A MICRON
TECHNICAL
MARKETING
BRIEF

Data Sanitation: Securely Erasing Micron® SATA SSDs

Jon Tanguy, Senior Technical Marketing Engineer

Introduction

In an era where protecting sensitive information is so important, protecting data on storage devices is critical at every step in the life cycle of these devices, including at end-of-life and when devices are redeployed to other purposes. Because of this, the ability to ensure that user data is securely erased from a data storage device is critical. Micron's SSDs provide very effective and efficient means to do so. In fact, SSDs can provide tremendous advantages over HDDs with regard to the speed and security of the full-drive erase functions.

This brief describes Micron's methodologies for completely erasing, or "sanitizing" SSDs within the Serial Advanced Technology Attachment (SATA) and Trusted Computing Group (TCG) protocols.

Erasing SSDs vs. HDDs

Historically, the accepted method of permanently removing data from magnetic media, as in HDDs, was to overwrite the data with a pre-determined data pattern, like "all 0's" or a random data pattern. To truly make the data unrecoverable, this could take several passes and many hours of operation time. This can be very inefficient and expensive.

However, for the NAND flash memory in most SSDs, there is no overwrite command available. NAND flash is unique in that when data is stored in a particular storage element within the SSD, the data must first undergo a separate ERASE command before a new WRITE command can be performed at that physical location.

Because of this inherent characteristic of NAND flash media, when the host computer instructs an SSD to overwrite data, the drive will have to first issue the ERASE command to each of the targeted storage elements. Only after this erase step is complete will the drive proceed to write the desired data pattern to the erased elements. The inefficiency of this is obvious. Elements of the NAND flash which have already been erased once are now filled with data.

Even worse, when the host computer needs to write new user data, the drive must first ERASE the data pattern which was written, AGAIN! Now, inefficiency compounds because of the attempt to treat an SSD like an HDD.

Fortunately, Micron's SSDs provide a fast and efficient means of eliminating all data from the drive, without redundantly erasing, filling and re-erasing the drive.

What is SANITIZE?

The word "sanitize" has obvious connotations with regard to cleaning up unwanted or unneeded data. However, "sanitize" is a term of art where data security is concerned, describing a process by which data is removed from a storage device to a point that exceeds the ability to reconstruct the data by known forensic means. When used in all caps, as in SANITIZE, it refers to the command specified by the ATA Command Set (ACS) which sets in motion the sanitizing of data on an SSD.

Sanitize is most inclusively described in government specifications. In particular, the National Institute of Standards and Technology (NIST, USA) describes this function in a document called Special Publication 800-88, "Guidelines for Media Sanitation," currently at Revision 1 published in 2014, and available at SP800-88r1. The document is intended to "assist organizations and system owners in making practical sanitizing decisions based on the categorization of confidentiality of their information."

SP800-88r1 includes new descriptions of data sanitizing

processes now in practice due to the new nature of data storage on SSD, in addition to more traditional techniques that continue to be used for hard drives and magnetic media. It acknowledges that hard drive methods for sanitizing are inappropriate for SSD, and may often be counterproductive.

In the latest ATA specification, the sanitize command is called out in two ways: SANITIZE BLOCK ERASE and SANITIZE CRYPTO SCRAMBLE, which are separate methods described next. The ATA specification also describes SANITIZE OVERWRITE ERASE, which is applicable only to HDDs and this is not covered in this paper.

Legacy Command: Security Erase

Another method to erase an entire SSD is known as Security Erase, which comes from an older portion of the ATA spec. Some of Micron's older SSDs that support only the SATA 3.0 specification do not support SANITIZE, so Security Erase is the preferred method. On newer Micron SSDs that support SATA 3.1 and later, the SSD supports both Security Erase and Sanitize commands. At the media level, Sanitize and Security Erase perform the same operation. Only the interface commands are different.

In this technical brief, we will continue to use the term "sanitize," with the understanding that Sanitize Block Erase and Security Erase perform the same operation.

To execute a Security Erase, Micron recommends implementing the SECURITY ERASE PREPARE followed by SECURITY ERASE UNIT commands as described in the ATA Command Set published interface standard, available at t13.org. The command ENHANCED SECURITY ERASE UNIT, as implemented on Micron SSDs, enables Cryptographic Erase, as described later in this paper.

Command Execution

Whether the sanitize operation is executed using SANITIZE BLOCK ERASE or the legacy SECURITY ERASE UNIT command, the drive-level operation is the same. Micron's proprietary firmware instructs the SSD controller to send a BLOCK ERASE command to all NAND devices on the drive—including the NAND space reserved for overprovisioning and retired blocks, areas which are inaccessible by the host computer or the user.

When the sanitize operation is initiated by the host computer, the SSD controller simultaneously erases the maximum number of NAND FLASH elements allowed under the SSD's maximum-rated power consumption specification. Because of this parallelism, the SANITIZE BLOCK ERASE or the SECURITY ERASE UNIT command can be completed within one minute on the majority of Micron's SSDs; this is a quantum leap beyond a similar operation in HDDs, which can take hours to securely and completely eliminate user data.

What Data Is Not Erased?

The entire user space and over-provision space are completely and irretrievably erased. Every block in the user space is ready to accept new host-written data, moving the drive to its highest performance state, FOB (fresh-out-of-box).

However, some data must be left in place for normal drive operation. This includes the following required data: SSD firmware copies that reside in the NAND, all SMART data, and retired NAND block mapping tables.

How Secure Is SANITIZE?

Some engineers and scientists have detected stray electrons in NAND cells after an erase, and Micron acknowledges this possibility. However, because a block erase operation raises every NAND cell to an identical erase voltage regardless of the cell's previous state, Micron contends that it is impossible to determine the previous state of the cell based on leftover, stray signals.

