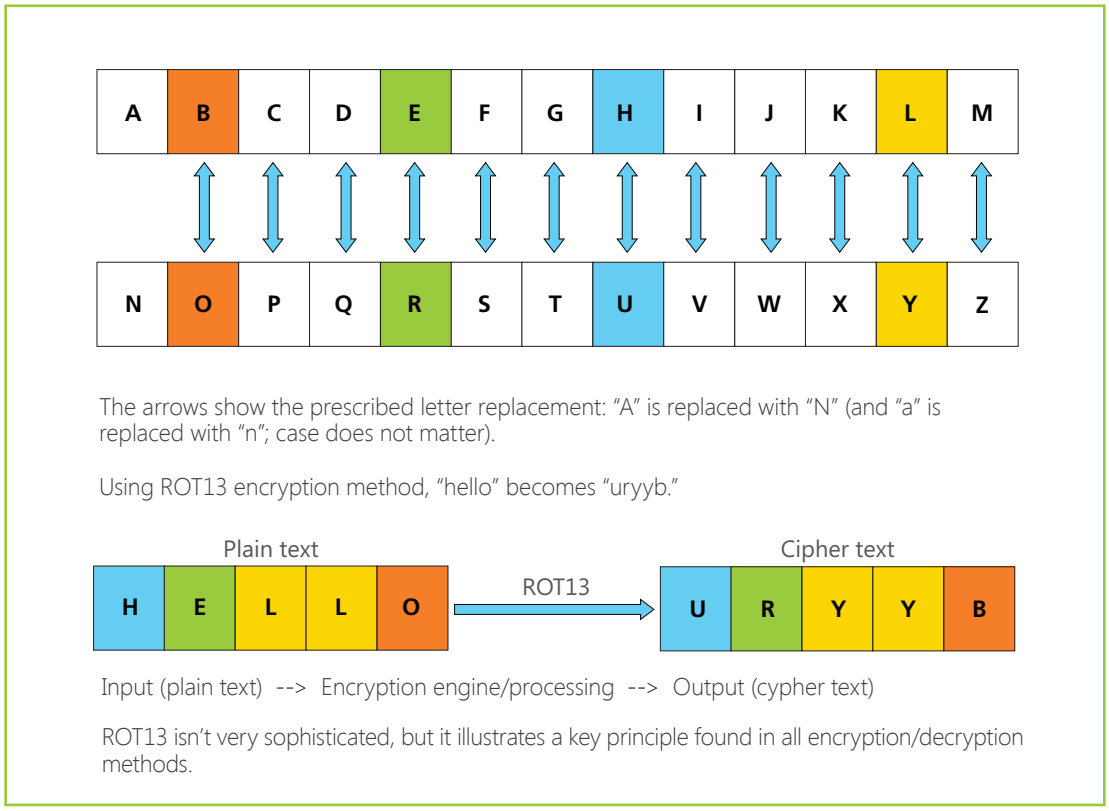

Figure 1: Simple Encryption

Factors Driving Adoption

More and more data storage applications are adopting — and even requiring — encrypted solutions. Mobile computing is where much of the pioneering work on encrypted storage was done simply because these devices (like laptops and tablets) take sensitive data out into the world where the likelihood of being lost or stolen increases. However, the miniaturization of computing hardware isn't limited to mobile devices. Desktop computers and workstations are no longer cumbersome and immune from theft. Even in the data center, server hardware is smaller, and though rare, entire servers have gone missing from computer rooms.

Data Is More Valuable Than Its Device

One doesn't have to look far to find many well-publicized examples of mobile workers losing a notebook computer containing sensitive information like client social security numbers, credit card information, and even business research and intelligence. Theft of personal computers from homes and businesses is certainly common. In the past, the motivation for thefts was to sell the stolen hardware. But today, identity theft and other electronic crimes make data stored on the computer much more valuable than the computer itself.

Even systems that are closely controlled by their owners are vulnerable. Computer hacking has graduated from an annoyance to big business. Beyond wanting to impress their peers, hackers today are out to compromise systems and steal sensitive (and valuable) data, which they can then sell to the highest bidder. Encryption is even becoming a weapon of choice for attackers in the form of "ransomware." Sensitive data is encrypted with a key known only to the attacker who forces the victim to pay in untraceable currency to get the key to unlock sometimes invaluable data.

Sensitive Data Coming Out of Retirement

One common data loss vector happens when data storage devices are retired or redeployed. Tens of thousands of disk drives and SSDs are retired from service every day in data centers around the world. There have been well-publicized events when these retired drives have found their way to second-hand stores or online resellers with sensitive — even top-secret — data still stored and unencrypted.

