White Paper

Hardware-based AES Encrypted Storage Solution

The AES hardware-encrypted SSD can reliably encrypt and decrypt data, while TCG OPAL 2.0 compliance offers flexible data access management as well as additional security measures.

Introduction

Secure data encryption is essential for a wide variety of mission-critical applications pertaining to both civilian matters and national security. These sectors both require comprehensive safeguards to protect sensitive data.

Advanced Encryption Standard (AES) hardware-encrypted solid state drives (SSD), also called self-encrypting drives (SED), offer a proven and efficient method of encrypting stored data. TCG OPAL 2.0 compliance enables additional security layers and extended user management options.

Because of its complexity, it is not possible to brute-force the AES algorithm using any current or foreseeable technology. There are however other ways to crack the cipher; many of which can be addressed by applying hardware-based encryption as opposed to a software solution.

This paper will expand on this issue and other challenges such a data management, while also giving a more thorough explanation on the different features of AES and the related tools and standards.

Background

The theoretical framework for block ciphers such as AES was proposed in the 1940s, while the first widespread use started in the 1970s with AES's progenitor Data Encryption Standard (DES). DES was abandoned in the beginning of the 2000s as it was seen as not being up to par.

The American National Institute of Standards and Technology (NIST) adopted AES in 2002. AES is also known as Rijndael after its two inventors. It was a specification for electronic data encryption and was chosen for its optimal balance between performance and security. The algorithm was the first of publicly available ciphers to be approved by the US National Security Agency (NSA) to protect classified information.

The hardware encrypted drive utilizes a built-in AES 256-bit encrypted engine located in the controller. The AES engine confirms to the AES algorithm (certificate No. 2474), the Deterministic Random Bit Generator (DRBG) algorithm (certificate No. 337), and the Secure Hash Standard (SHS) algorithm (certificate No. 2093).

Challenges

Challenges pertaining to SSDs and data security can be separated into three categories: secure data encryption, software encryption issues and management.

Secure Data Encryption

The main challenge with data encryption is keeping the encrypted data safe. This means being safe from brute-force attacks and other cracking attempts. The encryption level not only has to handle current threats, but also potential future decryption techniques and the threat that comes along with exponentially growing computational power.

Another aspect to consider is how to render the data unusable if the storage drive is compromised. Any drive that falls into the wrong hands will eventually, at least in theory, be cracked. As such, there have to be measures available to quickly sanitize sensitive data.

Limitations of Software Encryption

Software encryption is a reliable method to secure data and is easily implemented, but there are drawbacks:

- Lowers system performance: As all encryption and decryption is handled by the CPU, system performance slows down when data is written or read.
- More vulnerable: Software encryption is only as strong as the system it operates on; a flaw in the OS can easily be used to break the encryption. In addition, it is naturally susceptible to viruses and malware and more prone to human error, such as the user altering or turning off the encryption.
- Unencrypted data: There might be files and data that are hidden and will remain unencrypted.
- OS dependence: The software is dependent on the OS, thus limiting what software can be used.

Management

If several users are accessing the drive, simply encrypting all the data might not be enough as each user has different clearance levels. This requires different access ranges to ensure that the data is kept at a strict need-to-know basis.

Solutions

Hardware AES Security

AES Encryption Key

Data encrypted with the 256-bit AES key is protected behind an algorithm that with today's technology is all but impossible to crack. While theoretical attacks have been shown to be possible, they are nowhere near feasible as it would take billions of years to brute force.

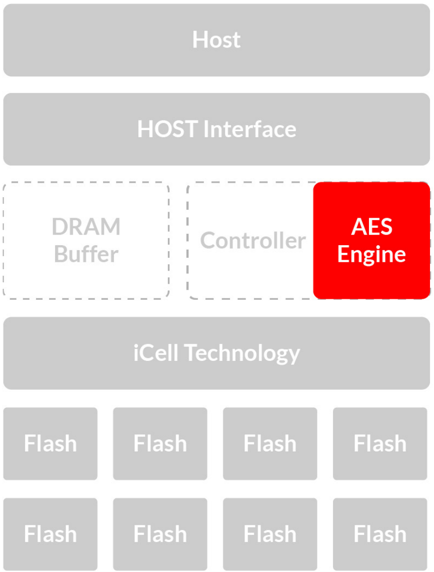


Figure 1: Hardware-based 256-bit AES engine in controller

The AES engine is a hardware design that is built inside the controller (see figure 1), in other words, there is no impact on CPU performance, as the controller will handle all encryption and decryption.

