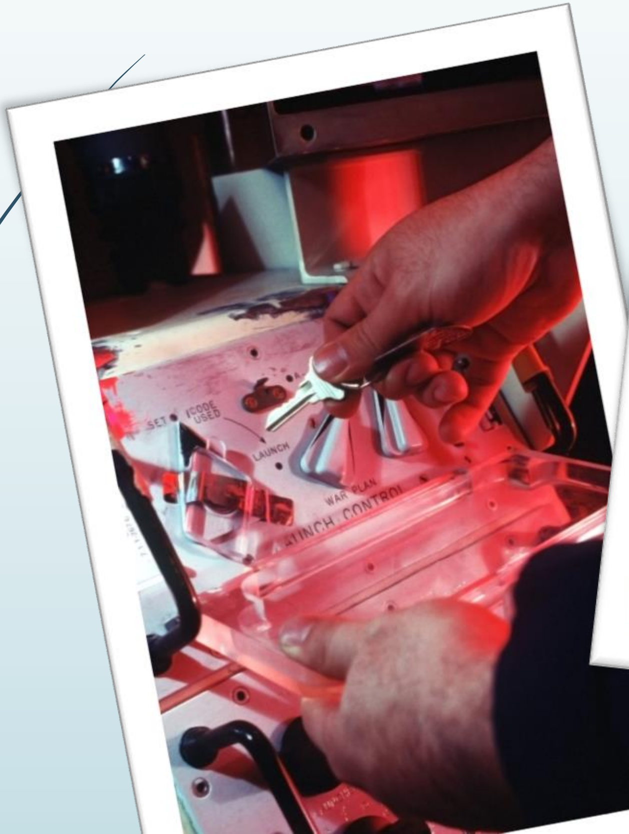
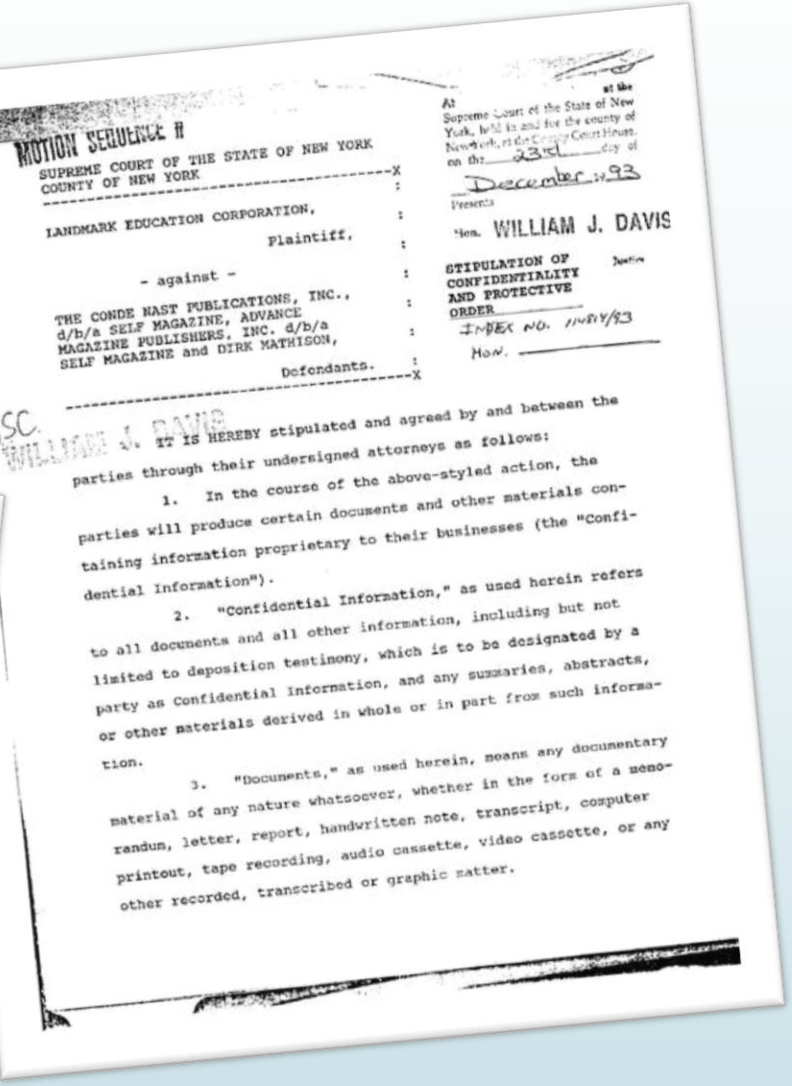
Challenges in Reliably Sanitizing Solid State Disks