New Rules and Regulations

The sheer volume of data intrusions and data loss is now driving changes to corporate policy and legal governance, demanding solutions to the problem. Governments throughout the world have passed regulations that put responsibility for data protection on both the end user and the corporate officer, with severe consequences when protection is insufficient. Even when no customer or client data is at risk, internal corporate documents — designs and intellectual property, security policies and processes, corporate financial data and other sensitive information — all must be kept private.

Computer hacking has graduated from an annoyance to big business. Hackers are out to steal sensitive, valuable data and sell it to the highest bidder.

Protecting Data at Rest

Any encryption method at the storage device level is intended to protect "data at rest," meaning data that is stored and static on a device. Specifically, it refers to data stored on an unpowered device. Protecting data at rest ensures that the data remain secure if the owner loses physical control of the storage device. It's important to note that once proper credentials are delivered to unlock and decipher encrypted data, the data is "in the clear" and readable by anyone with access to the computer system. Because active computing leaves data in the clear, storage device encryption is not a substitute for network firewalls or malware/virus detection, prevention and mitigation. Storage device encryption is an important part of a layered approach to protecting sensitive data.

File Level vs. Full Disk Encryption

When considering encryption in a data storage system, it is important to think about the structures in which data is stored and accessed and how those structures are protected with common encryption techniques.

In any computer system, whether notebook, workstation or server, the storage device is almost always a hard disk drive (HDD) or a solid state drive (SSD). Regardless of the media type, data storage is divided into boot, operating system and user file/directory areas. In some implementations, these areas may be spread across multiple devices. Whether disk encryption schemes protect some or all of these three areas of the disk, they are commonly divided into two basic types: file/folder encryption and full disk encryption (FDE).

Figures 2 through 5 show examples of disks with different levels of encryption. Unencrypted areas are in yellow and encrypted areas in blue. In Figure 2, the system has no encryption implemented, so all sections of the disk are vulnerable: boot sector, operating system and user data. In Figure 3, the user's files and directories are encrypted, which assumes that the encryption is robust enough to make encrypted data essentially inaccessible to any user who does not have proper credentials. In Figure 4, the encryption extends to the OS itself, meaning all OS bits are encrypted as well as the data that the OS creates, temporary or permanent. In this example, the core library files, executables, user settings, and registry and swap files would be protected.

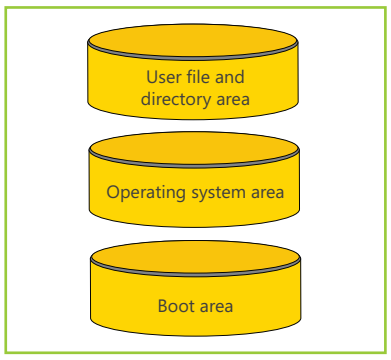

Figure 2: No Encryption – Entire Disk Vulnerable

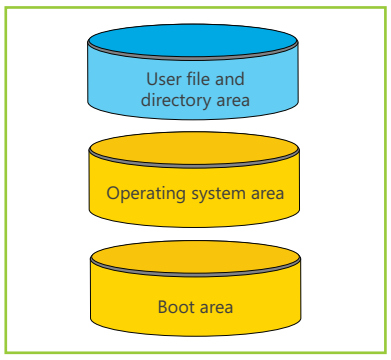

Figure 3: Partial Encryption – User Files and Directories Protected

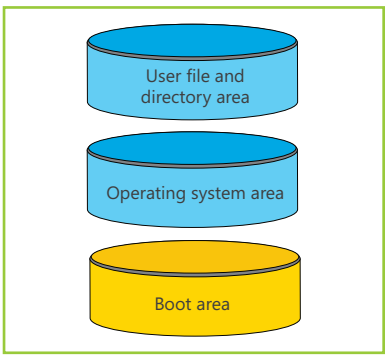

Figure 4: Partial Encryption – User Files, Directories, OS Protected

Note: *These figures are conceptual only. Particularly in SSDs, physical locations can be interspersed and fragmented due to dissociation between logical data addresses and physical storage locations.*

When encryption is extended to the next logical level — the entire disk — it is commonly referred to as full disk encryption (FDE), as shown in Figure 5. With FDE, all areas of the disk are encrypted and thus protected from unauthorized access — from the boot area, to the operating system, to the user data files and folders. Full disk encryption is the most sophisticated and secure method of data encryption on a local drive.

