Verifying SSD Sanitization

Paul Suhler, Micron

Mark Carlson, Toshiba Memory

(Absent co-author: John Geldman, Toshiba Memory)

NVM Express Developers Day – May 1, 2018

Why Sanitize SSDs?

- Returned, repurposed, or discarded storage devices probably contain confidential or personal data
  - Just letting these devices go free leads to newspaper headlines
  - A Sanitize operation deletes all user data from a storage device
- NVMe™, ATA, and SCSI Sanitize commands were designed to erase all accessible storage, both host and firmware accessible, no matter how long it takes
- So when your SSD is ready to move on, you want Sanitize to keep your secrets

Sanitize in NVMe™ (part 1)

- A sanitize operation is requested by a sanitize command
- Sanitize operations affect all allocable media in the entire NVM subsystem
- There are three sanitize operation ‘flavors’:

  Crypto Erase; Overwrite; Block Erase

- When a sanitize operation begins the device will return errors on read/write commands until the operation is successful

  The operation automatically continues to complete even if the operation is interrupted by a power cycle (unique behavior to sanitize)

Sanitize in NVMe™ (Part 2)

- A sanitize command may tell the device to:

  keep the device blocked if the sanitize operation fails; or

  to allow unblocking the device if the sanitize operation fails

- Sanitize operation status is communicated through a log page: Sanitize Status Log page
- The Format NVM command overlaps with sanitize functionality but misses many of these characteristics (that is another talk)

Why Is This Complicated?

- SSDs are funky writers
  - File systems both write data into random addresses as needed and overwrite as needed
  - But NAND doesn't work that way – it needs to fill physical circuits serially
  - So SSDs have:

    Firmware that maps logical addresses known to the host to physical addresses known to the firmware

    Extra hidden storage available to the firmware to make this magically work

        This magic is every SSD vendor's secret sauce, every SSD vendor's IP

Naïve Customer Says:

“Drive, prove that my data is sanitized”

This is the wrong question!

- What does sanitize do for you?
  - “A sanitize operation alters all user data in the NVM subsystem such that recovery of any previous user data from any cache, the non-volatile media, or any Controller Memory Buffer is not possible.”
  - Key points are that:
    - The promise is made over the interface
    - Sanitize affects all allocatable memory (more than what is accessible from the interface)
    - Some implementations of some sanitize methods leave the media unreadable, so only de-allocation patterns are available
    - Bad blocks that couldn’t be sanitized are removed from the allocatable pool
    - However, post sanitize checks can only check what is accessible from the interface

Can You Take the Drive at Its Word?

- Most of the time, yes
- But devices have been compromised (lessons from the past):
  - NSA toolkits included firmware hacks that resulted in devices reporting success without actually erasing data
- For Self Encrypted Devices (SED), not sharing keys increases security:
  - The security model of SED drives begins with the model that encryption keys have no path to escape device boundaries
  - What can’t be shared, can’t be leaked

Less-Naïve Customer

“Walk me through your sanitization firmware”

- Not much improvement
  - Doesn’t prove bugs are not present
  - Doesn’t prove a given drive wasn’t hacked
  - Exposes SSD vendor’s Intellectual Property
- What can be done?
  - Spot check with random LBA reads to ensure expected results
  - One time exhaustive LBA read (crawl) or sufficient random LBA reads for statistical process proof

Better: Third-Party Verification

- Test multiple instances of each vendor's drive
- Current private testing:
  - Ontrack
  - DriveSavers
- Possible future direction: NIST Sanitize Certification
  - See *Proposed Direction* slide below

Third-Party Testing Process

- Vendors submit multiple units with same firmware
- Test all drives:
  - Write known data across drive
  - Perform sanitization without deallocation
  - Examine addressable blocks through the interface to confirm the original data is not present
  - Deeper testing may include demounting and directly accessing NAND dies
    - Can be misleading (we'll discuss this on the next slide)
- Tester certifies that SSD/firmware combination meets standard

Testing Approaches

- Examine addressable blocks (per ISO/IEC 27040):
  - Full verification for process validation: Read all blocks (checking for anything but zeros is difficult to automate)
  - Representative sampling for ensuring a drive has been sanitized:
    - Divide LBA space into at least 1,000 sections, take two disjoint samples per section, each sample covering at least 5% of the section
    - Each new sampling run examines different samples from previous runs; samples are chosen pseudorandomly with a new seed
- Raw NAND content checking is hard to test without device vendor co-operation for:
  - NAND values that have been encoded for zero/one balancing
  - Identifying firmware blocks that aren't supposed to be changed
  - Identifying bad blocks that could not be modified and ensuring these bad blocks are not allocable

Possible Direction: Government Certification

- NIST could establish a new FIPS certification program for sanitization of SSDs
- Certification that drive complies with a FIPS would carry more weight than certification that drive meets a private company's standard.
- This program (like FIPS 140) would include both testing and design review but with a lower scope of evaluation
  - Standalone certification is preferred to encourage more participation, but this could be added to FIPS 140

Next Steps

- Discuss achievable scope limitations and testing schemes for NIST to establish an achievable certification program
  - Needs device vendors and labs to discuss feasibility and effectiveness
  - Discussions are underway with private testing companies and a NIST-certified lab

- Present interim status at FMS 2018

Thanks to …

Jon Tanguy (Micron) for his contributions

Mike Danielson (Micron) for the idea of a certification initiative

Related Documents

SP 800-88, *Guidelines for Media Sanitization*, Revision 1, December 2014

FIPS 140-2, *Security Requirements for Cryptographic Modules*, May, 25, 2001

ISO/IEC 27040, *Information technology — Security techniques — Storage security*, 2015-01-15


nvm
EXPRESS®
Architected for Performance