Benefits of Self-Encrypting Drives (SEDs)

Encryption, Authentication, and Sanitization of SSDs

Introduction

With the rise in worldwide compliance to more stringent data protection laws and regulations, businesses are grasping the importance of properly securing their data to avoid high penalties and cost of data loss.

As solid state drives (SSDs) become more popular for storing sensitive data, there is a growing need for strong data encryption and sanitization to mitigate this risk. In addition, SSDs require different methods of sanitization compared to traditional hard disk drives (HDDs) due to their inherent design differences.

Self-Encrypting Drives (SEDs) help resolve this problem. These types of storage devices automatically encrypt data without any user interaction and can provide an effective method of data erasure. In this whitepaper, we will refer to SSD-type SEDs and look into the three key components of SEDs: encryption, authentication, and sanitization.

AES Encryption

In 1997, NIST (National Institute of Standards and Technology) issued a call for proposals to establish a new specification for encryption of electronic data called AES (Advanced Encryption Standard). Among five finalists, the winning candidate based on several security, performance, and implementation criteria was Rijndael, an algorithm designed by two Belgian cryptologists, Vincent Rijmen and Joan Daemen.

The symmetric algorithm uses the same key for both encrypting and decrypting data. NIST selected three different key lengths: 128 (AES-128), 192 (AES-192), and 256 bits (AES-256). All Virtium SEDs use AES-256 encryption.

Table 1 – Final score of AES algorithm finalists

	Rijndael	Serpent	Twofish	MARS	RC6
General security	2	3	3	3	2
Implementation difficulty	3	3	2	1	1
Software performance	3	1	1	2	2
Smart card performance	3	3	2	1	1
Hardware performance	3	3	2	1	2
Design features	2	1	3	2	1
Total	**16**	**14**	**13**	**10**	**9**

Today, AES is the de facto security standard for the U.S. government. No method exists today to break the AES key in a reasonable amount of time. In doing so, everything known to be secure today in government, medical, and financial sectors would be at a huge risk.

Experts have calculated it would take 1 billion billion years to crack a 128-bit AES key using a brute force attack with a 10.51-petaflop supercomputer [1]. Not only is that longer than the age of the universe, but there would not even be enough energy to power such computations. This really puts into perspective how impractical it would be to break the key. Bumping up the key size to 256-bits exponentially drives out the figure to an even more impossible number of combinations and time to crack.

Table 2 - Key combinations and time to crack cryptographic key versus key size

Key size	Possible combinations	Time to crack*
56-bit (DES)	7.2×10^{16}	399 seconds
128-bit (AES)	3.4×10^{38}	1.02×10^{18} years
192-bit (AES)	6.2×10^{57}	1.872×10^{37} years
256-bit (AES)	1.1×10^{77}	3.31×10^{56} years

*Using brute force attack with a 10.51-petaflop supercomputer.

Hardware-Based Encryption

SEDs include dedicated AES encryption engines that do not require software to run on the host. The randomized AES encryption keys are generated at product initialization using the controller's true random number generator (TRNG) and encrypted in the SSD. This could also be implemented by a Trusted Platform Module (TPM) chip.

TPM is a standard defined by the Trusted Computing Group (TCG) as a hardware root of trust for cryptoprocessors, which includes encryption key generation as well as tamper-resistant key storage. Unlike software encryption, all bits are encrypted automatically without any user management. This provides an additional layer of security as the encryption key never leaves the drive and is never exposed to intrusion.

Furthermore, encryption key management is not required. Another advantage of hardware-based encryption is that it cannot be corrupted like software running under an operating system where it is vulnerable to viruses and other attacks.

It is important to keep in mind that SEDs are not meant to secure data-in-flight or intended to be a replacement for firewalls or virus protection software. While self-encryption provides data-at-rest protection in the event of a lost or stolen computer, it does not protect you from malware or ransomware on a system that has already been authenticated and logged in.

Authentication

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access to data.

On an SED, authentication is performed by a protected pre-boot OS on the drive itself. With pre-boot authentication (PBA), there is no way for a thief to start breaking into the contents of the drive. The PBA can often support multiple factor authentication such as biometrics, smart cards, or remote passwords.