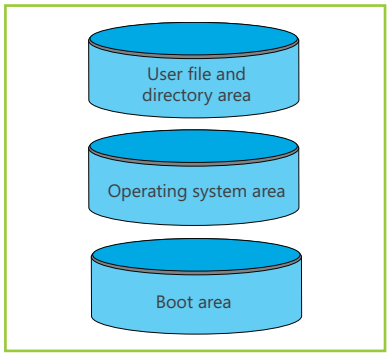

Figure 5: Full Encryption – Entire Disk Protected

Benefits of Folder and File Encryption

Benefits of implementing encryption at the folder/file level include:

- Data encryption can be implemented on local drives or network shares, giving consistent security regardless of the storage type (local or network).
- Because the same protection can be implemented on shared and local drives, it can be governed by consistent network and security policies, such as access control lists (ACLs) and authentication mechanisms (like passwords and biometrics). It can also be easily managed from a central location (like a policy server or biometric record server).
- The user can specify files/folders to encrypt, leaving non-sensitive data in the clear for easy access.

Encryption at the folder and file level offers an important advantage compared to FDE: Folder/file encryption is capable of protecting data in transit, whether sent via e-mail, shared via a removable drive like a USB stick drive or burned to optical media. Because the files themselves are encrypted independent of the media on which they are stored, protection is extended to data in transit. For this reason, even in a full drive encryption scheme, folder/ file encryption is a helpful tool to protect data in transit from one computer to another.

Figure 6 shows a folder/file encryption scheme where each user is employing folder/file encryption. The user on the left emails an encrypted file to the user on the right. The file stored in the system on the left is protected by file-level encryption and does not need to be decrypted prior to transmission because it is transmitted as cipher text (shown in blue). After received by the user on the right, the file (still encrypted) can be decrypted, assuming that the user on the right has the correct credentials.

IT managers should be aware that user mistakes can be a vulnerability in systems that deploy only folder/file encryption. Users can easily and inadvertently store sensitive data in unencrypted disk areas, leaving the data vulnerable to loss or breach.

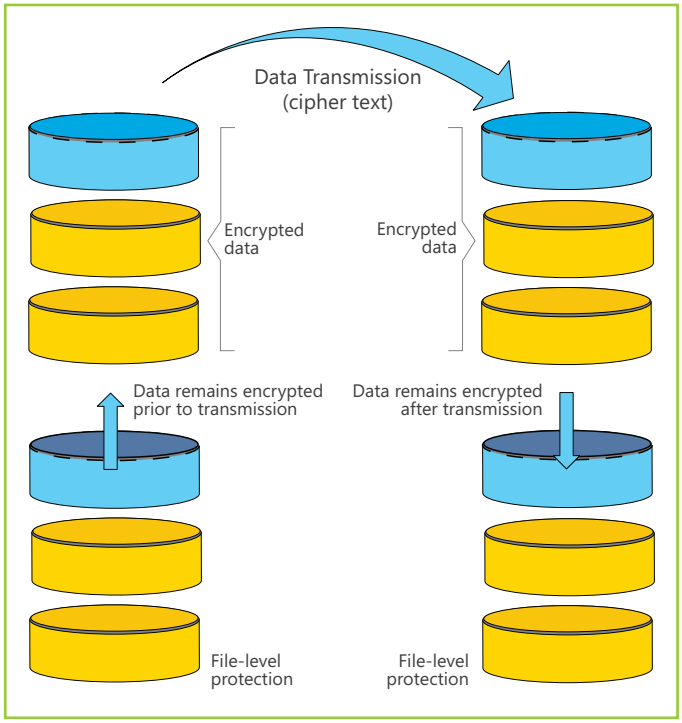

Figure 6: Folder and File Encryption

Benefits of Full Disk Encryption

Full disk encryption (FDE) has significant benefits over other levels of encryption, including:

- Typically, an FDE system requires one password entry at power-up. After the user is "authenticated," computing activity can continue normally. The encryption scheme is transparent to the user.
- The encryption mechanism itself can be implemented in hardware or software, offering design flexibility and cost options.
- Every bit on the storage device is encrypted: the operating system, user and program data, the applications themselves (and the data they create during normal operation), as well as the OS swap file (which may contain data otherwise held in memory).

