Erasure Verification of SSDs

What it is and should you care?

Robin England
Senior Research and Development Engineer

What is data erasure / sanitization?

A process by which all user data is irreversibly removed from the media. The process…

Must:

Prevent the subsequent recovery of data

Should:

Permit the re-use of the media

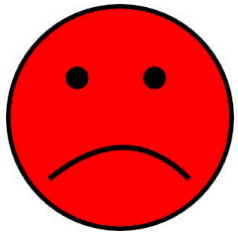
And most importantly must be...

Verifiable!

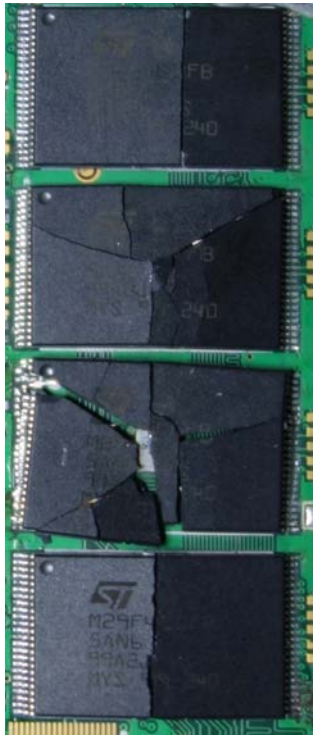
Why sanitize?

Data security breaches carry significant risks to both individuals and organizations…

- Identify theft
- Fraud, financial loss
- Regulatory compliance failure (penalties)
- Breach of Data Protection Act (legal)
- Loss of intellectual property
- Hacking of IT systems
- Damaged reputation



Alternatives?



Destroy?

- Expensive (loss of asset)
- Unpredictable results
- Often requires a 3rd party – trust?
- Results cannot be verified

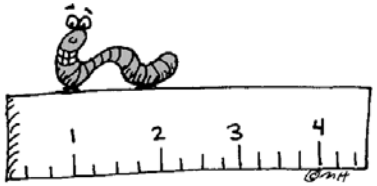
Encrypt?

80	33	31	64	63	48	32	36	3
90	F7	9B	DA	E4	10	02	00	0
A0	2B	CD	B0	43	2D	C5	58	9
B0	07	46	0B	1E	4B	C4	96	1
C0	73	AC	EB	FB	E3	44	98	F
D0	2F	CD	40	51	AF	7E	E1	B
E0	1E	34	F9	A3	95	FF	CD	6