Like the TPM standard, the TCG has defined a set of specifications called the Opal SSC (Security Subsystem Class) to standardize the security features of SEDs. Two other subsets under Opal are Opalite and Pyrite, a non-encrypting version of Opalite. These derivatives of Opal were designed for equivalency to the ATA Security feature set. Additional information on these specifications for SEDs can be found at trustedcomputinggroup.org.

Depending on the configuration, Virtium StorFly SEDs can support either TCG Opal 2.0 or ATA Security based authentication. The host system and its BIOS will determine which authentication method is used.

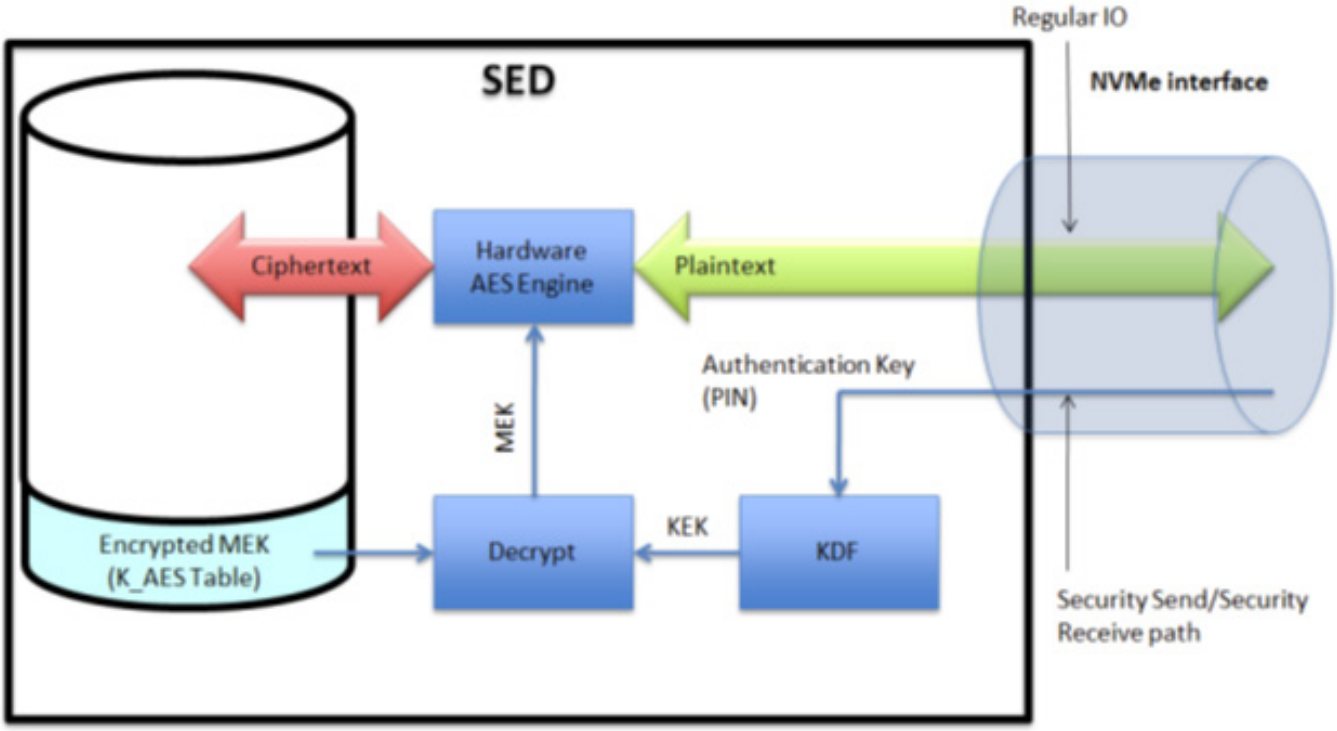

Figure 1 - SED block diagram

Sanitization

Various methods of sanitization are available for organizations based on the level of data protection required. NIST defines three different categories of sanitization for media: Clear, Purge, and Destroy.

> **Clear** - A method of sanitization by applying logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same interface available to the user; typically applied through the standard read and write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
>
> **Purge** - A method of sanitization by applying physical or logical techniques that renders Target Data recovery infeasible using state of the art laboratory techniques.
>
> **Destroy** - A method of sanitization that renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data. [6]

Permanently erasing data is a major concern for security-conscious customers who may follow one of several different military sanitization methods.