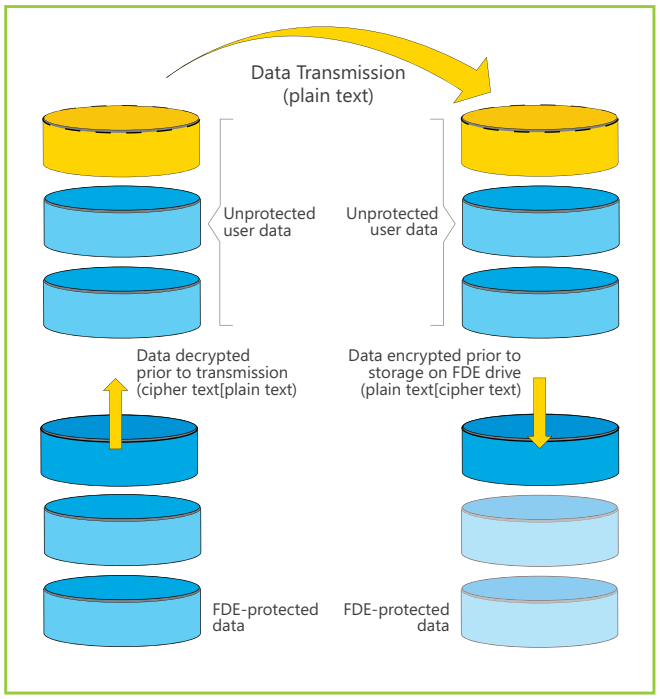

Figure 7: Full Disk Encryption

- A hard disk can be "married" to a platform via a Trusted Platform Module (TPM), making drives that are removed from the platform immediately unreadable when the device is detached, unless user credentials travel with the drive. (See the Role of a Trusted Platform Module section for more information.)

User Authentication in FDE Systems

While encryption algorithms alone are very interesting mathematical devices, they are useless without a robust authentication scheme that requires an authorized user to provide credentials to access the computing system and stored data. In simplest form, a user's credentials are delivered through a password or pass code; however, a user's credentials can also be confirmed via a biometric scan like a fingerprint reader or a voice or facial recognition scan. Smart cards, physical keys and other hardware methods are also used. Multi-factor authentication is also becoming important, combining a pass code with a second key, which can take a variety of forms.

Encryption can be a strong method to protect data, but the encryption scheme is only as strong as the password discipline. Short or easily guessable passwords enable easy by-pass of an encryption system. While a 256-bit encryption key could take literally thousands of years to break, a pass code of "1234" or "password" can be breached in just minutes.

FDE vs. SED

An SED is a special form of FDE, with some distinct differences and advantages. FDE is the more generic term that describes full encryption of a storage device's entire contents, usually accomplished using software tools. SED is a method of FDE that is always hardware-based.

SEDs can be extremely easy to deploy and support in a variety of enterprise environments.

An SED will always have a hardware-based encryption engine on board, often integrated into the drive's controller. Micron's SEDs use Advanced Encryption Standard (AES) 256-bit encryption engines and support the Trusted Computing Group (TCG) protocols for hardware-encrypted storage devices.

Specifically, Micron's personal storage SSDs support the TCG Security Subsystem Class (SSC) Opal protocol while its enterprise storage SSDs support the TCG SSC Enterprise protocol. (Contact your Micron sales representative to determine which protocols are supported for a specific Micron model number.)

Advantages of SED and Hardware Encryption

As previously mentioned, an SED hardware encryption implementation has some distinct advantages over a software FDE implementation.

Ease of Deployment

SEDs can be extremely easy to deploy and support — in an enterprise with many notebook computers or in a data center with server arrays containing huge numbers of drives. Even though bits written to the storage media are encrypted in an SED, unless a protection scheme is activated, a read command to the drive always decrypts the bits. So an unprotected drive behaves as if the data were completely unencrypted.

However, activating data protection is as simple as installing a security software application and clicking "Enable." No additional encryption step is necessary. Software encryption, on the other hand, can take hours for first-time encryption of user data.

Simpler Key Management

Key management is much simpler for SEDs, particularly for enterprise computing systems. An SED encryption key is generated internally to the drive and remains on the drive, unreadable by any interface command.

Micron SEDs create the encryption key using an on-board True Random Number Generator (TRNG), which is one of the most secure methods of key generation. Because the keys are self-generated and stay with the drive, the additional overhead of key management servers and software is unnecessary. The host computer only has to support authentication key security and management, as well as pass code backup and restore.

Performance

Performance is perhaps the most important advantage of SEDs. Many software encryption schemes come with a performance penalty. For example, in notebooks and PCs, software encryption requires constant CPU operational bandwidth. SEDs, on the other hand, perform encryption in-line in an engine separate from the drive's own controller. This removes the encryption workload from the CPU to provide performance that is effectively the same as a completely unencrypted system.

In server storage, the bandwidth necessary to perform the software encryption functions is finite, so as storage needs require more drives in the array, the system performance penalty can become a scalability limiter. But with SEDs in the storage arrays, the encryption load is spread among the individual drives. Therefore, the scalability of a hardware-encrypted system when adding SEDs is exactly the same as if those drives were not encrypted, limited only by the underlying system architecture.