Hardware-encryption also means that the process is fully OS independent, as it does not require compliance with any system or software.

It is not possible to observe the encryption process itself, meaning the user cannot see the encrypted data, as all data that is read will already have been decrypted.

When the SSD controller leaves manufacturing, a series of random numbers will already be generated as the AES key, which is then stored in the NAND flash and is only known by the drive itself. The data will be encrypted and decrypted with this internal AES 256-bit key for all the data written to and read from the device. SSDs with internal AES Encryption Key operate just like normal SSDs.

ATA Security Authorized Key

ATA security features are a set of commands that can help the user manage storage devices, and is accessed through the BIOS (see table 1).

In order to complete the physical security layer of protection, the AES encryption needs to be bundled with the ATA Security command. This is done by enabling an ATA authorized key, which offers an authentication for the drive owner to lock or unlock the SSD for read or write commands. If the authorized key is not set, the SSD will appear to behave like a normal SSD.

Unlike the AES key, the authorized key must be set by the user via BIOS configuration. The ATA Security Password has to be entered with each power cycle and only when correctly entered will the SSD be accessible.

Command	Command Code
SECURITY SET PASSWORD	0XF1
SECURITY UNLOCK	0XF2
SECURITY ERASE PREPARE	0XF3
SECURITY ERASE UNIT	0XF4
SECURITY FREEZE LOCK	0XF5
SECURITY DISABLE PASSWORD	0XF6

Table 1: ATA security command set

AES and ATA Key Combination

With the ATA security authorized key set, not only is the logical data safely encrypted, but the physical drive is protected as well. In other words, if the SSD falls into the wrong hands, the SSD cannot be opened without the password. The information stored inside the NAND flash is safe because all that can be read is randomized, encrypted data.

When the power is switched on, the user is required to enter an ATA security password to get access to the SSD, and the user is only then allowed to send read or write commands with the internal AES Encryption Key for encryption or decryption (see figure 2).

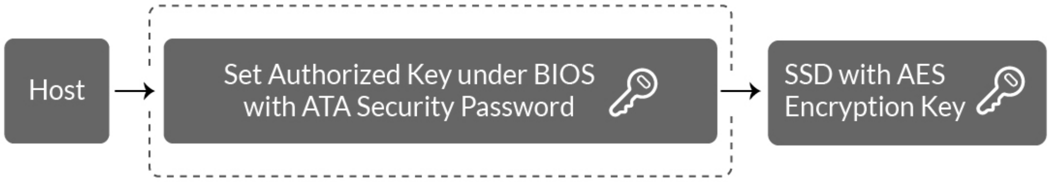


Figure 2: AES encryption works along with ATA security password to achieve full protection of the SSD

Sanitizing Drives

Sanitizing means rendering encrypted data useless by changing the AES encryption key. This operation is initiated through the ATA Cryptographic Erase command (see table 2). After the key has been altered, the data written with the previous key would appear to be random, incomprehensible data. This function also allows the user to verify that the hardware encryption actually works. The purpose of the ATA Cryptographic Erase command is to sanitize all user data and make it unreadable, leaving out time-consuming normal erase procedure that requires many cycles of data overwriting.

Field	Description	
FEATURE	0011h	
COUNT	Bit	Description
	15:5	Reserved
	4	FAILURE MODE bit
	3.0	Reserved
LDA	Bit	Description
	47:32	Reserved
	31:0	Shall be set to 4372_7970h(DWord)
DEVICE	Bit	Description
	7	Obsolete
	6	N/A
	5	Obsolete
	4	Transport Dependent
	3:0	Reserved
COMMAND	7:0 B4h	