Michael Wei, Steven Swanson
Non-volatile Systems Laboratory
UC San Diego

Confidential Data





MOTION SEQUENCE #

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

LANDMARK EDUCATION CORPORATION,

Plaintiff,

- against -

THE CONDE NAST PUBLICATIONS, INC.,
d/b/a SELF MAGAZINE, ADVANCE
MAGAZINE PUBLISHERS, INC. d/b/a
SELF MAGAZINE and DIRK MATHISON,

Defendants.

At at the
Supreme Court of the State of New
York, held in and for the county of
New York, at the County Court House,
on the 23rd day of
December 19 93

Present:

Hon. WILLIAM J. DAVIS
Justice

STIPULATION OF
CONFIDENTIALITY
AND PROTECTIVE
ORDER

INDEX NO. 114814/93

HON.

JSC.
WILLIAM J. DAVIS

IT IS HEREBY stipulated and agreed by and between the parties through their undersigned attorneys as follows:

1. In the course of the above-styled action, the parties will produce certain documents and other materials containing information proprietary to their businesses (the "Confidential Information").

2. "Confidential Information," as used herein refers to all documents and all other information, including but not limited to deposition testimony, which is to be designated by a party as Confidential Information, and any summaries, abstracts, or other materials derived in whole or in part from such information.

3. "Documents," as used herein, means any documentary material of any nature whatsoever, whether in the form of a memorandum, letter, report, handwritten note, transcript, computer printout, tape recording, audio cassette, video cassette, or any other recorded, transcribed or graphic matter.

Overview

- **Past work in sanitizing disks**
- US Coast Guard RMMs
    - Introduction
    - Sanitization & Evaluation
    - Report
- Scramble and Finally Erase (SAFE)