- Even encrypted data left on device is at risk

The best solution is to *verifiably* **sanitize!**

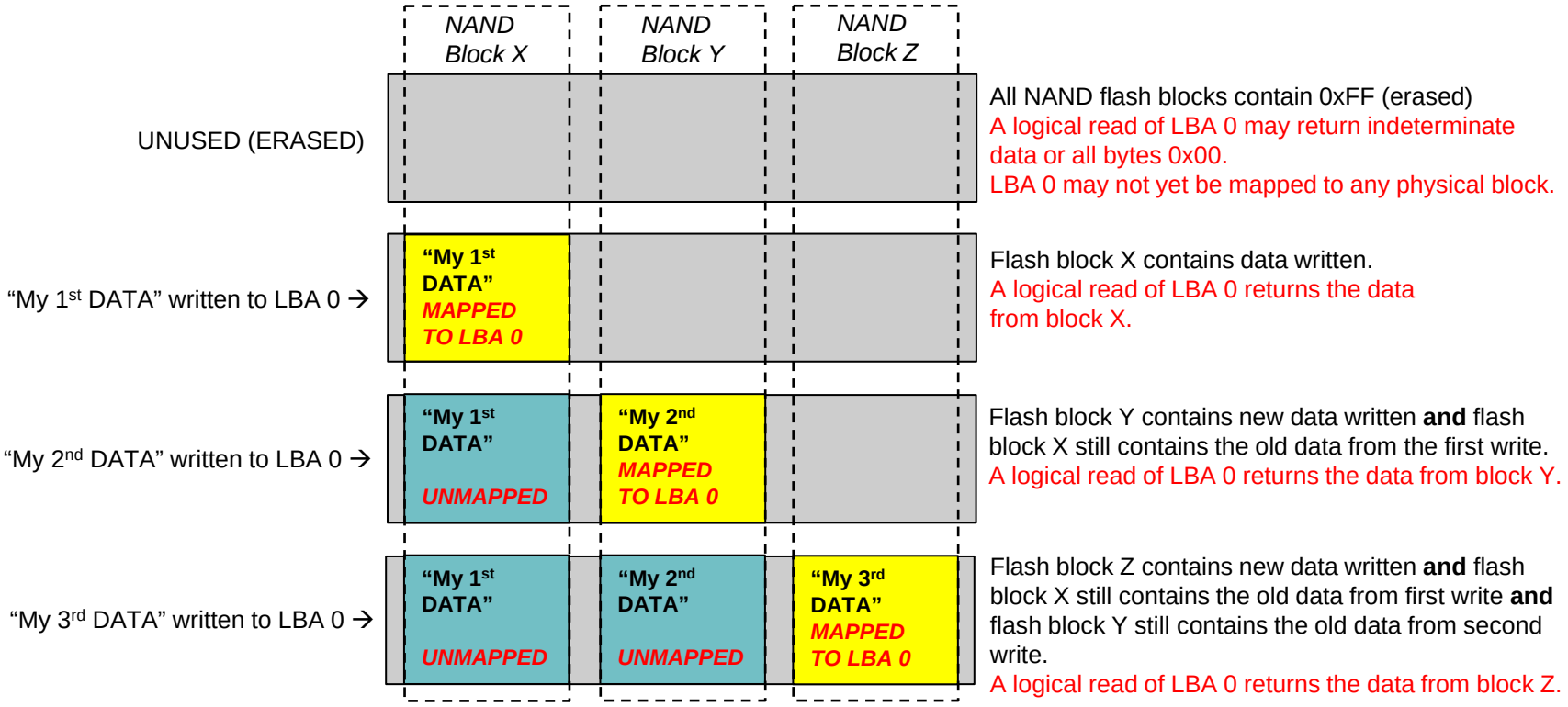
How do we measure sanitization success?



- Erased data cannot be recovered at the logical level i.e. standard read commands over device interface
- Erased data cannot be recovered using vendor-unique commands nor firmware hacks
- Erased data cannot be recovered using physical-access methods (NAND memory removal and raw data extraction)

Method 1: Logical Overwrite

- Uses standard interface commands, writes incrementally to all *logical* blocks
- With SSD *physical* copies of old data in NAND not overwritten:



Method 2: Vendor Erase Function

- Invoked by standard interface command e.g. *ATA Secure Erase Unit* or *ACS-3 Sanitize Device*

- SSD firmware wholly responsible for the actual erase method used and how well it works.
- Just a Pass / Fail status back to host. Details would be nice!

Method 2: Vendor Erase Function

- Rather than pass / fail the SSD could instead provide feedback with empirical data upon completion of the vendor erase function...

- For a crypto-erase (proves DEK has changed):-

- Whilst not guaranteeing the erasure it inspires more confidence in the user that the SSD knows what *should* be done...

SSD Erasure Verification Service (EVS)

Purpose

To measure and report upon the effectiveness of our client's chosen sanitization method on a specific SSD model and revision

Level 1 (Logical)

- Tests if erased data can be read from the SSD using standard read commands over the device's interface
- No SSDs will be harmed at this level of the process!

Level 2 (Logical and Physical)

- Additionally tests if erased data can be read through extraction of raw data directly from the SSD's NAND memory
- The "guinea-pig" SSD will almost always be dismantled and destroyed during the physical verification process

SSD Erasure Verification Service (EVS)

The Process

1. SSD preparation

- Fixed data pattern: So we know what “user data” to look for!
- All LBAs written multiple times: So SSD uses as many as possible of its spare NAND flash blocks

2. Sanitization

- Client (or Kroll Ontrack) carries out chosen sanitization process on SSD
- This can be just one sanitization method or a combination of methods applied in a pre-determined sequence

SSD Erasure Verification Service (EVS)

The Process (continued..)