Table 3 - Various military sanitization methods

Method	Procedure
DoD NISPOM 5220.22-M	Erase, overwrite with a single character, and then erase again.
NSA/CSS Manual 130-2	Erase, overwrite with pseudo-random pattern twice, and then erase and overwrite with known pattern.
NSA/CSS Manual 9-12	Erase and overwrite with random data.
Army AR 380-19	Erase and overwrite with random data, erase and overwrite with specified character, and then erase and overwrite with its complement.
Navy NAVSO P-5239-26	Erase and overwrite with specified character, erase and overwrite with its complement, and then erase and overwrite with random data.
Air Force AFSSI-5020	Erase and overwrite with 00h, erase and overwrite with FFh, and then erase and overwrite with random data.
RCC-TG IRIG 106-07, Ch. 10	Erase and overwrite with 55h, erase and overwrite with AAh, and then erase and overwrite with ASCII string “Secure Erase”.

However, these methods were specifically written for traditional magnetic HDDs where residual charge would remain after erasing data. They often require overwriting three or more times over to assure the residual data cannot be retrieved. Depending on the capacity of the drive, the overwriting of data can often take hours or even days to complete.

Applying these sanitization methods to SSDs have been proven inefficient at securely erasing data. In addition, these methods would drastically reduce an SSD’s usable life. This is a result of the many fundamental differences between the way HDDs and SSDs store and manage data.

Experiments by professors and PhD students at the Center for Magnetic Recording and Research at the University of California in San Diego have shown that traditional single-file overwrite sanitization protocols failed when applied to SSDs. Between 4% and 75% of overwritten file contents were recovered using these government defined protocols [5]. To understand how this is possible, one must have a general understanding of data management between the flash translation layer (FTL) and the NAND flash.

The FTL manages the mapping between logical block addresses (LBAs) used by a host and physical block addresses in the flash. In NAND flash, data is accessed in relatively large chunks; read and written by page and erased by blocks. Since NAND flash is limited to a finite number of program/erase cycles, algorithms such as wear-leveling exist in the FTL to increase the life of a drive by attempting to evenly distribute writes across the flash. Algorithms such as wear-leveling that exist only in SSDs can create multiple copies of a single file leaving digital remnants across the drive.

How does one ensure data is unrecoverable on an SSD? In the following sections, we will explore the sanitization methods supported by Virtium StorFly SEDs.

ATA Security Erase

Virtium SEDs fully support the ATA Security feature set, which satisfies NIST Special Publication 800-88 Revision 1 requirements for the clear category of sanitization for SSDs.

Supported by both SED and non-SED drives, the ATA Security command set specifies a SECURITY ERASE UNIT command that erases all accessible user data by writing all binary 0's or 1's. There is also an ENHANCED ERASE mode that erases all reallocated user data and writes a vendor specific data pattern. Although all data in the user-accessible space is completely erased, some data such as the NAND block mapping tables may still physically reside on the SSD.

Support for built-in ATA security commands may also vary among manufacturers, so it is advised to check how they implement their secure erase.

Table 4 - ATA Security Erase mode characteristics

ERASE MODE bit	Erase Mode	Reallocated user data erased [a]	Data pattern [b]	User data erased [b]
0	Normal	No	binary 0's or binary 1's	0.. native max address
1	Enhanced [c]	Yes	vendor specific	

[a] User data sectors that were previously written and are no longer in use due to reallocation are written by the SECURITY ERASE UNIT command.
[b] The SECURITY ERASE UNIT command shall write the specified data pattern to the specified LBA range.
[c] The ENHANCED SECURITY ERASE SUPPORTED bit (see A.11.8.3.3) indicates whether the Enhanced Erase mode is supported.

Crypto Erase and Secure Erase

Virtium's crypto plus secure erase feature satisfies NIST Special Publication 800-88 Revision 1 requirements for the purge category of sanitization for SSDs.

The nature of self-encryption makes it relatively easy and reliable to sanitize or erase an SSD. For Virtium StorFly SEDs, a crypto erase plus secure erase can be implemented to fully restore the SSD to a fresh-out-of-box state.