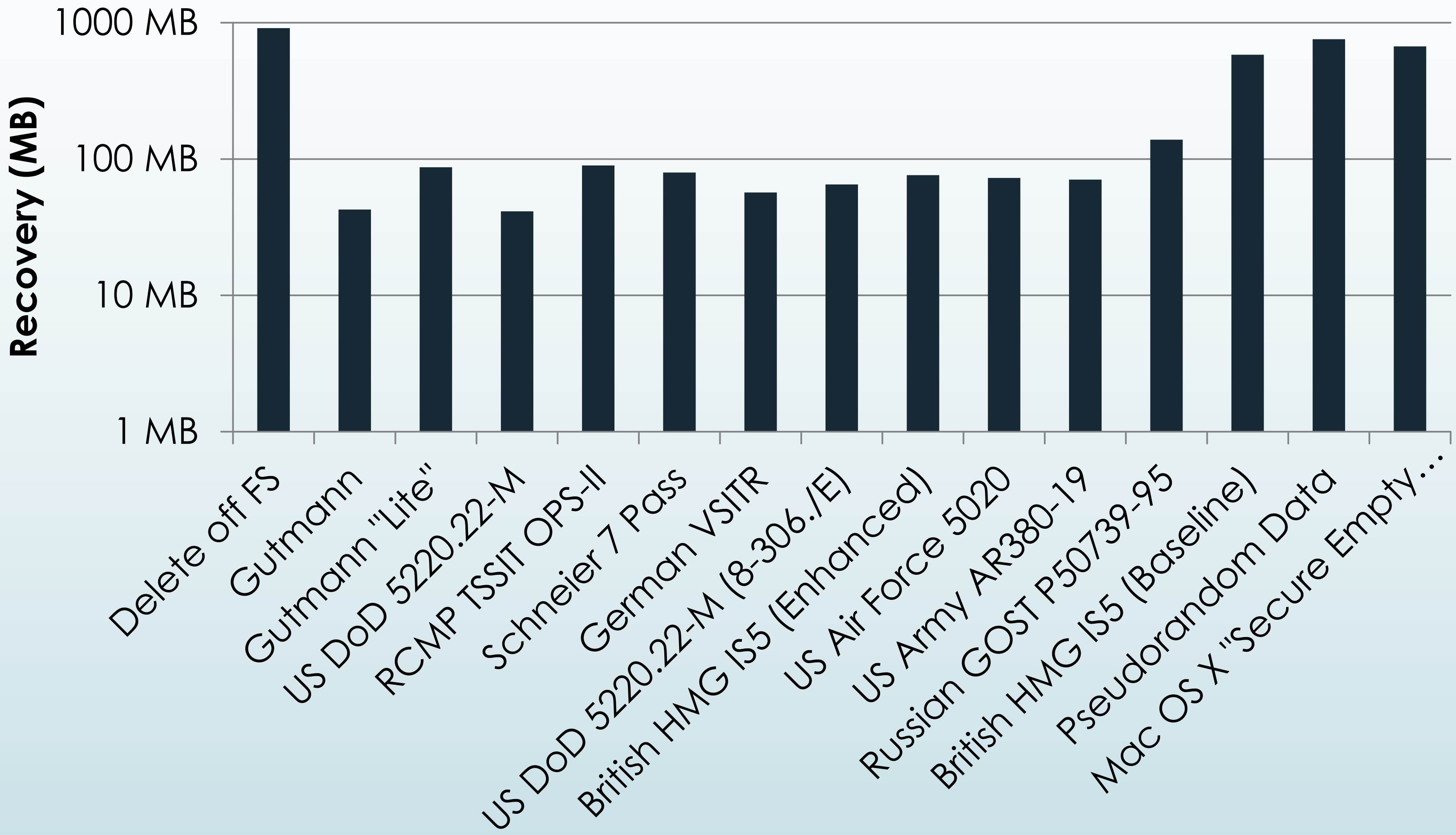
Previous Work: Reliably Sanitizing Solid-State Disks

- Published in 2011:
  Reliably Erasing Data from Flash-Based Solid State Drives
  Michael Wei, Laura M. Grupp, Frederick E. Spada, and Steven Swanson
  9th USENIX Conference on File and Storage Technologies (FAST' 11)
- Need to **verify** sanitization effectiveness
  - Built-in mechanisms are reliable when implemented correctly
  - Hard-drive techniques don't necessarily work
- Sanitizing single files (in place) is difficult
  - Software overwrite cannot reliably sanitize
  - Scrubbing allows us to sanitize files by modifying the FTL

Previous Work: Reliably Sanitizing Solid-State Disks

SSD Name	Controller	SECURITY ERASE UNIT (ATA-3)	SECURITY ERASE UNIT ENHANCED (ATA-3)
A	1	No	No
B	2	No (Reports yes)	No
C	1	Partial (Bugged)	No
D	3	Partial (Bugged)	No
E	4	Crypto Scrambles	Crypto Scrambles
F	5	Yes	Yes
G	6	Yes	No
H	7	Yes	Yes
I	8	Yes	Yes

Previous Work: Reliably Sanitizing Solid-State Disks



Overview

- Past work in sanitizing disks
- **US Coast Guard RMMs**
  - Introduction
  - Sanitization & Evaluation
  - Report
- Scramble and Finally Erase (SAFE)

