Securing Your SSD

"Ensuring you have the tools to protect your data"

Jon Tanguy, Sr. Technical Marketing Engineer

with Rob Strong, Sr. Engineer, SSD Security Architect

Micron Technology, Inc.

Start with Encryption

"Disk" Encryption is becoming ubiquitous

- Major SSD makers offer AES-256 hardware encryption
- Windows 10 security initiatives will make encryption easy and common through "eDrive."
    - Win8 and Win10 include hardware encryption management in BitLocker.
- Independent software vendors provide straightforward solutions, even at the single client level.

Media Sanitization

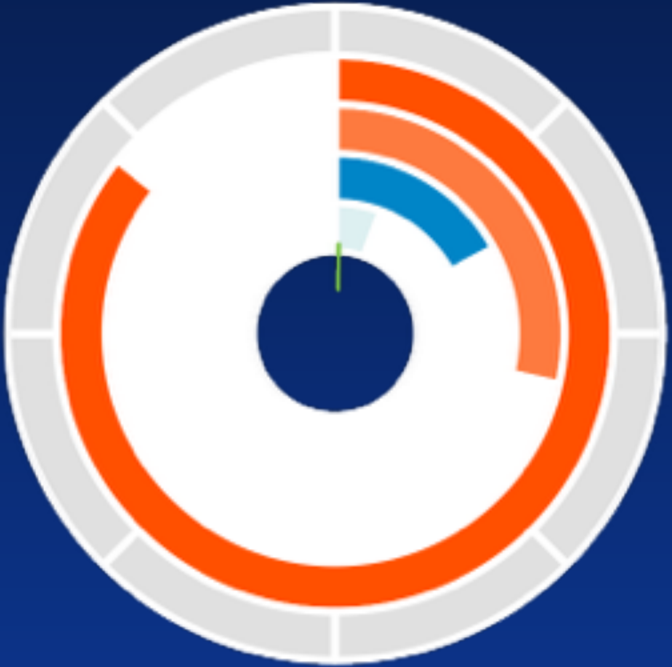
Fast, Easy and Inexpensive method for SSD repurpose/retirement

Look for SANITIZE commands for your SSD

- SANITIZE CRYPTO ERASE
  - Provides for rapid data destruction by deleting and generating a new encryption key
- SANITIZE BLOCK ERASE
  - All NAND blocks containing user data will be erased
- SANITIZE OVERWRITE is not supported for SSD (HDD command)
  - Overwrite adds unnecessary wear to NAND Flash, and may be ineffective.
- Many SSDs continue to support the ATA SECURITY ERASE UNIT command.

SANITIZE is now an accepted method per NIST SP800-88 Revision 1

How long does it take to "Sanitize" a 1TB Drive?



Time is Money!

Crypto Erase (media agnostic) : 1sec

SSD Sanitize Block Erase: 1min

SSD 1 Pass Overwrite : 40min ✗

SSD 3 Pass Overwrite : 120min ✗

HDD 1 Pass Overwrite : 200min

HDD 3 Pass Overwrite : 600min

✗ = *Please don't overwrite your SSD!*

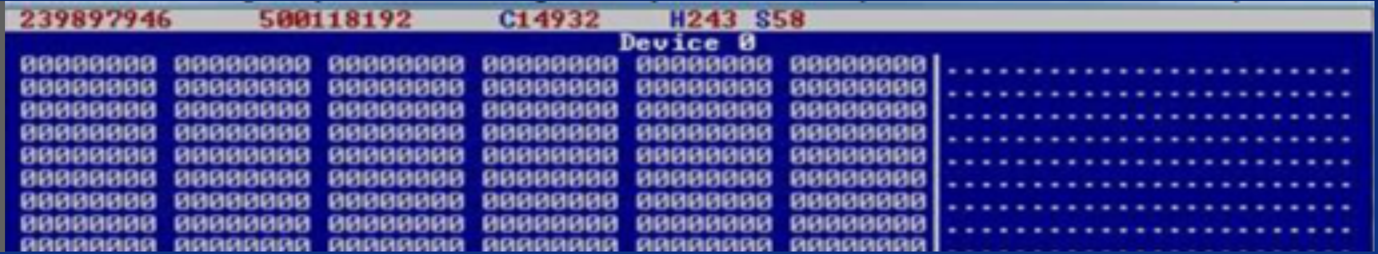
Third Party Validation of Sanitize

Providing Peace of Mind…

Academic reports cast doubt on the ability of solid state storage devices to be thoroughly erased, and some of that “FUD” remains…

- Many end customers want affirmation that SANITIZE functions as it should…
- “[Third-party certification] is intended to demonstrate the independent recognition of a well-known industry leader in erasure verification services for Micron’s data storage drives used in their system.”

Example of the 0x00 hex pattern found on every user-accessible sector of the SSD after Sanitization



```
239897946        5001118192        C14932     H243  S58
                                   Device 0
00000000 00000000 00000000 00000000 00000000 00000000 | ........................
00000000 00000000 00000000 00000000 00000000 00000000 | ........................
00000000 00000000 00000000 00000000 00000000 00000000 | ........................
00000000 00000000 00000000 00000000 00000000 00000000 | ........................
00000000 00000000 00000000 00000000 00000000 00000000 | ........................
00000000 00000000 00000000 00000000 00000000 00000000 | ........................
00000000 00000000 00000000 00000000 00000000 00000000 | ........................
00000000 00000000 00000000 00000000 00000000 00000000 | ........................
00000000 00000000 00000000 00000000 00000000 00000000 |
```

Next step: Can we delete, destroy and validate that individual files and folders are deleted?

- SNIA SSSI Data Recovery/Erase SIG is on the case.

Hardening the Target

Protecting SSD (and other endpoint) Firmware

Can SSD/HDD Firmware really be hacked?

- Turns out that the answer may very well be “yes.”
- Intruders could take advantage of the SATA 0x92 “DOWNLOAD MICROCODE” command to deliver a new, possibly undetectable, firmware image.
- The task is enormous. Requires in-depth knowledge of SSD architecture and firmware.

Hardening the Target

Protecting SSD (and other endpoint) Firmware

What should we do?

- First, sign the binaries.
  - Your Device Manufacturer should follow known protocols to protect signature server and infrastructure.
- Protect/Fuse JTAG, serial port, etc.; Or implement encryption
- FW Attestation with an immutable Core Root of Trust for Measurement at boot time.
- Cryptographically prevent firmware modification via physical access
- Continue to prohibit “backdoor” access.
- Institutionalize “Threat Modeling.” **Nothing is impossible**

Your Presenter

Jon Tanguy

Sr. Technical Marketing Engineer
Micron Technology, Inc.
Boise, ID USA
http://www.micron.com/products/solid-state-storage
@JTanguyFlash

Jon is a Sr. Technical Marketing Engineer in Micron's Storage Business Unit in Boise, Idaho. Jon facilitates new product integration and customer qualifications for notebook and desktop applications, as well as SSD in the data center. Jon is a creator of Micron's technical documentation, such as white papers and tech notes, and a blogger at Micron's Storage Blogs. Jon plays a key role in product planning and development, bringing the voice of the customer directly to the development team.

Jon has more than 20 years of experience in the data storage industry, working with both magnetic media and solid state technologies.

Jon earned his Bachelor of Science degree in Electrical and Computer Engineering from the University of Colorado at Boulder.