Pre-Boot Authentication

For client computing systems (notebooks and desktops) the TCG Opal specification provides an additional security feature known as pre-boot authentication (PBA). PBA can be performed in a system BIOS or UEFI, enabling authentication by password or other methods before the OS is up and running. This prevents potential OS-level malware from detecting and attacking the authentication process in what is usually known as a "rootkit attack" or sometimes more informally as an "evil maid attack." These types of attacks could launch a keystroke logging program that records a password entry for later use in a data theft.

BIOS/UEFI deployment is ideal for single-computer implementation. However, in an enterprise that may own and manage many computers, the Opal-compliant drive also enables PBA in a special boot area created by management software. After the BIOS/UEFI is complete, all system hardware is activated and a special-purpose graphical user interface (GUI) within this small boot area can operate.

In this fashion, PBA enables communication hardware, such as the Wi-Fi modem or NIC card, to reach out to the home office over the Internet and authenticate with a corporation's IT office prior to user authentication. Thus, an IT manager can disallow access to a stolen or lost notebook even when that computer is outside the walls of the company.

Note: Specific functionality of this special-purpose GUI for PBA is beyond the scope of the drive manufacturer. Details are available from the specific security software vendor.

Performance is an important advantage of SEDs. Because they perform encryption in-line in an engine separate from the drive's controller, SEDs provide performance that is effectively the same as a completely unencrypted system.

Considerations for Software Encryption

Performance Degradation

As mentioned earlier, software encryption mechanisms often rely on CPU and memory resources in the host system. Therefore, software encryption often causes a significant and noticeable reduction in data throughput performance.

End-to-end software encryption management requires encryption of data blocks that are not in use (in addition to user data), which adds even more performance overhead. This is especially important for SSDs because end-to-end encryption can result in an SSD that behaves as if it were 100% full. Micron has observed as much as a 20% degradation in data throughput due to software encryption, especially for write speeds.

Upgrade Path Difficulties

Just as the initial deployment of hardware encryption can be disruptive (requiring new hardware), software encryption methods can be subject to interoperability concerns among software applications, operating systems, patch levels and other software elements essential to end-user productivity.

Some software encryption deployments prohibit certain firmware updates. In these cases, before an update is performed, all user data must be decrypted, leaving it temporarily vulnerable. Then it must be re-encrypted after the firmware update is complete. Even on an extremely fast SSD, decrypt and encrypt steps can take significant time. For example, encrypting 25GB of user data can take more than one hour even on a very fast system.

A time-consuming decryption step is also required when cloning a drive: Cloning an encrypted drive to a new drive results in a drive full of unreadable data because the two drives will have different encryption keys.

Software Additions to Existing Hardware and Platforms

Fortunately, software typically does not require deployment of additional hardware; therefore, it can easily be added to existing environments with less disruption and less cost compared to hardware-based encryption. Often, software encryption methods can be integrated into the operating system.

Role of Trusted Platform Module

The Trusted Platform Module (TPM) is a tamper-resistant hardware device permanently affixed to a system main-board to help integrate basic security management functions and thwart common attacks. As shown in Figure 8, TPM provides several essential functions that help make encryption more robust and easier to implement, including the following examples:

- Platform identification to ensure that the platform accessing the data is what it claims to be
- Secure subsystem to ensure a hardened area within the host
- Platform configuration definitions (registers)
- Random number and hash generation
- Encryption/decryption key generation
- Key storage

In addition, the following essential functions are all housed inside the TPM chip or inside a notebook, desktop, server or storage array:

- Nonvolatile secure storage
- Platform configuration data
- Opt in/out switch
- Hardened execution partition
- Data-unique platform ID keys

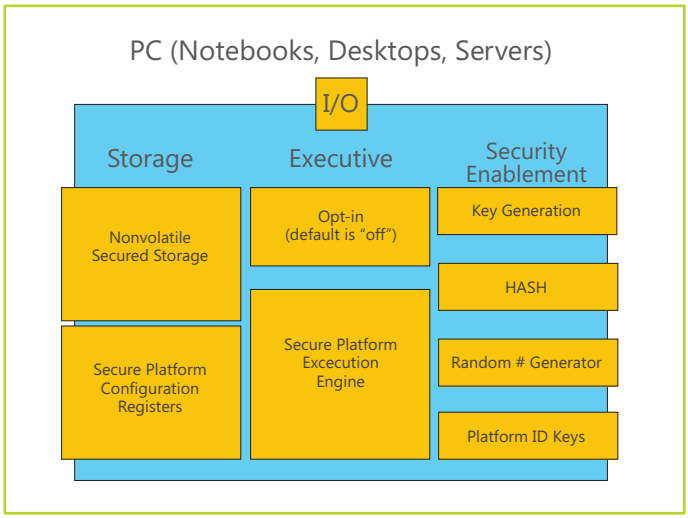

Figure 8: Trusted Platform Module (TPM)

Another essential function of the TPM is to establish the identity of the system itself with respect to the encrypted data. The TPM and the disk drive can be "married" to one another. The data storage system, such as an SED, and the system main-board are closely coupled through the use of stored decryption keys.