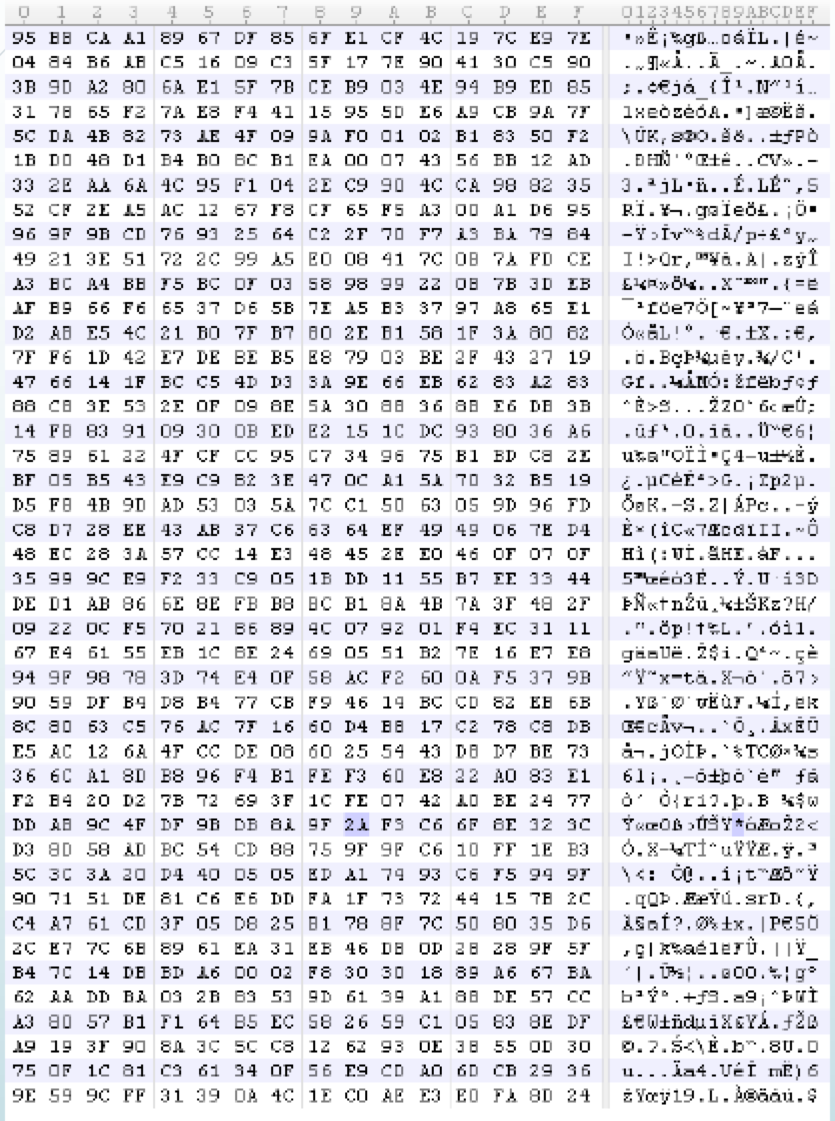
Coast Guard RMMs

- Part of the **NATO** ISR INTEROPERABILITY ARCHITECTURE (NIIA)
  - One storage interface and device for all NATO organizations
  - Can support SSDs or Hard Drive Arrays
- Need to be sanitized
  - At end of-life
  - If unit is in danger (i.e. plane crash, hostile takeover, etc.)
  - **If security classification level changes**
  - Want to use the same drive for both classified and unclassified missions

Sanitization and evaluation

- Wrote our fingerprint using the USB interface
- Returned drives to Coast Guard for sanitization
- Attempted to recover the fingerprint