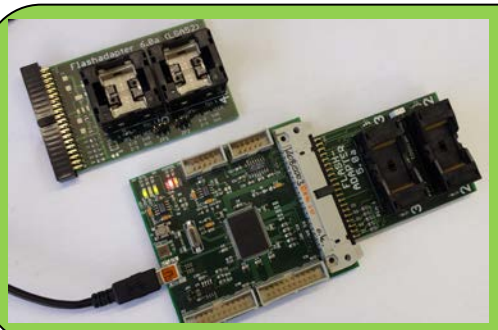
3. Verification

- To level required by client:
- Level 1: Logical verification only
- Level 2: Logical and physical verification: Remove NAND flash, extract raw data, process (to reverse modifications applied by SSD controller), search for user data

4. Report

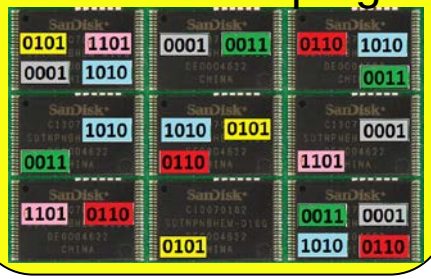
- A conclusion regarding the effectiveness of the sanitization process on the tested SSD model and revision

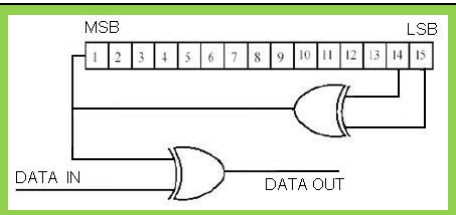
Erasure Verification – Technical Challenges and relationship to DR (Data Recovery)



NAND Reader

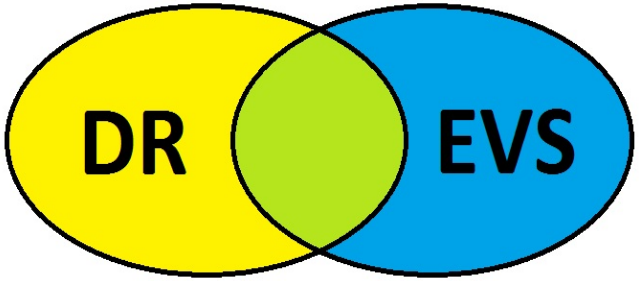
Data de-Striping

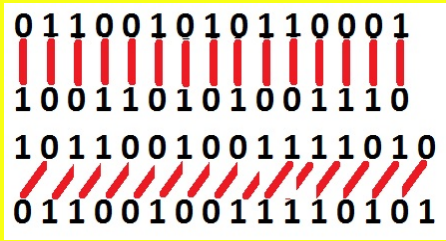




Data descrambler, decoder, de-randomizer

Error-correction (ECC)





Bit-level manipulations

Data decryption

80	33	31	64	63	48	32	36	3
90	F7	9B	DA	E4	10	02	00	0
A0	2B	CD	B0	43	2D	C5	58	9
B0	07	46	0B	1E	4B	C4	96	1
C0	73	AC	EB	FB	E3	44	98	F
D0	2F	CD	40	51	AF	7E	E1	B
E0	1E	34	F9	A3	95	FF	CD	6

Who needs and who uses EVS?

- Large SSD storage integrators
- Value-Added Resellers
- SSD and mobile device manufacturers
- Anyone with a need to independently verify their sanitization process for SSD and NAND flash memory

- Case Studies:
  - Corporate IT end user
    - Which sanitization method to use?
    - Which model of SSD to choose?

  - Mobile Phone / Tablet manufacturer
    - Is existing sanitization method effective on all variants of integrated NAND flash drive?

Summary

- Sanitization is an essential component of data management and the chosen sanitization method must be verifiable.
- A sanitization process that has been tried and trusted on other media types (e.g. hard drives) may not be adequate for SSD.
- End-users have little confidence in the effectiveness of the SSD internal vendor erase function. Device manufacturers and Standards could help by implementing an *empirical* report of erase function outcome.
- Erasure Verification provides an independent check that a sanitization process works to the desired level on known hardware.
- Erasure verification (at NAND flash level) is a complex task and requires a sound understanding of SSD and NAND flash technologies.

Thank You!

Please visit us at booth #819