Once the disk drive and the TPM are "married," it is nearly impossible to read the data on that hard drive when the drive is removed from the original system and installed in another. The TPM signatures don't match and the data won't decrypt.

When data is encrypted, the key used to authenticate the user must be stored somewhere. For ease of use, the key should always be readily accessible to the user and be tamper-resistant. An ideal place for key storage is the TPM itself; it provides both a secure platform execution engine and the capability to generate keys and random numbers (essential functions), as well as a tamper-resistant storage area for those keys.

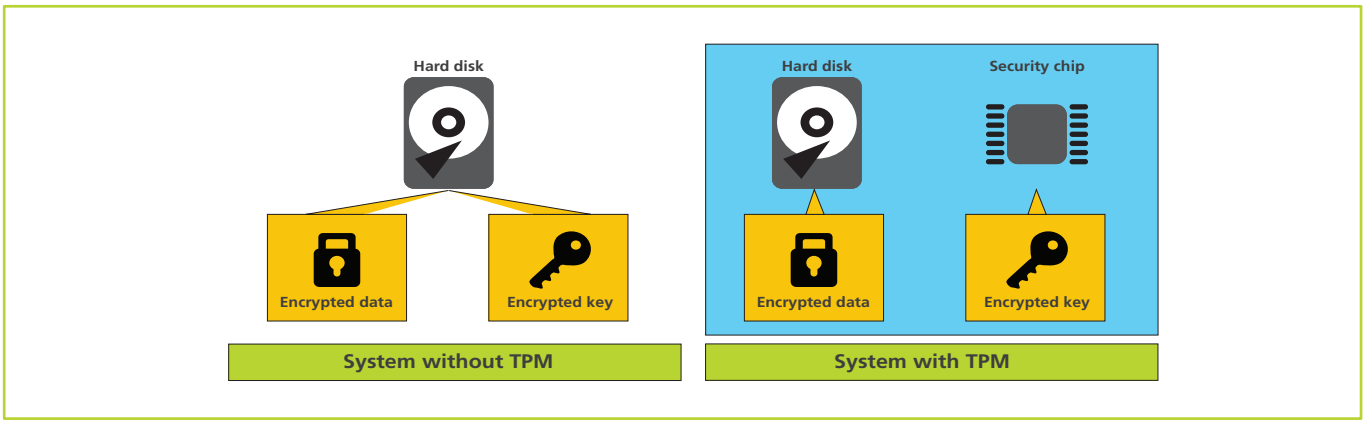

Figure 9: System Comparison

As shown in Figure 9, in a system without a TPM, the decryption keys are stored on the local hard disk — the same media that should be protected with encryption. Storing the key and the data on the same media increases the risk of unauthorized access.

In a system with a TPM, the decryption key comes from the TPM itself. If the drive is removed from the system, the TPM and drive are decoupled; and since the decryption key is stored on the TPM, it is impossible to read the data.

Note that although a TPM makes deployment of an SED easier, is not required. Without a TPM, some systems require special OS registry settings to operate. Others use an external device like a USB thumb drive as a key. Using this key does provide a more secure authentication process, but it can be quite inconvenient and poses a risk of data loss if the USB key is lost.

Role of Trusted Computing Group

Who is the Trusted Computing Group (TCG) and how do they factor into encryption and authentication? Founded in 2003, TCG is, at its core, a standards organization. Membership-driven, TCG's primary role is to gain consensus from membership, develop and publish standards, and drive adoption of these standards in the industry.

Organized by functional area, standards are developed and proposed by groups within TCG whose members are experts in a given area. Once a standard is published, TCG drives the adoption of the standard within the developer community and end-user markets.

As a standards body, TCG plays an essential role in getting the different encryption and authentication methods to work together (via standards). Micron Technology is a contributing member of the TCG.

Role of the OS

What role does the OS play in data encryption? In many cases, the OS is simply a bystander. Encryption management and authentication functions are handled by an application, and in the case of PBA, these applications run before the OS boots. However, applications within the OS can run for operations such as password changes and enabling or disabling certain security functions authenticated by the user. In other cases, encryption functions and SED management can be integrated into the OS.

