



SECURE ERASE in NAND-Based Solid State Drives (SSDs)

Jon Tanguy
Applications Engineer
Micron Technology, Inc.

SECURE ERASE in NAND-Based SSDs

- ATA specification requires that SECURE ERASE deletes all user, partition, and OS data irretrievably
- Some methods for SECURE ERASE were inherited from HDD industry
- More correctly, SSD should use erase features native to NAND

- Micron SECURE ERASE methodology:
 - SECURE ERASE command from host initiates NAND-level BLOCK ERASE command to all NAND devices
 - Execute with as much parallelism as possible within power supply limit
 - Erase all user accessible areas, including user data, OS, and partition; areas used for over-provisioning are erased, as is the FTL page table (which is subsequently rebuilt)

- C400: SECURE ERASE can be completed in 60 seconds for a 512GB drive

- What is not erased?
 - Firmware copies
 - SMART data
 - Bad block tables

- How secure is SECURE ERASE?
 - Very!
 - While there may be stray electrons remaining in cell after erase, it is statistically impossible to tell the difference between a previous 1 or 0
 - SECURE ERASE may be interrupted by POWER cycle, but will restart on next power-up
 - Drive cannot return 50 status until SECURE ERASE successfully completes

Some concerns remain

- Bad blocks due to erase failure:
 - Drive makes every effort to erase data even in retired blocks
 - If block returns erase fail status, erase cannot be guaranteed
 - Typically, the erase fail effects several bits; observations show that >90% of bits in block are successfully erased
 - Bad blocks remain inaccessible through interface



SECURE ERASE in NAND-Based SSDs

Some concerns remain

- SECURE ERASE of individual files:
 - No standard method exists
 - Data pages cannot be erased until garbage collection arranges deleted areas in contiguous blocks

SECURE ERASE in NAND-Based SSDs

- Other security steps can be taken
 - Self-encrypted drive (SED); AES hardware encryption
 - If encryption key security is maintained, reading back NAND component will yield nonsensical data
 - ATA CRYPTO ERASE command
 - Delete (and erase) the encryption key
 - SECURE ERASE for good measure
 - Non-interface ERASE commands
 - Destructive erase



SECURE ERASE in NAND-Based SSDs

- Questions?

Revisit the Micron FMS presentations at www.micron.com/fms



Jon Tanguy

- Applications Engineering, NAND Solutions Group, SSD Product Marketing, Micron Technology, Inc.
- Facilitates new product integration and qualifications for notebook and desktop applications
- Data storage experience in HDD and solid state industries in manufacturing, new product and process development, quality/reliability, and applications
- Earned a BS degree in Electrical and Computer Engineering from the University of Colorado at Boulder

Revisit the Micron FMS presentations at www.micron.com/fms

©2011 Micron Technology, Inc. All rights reserved. Products are warranted only to meet Micron's production data sheet specifications. Information, products and/or specifications are subject to change without notice. All information is provided on an "AS IS" basis without warranties of any kind. Dates are estimates only. Drawings not to scale. Micron and the Micron logo are trademarks of Micron Technology, Inc. All other trademarks are the property of their respective owners.