A MICRON
TECHNICAL
MARKETING
BRIEF

# Securely Erasing Micron® SATA SSDs

*Jon Tanguy, Senior Technical Marketing Engineer*

## Introduction

In an era where protecting sensitive information is so important, the ability to ensure that user data is securely erased from a data storage device is critical. Micron's solid state drives (SSDs) provide very effective and efficient means to do so. In fact, SSDs can provide tremendous advantages over hard disk drives (HDDs) with regard to the speed and security of the full-drive erase functions. This brief describes Micron's methodologies for erasing SSDs within the Serial Advanced Technology Attachment (SATA) and Trusted Computing Group (TCG) protocols.

## Erasing SSDs vs. HDDs

Unlike with magnetic media (e.g., HDDs), data previously stored on NAND Flash media cannot be directly overwritten. Rather, in order to prepare a NAND Flash memory element to receive a new PROGRAM command (i.e., a new write), a separate ERASE operation must be performed. The act of writing a specified data pattern, such as "all 0s," to every logical address on the SSD requires the entire user space to be erased, element-by-element, which prepares that user space to receive the new data pattern. Only then can the new data pattern be written. This second step is redundant as well as time consuming, considering that the prior erase step has already eliminated the previous data.

Even worse, writing a predetermined data pattern to a NAND Flash-based SSD does not result in an empty drive. Instead, it results in a full drive with a data pattern that must be erased before new user data can be written. Depending on the physical configuration of the SSD in question, this may leave the unit in a suboptimal performance state until the data pattern is properly erased. See **Micron's Best Practices for SSD Performance Measurement technical brief** for further information on these performance states.

## Securely Erasing Data

To securely erase all user data from an SSD and restore the drive to a fresh-out-of-box (FOB) performance state, Micron recommends implementing the SECURITY ERASE PREPARE and SECURITY ERASE UNIT commands (described in the ATA Command Set published interface standard, available at **t13.org**).

When the SECURITY ERASE UNIT command is issued, 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, which is not accessible by the host computer or the user. After the erase is initiated by the host computer, the controller simultaneously erases the maximum number of NAND Flash devices allowed by the SSD's maximum-rated power consumption specification. Because of this parallelism, the SECURITY ERASE UNIT command can be completed within one minute on the majority of Micron's SSDs; this is a quantum leap ahead of a similar operation in HDDs, which can take hours to securely eliminate user data.

## What Data Is Not Erased?

All data in the user space is completely and irretrievably erased, and every block in the user space is ready to accept new host-written data, which moves the drive to its highest performance state (FOB). However, some data must be left in place; this includes data required for normal drive operation: SSD firmware copies that reside in the NAND, all SMART data, and retired NAND block mapping tables.

## How Secure Is a Secure Erase?

Some engineers and scientists have detected stray electrons in NAND cells after an erase. Micron acknowledges this possibility. However, because a block erase raises every NAND cell to an identical erase voltage regardless of the cell's previous state, Micron contends



Micron®

that it is impossible to determine the previous state of the cell based on leftover, stray signals.

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

During the SECURITY ERASE UNIT operation, every effort is made to also erase data that may exist in retired NAND blocks. The most common reason for retiring a NAND block is because 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 erased. These 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. The risk of reconstructing usable data from NAND blocks that are not fully erased is exceedingly low—even when device-level detection is attempted.

## Sanitize Functionality

Historically, media sanitization has required that magnetic media, like HDDs, be erased using signals specified by industry and government experts to ensure that no stray magnetic signals remain on the media. ATA sanitize functionality has been implemented in SSDs with the same intent—but with features specific to NAND Flash devices.

Several of Micron's SSDs include sanitize functionality, which also provides effective means to completely erase the SSDs. Like the ATA SECURITY ERASE commands, the SANITIZE BLOCK ERASE command can be used to trigger the SSD controller to send BLOCK ERASE commands to the entire SSD user space—including any over-provisioned space—effectively eliminating all user data. Refer to the specific Micron data sheet to determine whether an SSD supports sanitize functionality. Micron's SSDs do not support the SANITIZE OVERWRITE ERASE command, which is typically used for HDDs.

## 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. An SED, in conjunction with an encryption key management software package from an independent software vendor (ISV), provides another efficient way to keep data secure. For the purpose of permanently eliminating data, Micron's SEDs support the CRYPTOGRAPHIC ERASE command, which deletes and replaces the encryption key. After the encryption key has been replaced, data bits remain on the NAND array but are completely unintelligible. One major advantage of cryptographic erase is that the operation can be completed in less than two seconds.

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. To ensure that all user data is completely erased and forever irretrievable, Micron recommends following the CRYPTOGRAPHIC ERASE command with a SECURITY ERASE UNIT command. This combination of commands will return the drive to its FOB performance state while a CRYPTOGRAPHIC ERASE command alone will not complete this re-initialization.

Micron's SEDs comply with TCG Opal specifications 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. Most encryption management software packages—from BitLocker to Wave Systems to Winmagic—provide redundant backup capabilities for passwords, authentication keys, and other access codes. However, it is still possible to lose these access codes, as well as the user data secured behind them. In this unfortunate circumstance, even the storage device manufacturer, like Micron, cannot decrypt and recover the user data. The 256-bit encryption is all but unbreakable, which is compounded by the fact that a locked SED with a lost

access code cannot be used at all; it is equivalent to nothing more than a brick—and for larger solid state SEDs, that is a very expensive brick.

To help resolve part of this problem, Micron's M500 family of SEDs—including the M500, M510, and M550 drives—support physical security identification (PSID) code revert functionality (identified by a string of 32 ASCII characters printed on the top cover of each M500-series SSD). Although PSID revert functionality cannot recover user data when an access code is lost, the PSID REVERT function can be used to unlock the SED, initiate a CRYPTOGRAPHIC ERASE command, and return the drive to normal functionality.

## 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 is redundant, unnecessary, and a potentially insecure method of eliminating data. NAND Flash is properly erased using the BLOCK ERASE function.

Micron strongly recommends that ATA SECURITY ERASE commands or the SANITIZE BLOCK ERASE command (for capable SSDs) be used instead of a data overwrite algorithm. This 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 SECURITY ERASE operation can then be used to eliminate data and return the SSD to its FOB performance state.