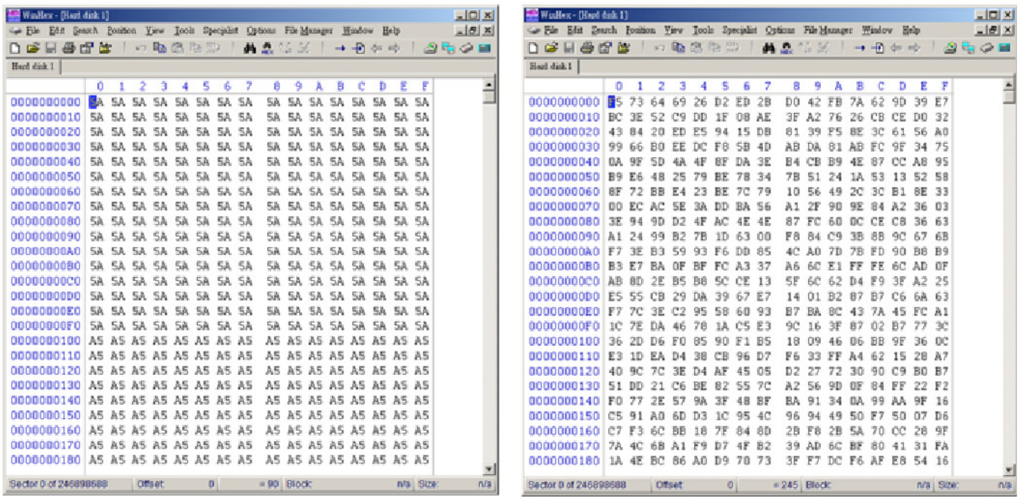
Table 2: ATA Cryptographic Erase command

For example:

1. The user receives a self-encrypted SSD and inputs 'AA55', the user will read the same data pattern as AA55 as the SSD internally encrypts and decrypts the data with Key A which is generated by the firmware before leaving the factory.
2. Key A is then changed to Key B using the ATA Cryptographic Erase command. At this time, the user is only able to read data as a random string of alphanumerics (See figure 5).
3. If you write the sequence AA55 with Key B again, then the system will output AA55 again as the data is also decrypted by Key B.

Both Key A and Key B are invisible to the user as they are randomly generated by the SSD firmware.

Before **After**



AA55 written with Key A **Read as random data with Key B**

Figure 3: Using the ATA Cryptographic Erase Command to alter the AES encryption key

TCG OPAL 2.0

With TCG OPAL 2.0 a new layer is added on top of the basic setup explained above. It is a set of security protocol specifications defined for industrial data storage devices, and are published by the Trusted Computing Group's Storage Work Group. To take full advantage of TCG OPAL 2.0, the standard involves not only SSD vendors, but also system installation and management. Third party encryption software and utilities are also required to fully implement OPAL functions.

TCG OPAL states that SSDs must be self-encrypted with an AES hardware encryption engine. In-addition, the user is required to pass a boot-up authorization procedure. When the system is switched on, a pre-boot shadow image will be shown to safeguard the real Master Boot Record (MBR). Once the authorized password is entered, the real MBR and OS will be loaded for further authority management (see figure 4).

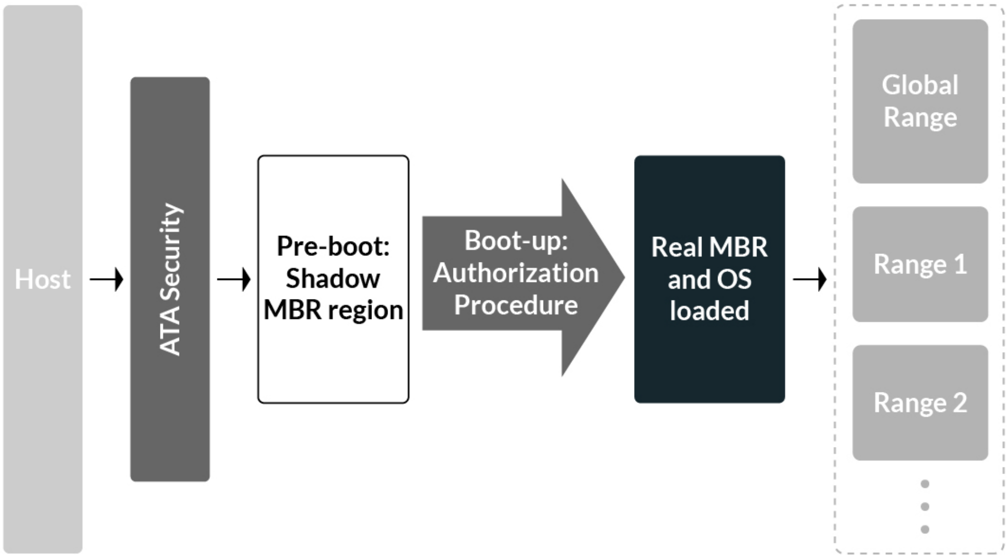


Figure 4: TCG OPAL 2.0 Operation Process

OPAL also allows for the partition of access control to read/write/erase independent LBA ranges for individual users (see figure 5). “Global Range” is the default settings that encompass the whole user data area. In the figure below, the drive has been altered such that LBA Range 1 and 2 can only be accessed by user 2 and 3 respectively.