Additionally, the SANITIZE operation cannot be interrupted like a full disk write can be. Cutting off power may interrupt a SANITIZE command, but the erase immediately restarts when power is restored. The SSD cannot communicate with a host computer until the SANITIZE command has successfully completed.

During the SANITIZE operation, every effort is also made to erase data that may exist in retired NAND blocks. In fact, the most common reason for retiring a NAND block is the block could not be successfully erased. However, Micron engineers have found that when an erase fails, more than 90% of the bits in the failed block are successfully erased. The unerased bits are almost never consecutive, so they do not yield coherent data during device-level detection. The bad blocks are not accessible via the SATA interface and require the ability to detect

bits from a detached NAND flash component. Therefore, the risk of reconstructing usable data from NAND blocks that are not fully erased is exceedingly low—even when device-level detection is attempted.

Validating SANITIZE

Micron understands some customers manage data that is so sensitive, the customer cannot simply take our word that data is permanently, securely sanitized. For some of our products, we have worked with third-party security firms to confirm that after SANITIZE is executed per specification, all data is confirmed and certified to be irretrievable. We keep certificates on file for some products, and if certificates do not exist, we can ask for further testing and certification. Contact your Micron Sales representative for details.

SAS and PCIe/NVMe SSDs

Although this paper does not discuss this in detail, both SAS and PCIe/NVMe protocols have commands which initiate the same operation as the SATA SANITIZE command. In SAS, the command is FORMAT UNIT, while in PCIe/NVMe the command is FORMAT NVM.

Additional Security Through Encryption

Micron offers a family of self-encrypting drives (SEDs) that use a 256-bit advanced encryption standard (AES) engine to provide state-of-the-art data protection.

In addition to providing a strong, secure method of protecting user data under pass code control, SEDs also provide a very efficient means of rendering all of the data on the drive unreadable.

For the purpose of permanently eliminating data, Micron's SATA SEDs support the SATA standard SANITIZE CRYPTO SCRAMBLE command, which deletes and replaces the encryption key. After the encryption key has been replaced, data bits remain stored in place but are completely unintelligible. One major advantage of this cryptographic erase operation is that it can be completed in less than two seconds for most drives.

Today, it is commonly believed that a 256-bit encryption key is all but completely unbreakable. However, it is conceivable that one day there will be sufficient supercomputing power to break such a cipher in a reasonable amount of time. Therefore, when time allows and to ensure all user data is completely erased and forever irretrievable, Micron recommends following the SANITIZE CRYPTO SCRAMBLE command with a SANITIZE BLOCK ERASE command. This combination of commands will also return the drive to its fresh-out-of-box (FOB) performance state while a CRYPTO SCRAMBLE command alone will not re-initialize the drive to this "like new" state.

Micron's SEDs comply with TCG Opal specifications

Figure 1: Micron SED with 32-Character PSID and Corresponding 2D Bar Code

for client computing storage devices. Additional SED information is available at micron.com and trustedcomputinggroup.org.

PSID Revert Functionality

While SEDs provide tremendous aid in protecting data from unauthorized viewing, there are risks, including losing an authentication key or password. IT management applications provide several ways to redundantly backup passwords, authentication keys and other access codes. Taking advantage of these features is strongly recommended. However, it is still possible to lose these passwords. In this unfortunate circumstance, even the storage device manufacturer, like Micron, cannot decrypt and recover the user data. Therefore, important data could be permanently lost.

Not only can the data be lost, but an encryption locked drive is blocked from normal re-format operations. So,

the user data is lost AND the drive itself is unusable.

To help resolve part of this problem, Micron's family of SEDs support physical security identification (PSID) revert functionality. The PSID is a string of 32 ASCII characters printed on the serial number label of each SSD. The PSID is unique to each drive.

Although PSID revert functionality cannot recover user data when a pass code is lost, the PSID REVERT function can be used to unlock the SED; initiate a SANITIZE CRYPTO SCRAMBLE command; and return the drive to normal functionality, enabling its reuse.

Note that older Micron SSDs which supported the Opal 1.0 specification do not include PSID Revert functionality.

Micron Storage Executive Software

Micron has now released a free software utility called Micron Storage Executive to manage many Micron SSD features. With an easy-to-use Windows® or Linux® GUI and a command line interface (CLI) option, it includes functionality to execute both SANITIZE BLOCK ERASE and PSID REVERT commands. See Micron's Storage Executive Software to download the software and documentation locations.

Micron's SEDs also provide cryptographic erase functionality that can be used to make data on the SSD unreadable by almost any currently known decryption technology. The SANITIZE BLOCK ERASE operation can then be used to eliminate data and return the SSD to its FOB performance state.

Conclusion

Writing or overwriting data to the full disk pack is the accepted practice of securely eliminating data from an HDD. However, in the case of NAND flash-based SSDs, overwriting to eliminate data is redundant, unnecessary and potentially unsecure. NAND flash is properly erased using the BLOCK ERASE function.

Micron strongly recommends that the SANITIZE BLOCK ERASE command be used instead of a data overwrite algorithm. For older Micron SSDs, the SECURITY ERASE command is recommended. Either of these commands ensures that the SSD properly executes the BLOCK ERASE command across the entire user space, overprovisioned space, and spare block and bad block locations.

Micron's SEDs also provide cryptographic erase functionality that can be used to make data on the SSD unreadable by almost any currently known decryption technology. The SANITIZE BLOCK ERASE operation can then be used to physically eliminate data and return the SSD to its FOB performance state.

micron.com