Note: Detailed instruction on implementation of SEDs within an OS are available from the OS vendor.

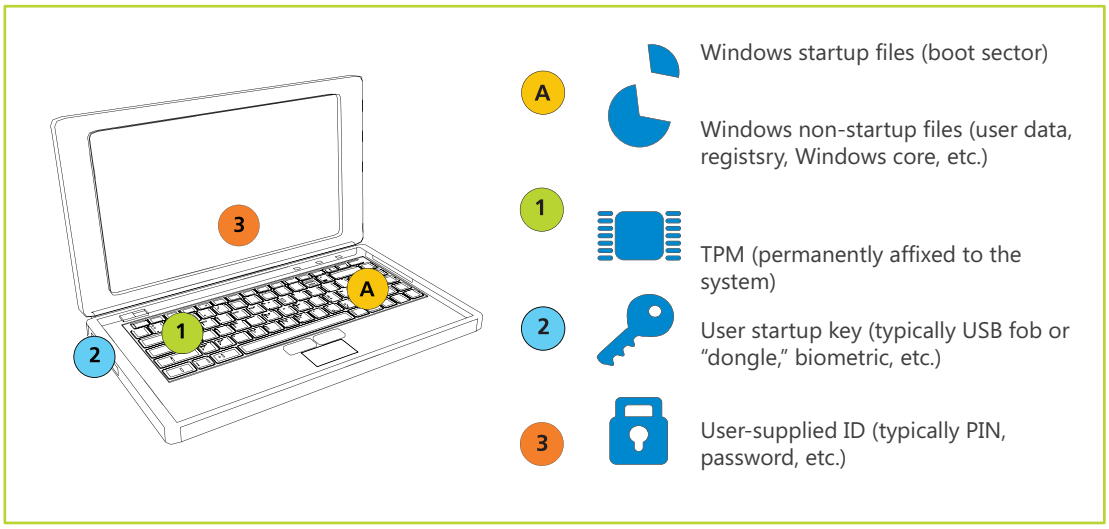

Figure 10: Role of the OS

Important BitLocker Developments in Windows 8 and Windows 10

One of the most common OS-based encryption management schemes is Microsoft® BitLocker®, within the Windows® OS. In previous versions of Windows, BitLocker provided only software encryption. However, beginning with Windows 8 and continuing to Windows 10, BitLocker provides integrated support for either software encryption (as in Windows 7) or hardware encryption using an SED. This SED support is available only in the Professional and Enterprise versions of Windows 8 and Windows 10. Windows 7 BitLocker only supports software encryption — and only in the Enterprise and Ultimate editions.

Microsoft deploys hardware encryption under the moniker "encrypted hard drive," where the SSD must meet the following criteria: TCG Opal 2.0 protocol requirements and IEEE-1667, the "Protocol for Authentication of Removable Storage Devices."

Micron's newer SEDs meet both requirements and can be seamlessly integrated into a hardware encryption system under BitLocker in Windows 8 and 10 Enterprise and Professional versions. Contact your Micron sales representative to determine which Micron SSDs support encrypted hard drives.

Microsoft provides support documentation with important system-level requirements. Visit **microsoft.com** and search for "encrypted hard drive."

Universal Adoption of Data Encryption

Despite some concerns over complexity, clearly an encrypted drive is more secure than an unencrypted drive. With security garnering so much attention lately, why isn't SED, or the more general FDE, universally adopted?

In 2015, Coughlin and Associates, an industry analysis firm, reported that by 2017, nearly 100% of SSDs intended for notebook and desktop applications would have SED capability, but that unless circumstances changed, only 10% of these SEDs will use encryption features. The Ponemon Institute, a pre-eminent research center dedicated to privacy, data protection, and information security policy, conducted an end-user survey to determine why. System performance, complexity, and cost concerns are among the top reasons stated.

Trend Toward Hardware-Based Encryption

The SED with hardware-based encryption can address all the concerns discussed in the Ponemon report. While the other encryption schemes discussed here are perfectly acceptable options, the SED offers the best combination of benefits to the end user and system designer.