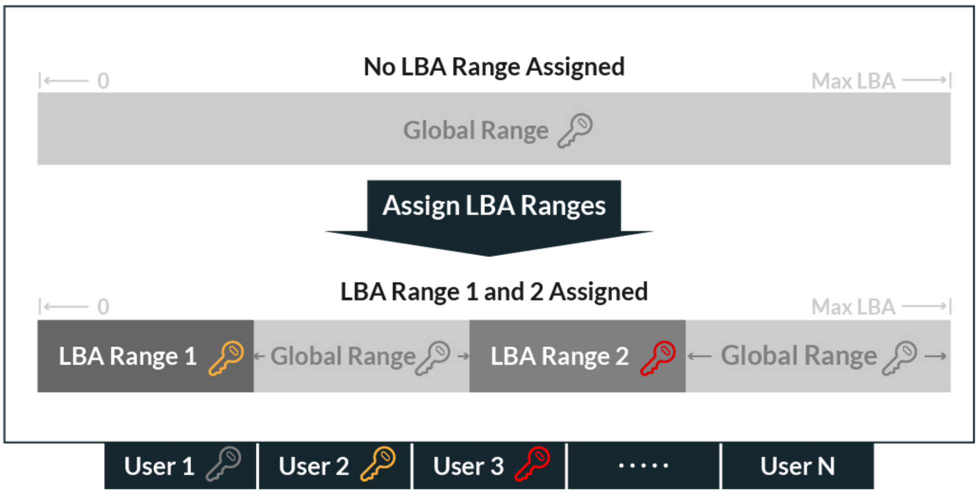


Figure 5: LBA Range Operation

SEDs compliant with TCG OPAL 2.0 enables the use of both Manufacturer Secure ID (MSID) and Physical Secure ID (PSID):

- MSID: MSID works as a master ID that must be input to access the real MBR. After accessing it for the first time, the user can then set up passwords for individual LBA ranges and create a multiple-user system.
- PSID: PSID is a command that can be input to revert the SSD back to default factory settings. This means that the AES Encryption Key will be permanently changed and user data will be randomized, affectively sanitizing the drive. At the same time, the main password will revert to MSID.

Conclusion

TCG OPAL 2.0 certified AES hardware encryption offers strong, multilayered protection for confidential data.

By keeping the encryption/ decryption process in the SSD controller, the user avoids the risks and drawbacks associated with software encryption such as OS weaknesses to cracking, OS dependence and reliance on system CPU.

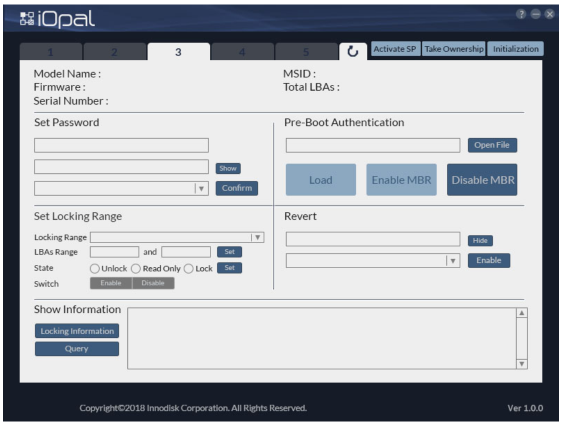
If the data you are storing is critical, a hardware-based AES solution will always be the more secure choice.

The Innodisk Solution

Innodisk's intergrated AES Solutions

Hardware-based 256 Bit AES Key	Data Destroy	TCG OPAL 2.0	IEEE 1667
AES Security provides a hardware-based mechanism for data encryption/ decryption	By altering the AES Key, data is destroyed in less than a second	Independent access to read/ write/ erase specific data areas (LBA ranges)	Compliant with TCG OPAL for IEEE 1667

iOpal



TCG Opal-Compliant Software

The TCG defined standard for self-encrypting drives (SED) emphasizes data security and ease of use. Innodisk's software conforms to thisstandard and can provide a simple and intuitive way to handle SED management. The software allows the user to easily define different ranges for different users – allowing for a system where data is shared on a strictly need-to-know basis

Innodisk Corporation

5F., NO. 237, Sec. 1, Datong Rd., Xizhi Dist., New Tapei City, 221, Taiwan
Tel : +886-2-7703-3000
Fax : +886-2-7703-3555
E-Mail : sales@innodisk.com
Website : www.innodisk.com

innodisk