When executing a crypto erase, the host can scramble the media encryption key (MEK) via the built-in random number generator or specify a user-generated MEK. This renders the data unreadable almost instantly (~300 us) at very low power (~20 mW). Nothing can be recovered from the encrypted data as it becomes meaningless and virtually erased without the key to decrypt it. The same command also provides an option to follow-up with a secure erase, which further sanitizes all user and reallocated data blocks including the spare area in less than a minute.

Table 5 - Virtium SED typical erase times and power consumption

Capacity	Flash Type	Crypto Erase		Secure Erase	
		Max Time	Max Power	Max Time	Max Power
480 GB	MLC	300 us	0.02 W	17.17 s	0.73 W
960 GB	MLC	300 us	0.02 W	34.55 s	0.55 W
256 GB	SLC	300 us	0.02 W	15.75 s	1.09 W

Cryptographic erasure gives the benefit of erasing data faster than a secure erase while sustaining the overall life of the drive for further use and is the most efficient way to permanently erase data on the SSD.

Additionally, Virtium's Secure Erase is persistent over power cycles as the drive cannot be accessed until the erase operation is complete. In other words, if the SED loses power during the erase, it will automatically resume erasing upon subsequent power cycles.

Conclusion

The demand for more secure IoT solutions will give SEDs a strong foothold in the industrial SSD market. Due to the complications of the SSD's FTL function, data encryption with cryptographic disk erasure is the best method of sanitization for SSDs. SEDs offer these features and provide the best benefits in terms of performance, security, and cost.

By carrying out on-the-fly encryption within the SED hardware, users can benefit from better performance than software-based encryption. There is no burden on the host system and no extra host encryption elements required. Furthermore, hardware-based security can more effectively restrict access from the outside. An operating system provides open access to applications and thus exposes these access points to unauthorized use.

Using proven AES-256 encryption, SED customers have peace of mind knowing their data at rest is secure and can be instantly sanitized via a crypto erase. The MEK is non-retrievable and non-changeable without the complete loss of the data encrypted on the SSD. This eliminates the need for time-consuming data overwriting processes of non-encrypted drives and also provides an effective sanitization process for SSDs.

Virtium offers a full line of SEDs that support all SATA formats including Slim SATA, mSATA, and CFast, which are not typically supported by competitive solutions. Virtium is also one of the few that provides three different endurance classes of SEDs including PE (SLC), XE (iMLC), and CE (MLC). In addition, Virtium SEDs support industrial operating temperatures to extend security to designs in extreme operating conditions.

References

[1] Arora, Mohit. “How Secure Is AES against Brute Force Attacks? | EE Times.” EETimes. July 5, 2012. Accessed November 14, 2016. http://www.eetimes.com/document.asp?doc_id=1279619.

[2] ATA/ATAPI Command Set - 3 (ACS-3) [INCITS T13/2161-D]. Available from http://www.t13.org.

[3] German Society of Telemetering, Proceedings of the European Telemetry Conference, p.18, May 24-27, 2004, Garmisch – Partenkirchen, Germany.

[4] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, and Edward Roback, Report on the Development of the Advanced Encryption Standard (AES), available at http://www.nist.gov/aes.

[5] Michael Wei , Laura M. Grupp , Frederick E. Spada , Steven Swanson, Reliably erasing data from flash-based solid state drives, Proceedings of the 9th USENIX conference on File and storage technologies, p.8-8, February 15-17, 2011, San Jose, California.

[6] National Institute of Standards and Technology, NIST Special Publication 800-88 Revision 1: Guidelines for Media Sanitization, available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

[7] Trusted Computing Group and NVM Express Joint White Paper: TCG Storage, Opal, and NVMe, available at http://www.trustedcomputinggroup.org/wp-content/uploads/TCGandNVMe_Joint_White_Paper-TCG_Storage_Opal_and_NVMe_FINAL.pdf.

Virtium manufactures memory and storage solutions for the world’s top industrial embedded OEMs. For two decades we have designed, built and supported our products in the USA - fortified by a network of global locations. Our world-class technology and unsurpassed support provide a superior customer experience that continuously results in better industrial embedded products for our increasingly interconnected world.

Virtium
Solid State Storage and Memory

30052 Tomas | Rancho Santa Margarita, CA 92688
Phone: 949-888-2444 | Fax: 949-888-2445
www.virtium.com