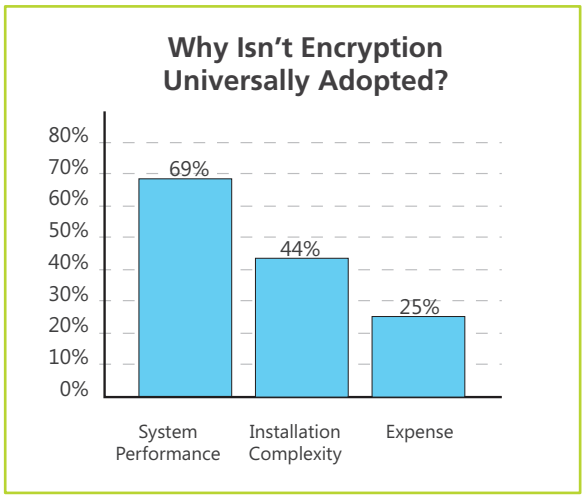

Figure 11: Perceived Impediments to Encryption Adoption

Hardware-based encryption is superior to software-based encryption in the following three major categories discussed in the Ponemon study above:

- **Performance:** Hardware encryption does not incur the CPU and memory overhead that software encryption does and, therefore, maximizes performance. Hardware encryption will seem invisible to the user.
- **Total Cost of Ownership (TCO):** SEDs offer the lowest TCO for encryption solutions with the best performance, lowest acquisition costs, higher user productivity, and simplest IT management and deployment (Source: Report by Trusted Computing Group, April 2013).
- **Data Security:** 256-bit hardware-based self-encryption and user authentication offer superior protection against data breaches, loss and theft compared to software-based encryption, which is vulnerable to attack through the memory device, OS and BIOS. Hardware-based encryption is performed in the hardware — user authentication is performed by the drive before it will unlock, independent of the operating system.

Government Standards and Requirements

The final piece of a complete managed security system is meeting government standards and receiving government certifications for secure, encrypted data storage. In the United States, these standards are managed under the Federal Information Processing Standards, known as FIPS. Specifically, the document controlling cryptographic devices is FIPS 140, Revision 2, or "FIPS 140-2." The National Institute of Standards and Technology (NIST) in the U.S. and the Communications Security Establishment (CSE) in Canada are responsible for certification of devices under FIPS 140-2.

FIPS 140-2 requirements are described using four different levels, with increasing security requirements:

- **Level 1:** Basic security of the encryption engine and associated firmware
- **Level 2:** Level 1 plus requirements for tamper evidence that clearly show an attempted physical intrusion of the storage device.
- **Level 3:** Level 2 plus requirements for tamper resistance to prevent an intruder from detecting secure information in the cryptographic module.
- **Level 4:** Level 3 plus requirements for high probability of detection of an attack and the capability to destroy secure information cryptographically, or otherwise, upon detection of an attack.

In most cases, Micron SEDs will meet FIPS 140-2, Level 2, when and if certified.

The next revision of the FIPS 140 document will be called FIPS 140-3 and is scheduled for document release during 2017. FIPS 140-3 has undergone many iterations prior to its publication, but the final release will be a direct implementation of the ISO/IEC 19790:2012 document. This will allow for greater international compliance and consistency with regard to encryption standards.

An emerging new requirement for computer security is known as "Common Criteria." The Common Criteria is an international standard, under ISO/IEC 15408, and administered in the USA by the National Information Assurance Partnership (NIAP). This document provides a framework describing Security Functional Requirements (SFR) and Security Assurance Requirements (SAR). Storage device manufacturers implement security features as described in this paper, and the Common Criteria allows testing laboratories to evaluate and grade these claims, providing assurance to the customer that security features work as expected.

Micron's security architecture team will continue to strive toward compliance with these security standards, and for necessary markets, achieve certifications that our specific products meet these standards.

Conclusion

Starting with the M500 SED, Micron provides the full benefits of hardware-based encryption to its personal storage SSDs by enabling hardware encryption according to the TCG Opal protocol or the ATA Security protocol. Micron's family of SEDs provide an ideal solution for any application that needs easily integrated, cost-effective data protection.

In 2015, Micron's M500DC and M510DC became the first SATA SSDs in the world to offer the option for a TCG Enterprise SED, bringing easy and efficient SATA hardware encryption to the data center.

During 2016, the Micron SED family is expanding to include encrypted SAS drives and PCIe® NVMe™ SSDs. In early 2017, Micron will offer its first FIPS 140-2 Level 2-certified SATA SSDs for enterprise and client computing.

Featuring an AES-256 encryption engine coupled with powerful firmware algorithms, Micron's SEDs provide hardware-based data encryption — with no loss of SSD performance — in accordance with industry standards for trusted peripherals and government data security regulations.

Micron's SEDs are designed to work with mainstream third-party independent software vendor (ISV) encryption management tools to provide a complete data security system. Micron's SEDs are also certified under the Windows Hardware Certification Kit (WHCK), and therefore, compatible with Windows 10 BitLocker.

Get solid data security solutions at **micron.com/federal**.

Micron SEDs provide hardware-based data encryption in accordance with industry standards for trusted peripherals and government data security regulations.