Report



```
 0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
95 BB CA A1 89 67 DF 85 6F E1 CF 4C 19 7C E9 7E   •»Ê¡‰gß…oáÏL.|é~
04 84 B6 AB C5 16 D9 C3 5F 17 7E 90 41 30 C5 90   .„¶«Å.ÙÃ_.~.A0Å.
3B 9D A2 80 6A E1 5F 7B CE B9 03 4E 94 B9 ED 85   ;.¢€já_{Î¹.N”¹í…
31 78 65 F2 7A E8 F4 41 15 95 5D E6 A9 CB 9A 7F   1xeòzèôA.•]æ©Ëš.
5C DA 4B 82 73 AE 4F 09 9A F0 01 02 B1 83 50 F2   \ÚK‚s®O.šð..±ƒPò
1B D0 48 D1 B4 B0 BC B1 EA 00 07 43 56 BB 12 AD   .ÐHÑ´°¼±ê..CV».-
33 2E AA 6A 4C 95 F1 04 2E C9 90 4C CA 98 82 35   3.ªjL•ñ..É.LÊ˜‚5
52 CF 2E A5 AC 12 67 F8 CF 65 F5 A3 00 A1 D6 95   RÏ.¥¬.gøÏeõ£.¡Ö•
96 9F 9B CD 76 93 25 64 C2 2F 70 F7 A3 BA 79 84   –Ÿ›Ív“%dÂ/p÷£ºy„
49 21 3E 51 72 2C 99 A5 E0 08 41 7C 08 7A FD CE   I!>Qr,™¥à.A|.zýÎ
A3 BC A4 BB F5 BC DF 03 58 98 99 22 08 7B 3D EB   £¼¤»õ¼ß.X˜™".{=ë
AF B9 66 F6 65 37 D6 5B 7E A5 B3 37 97 A8 65 E1   ¯¹föe7Ö[~¥³7—¨eá
D2 AB E5 4C 21 B0 7F B7 80 2E B1 58 1F 3A 80 82   Ò«åL!°.·€.±X.:€‚
7F F6 1D 42 E7 DE BE B5 E8 79 03 BE 2F 43 27 19   .ö.BçÞ¾µèy.¾/C'.
47 66 14 1F BC C5 4D D3 3A 9E 66 EB 62 83 A2 83   Gf..¼ÅMÓ:žfëbƒ¢ƒ
88 C8 3E 53 2E 0F D9 8E 5A 30 88 36 88 E6 DB 3B   ˆÈ>S..ÙŽZ0ˆ6ˆæÛ;
14 FB 83 91 09 30 0B ED E2 15 1C DC 93 80 36 A6   .ûƒ‘.0.íâ..Ü“€6¦
75 89 61 22 4F CF CC 95 C7 34 96 75 B1 BD C8 2E   u‰a"OÏÌ•Ç4–u±½È.
BF 05 B5 43 E9 C9 B2 3E 47 0C A1 5A 70 32 B5 19   ¿.µCéÉ²>G.¡Zp2µ.
D5 F8 4B 9D AD 53 D3 5A 7C C1 50 63 05 9D 96 FD   ÕøK.-S.Z|ÁPc..–ý
C8 D7 28 EE 43 AB 37 C6 63 64 EF 49 49 06 7E D4   È×(îC«7ÆcdïII.~Ô
48 EC 28 3A 57 CC 14 E3 48 45 2E E0 46 0F 07 0F   Hì(:WÌ.ãHE.àF...
35 99 9C E9 F2 33 C9 05 1B DD 11 55 B7 EE 33 44   5™œéò3É..Ý.U·î3D
DE D1 AB 86 6E 8E FB B8 BC B1 8A 4B 7A 3F 48 2F   ÞÑ«†nŽû¸¼±ŠKz?H/
09 22 0C F5 70 21 86 89 4C 07 92 01 F4 EC 31 11   .".õp!†‰L.’.ôì1.
67 E4 61 55 EB 1C BE 24 69 05 51 B2 7E 16 E7 E8   gäaUë.¾$i.Q²~.çè
94 9F 98 78 3D 74 E4 0F 58 AC F2 60 0A F5 37 9B   ”Ÿ˜x=tä.X¬ò`.õ7›
90 59 DF B4 D8 B4 77 CB F9 46 19 BC CD 82 EB 6B   .Yß´Ø´wËùF.¼Í‚ëk
8C 80 63 C5 76 AC 7F 16 60 D4 B8 17 C2 78 C8 DB   Œ€cÅv¬..`Ô¸.ÂxÈÛ
E5 AC 12 6A 4F CC DE 08 60 25 54 43 D8 D7 BE 73   å¬.jOÌÞ.`%TCØ×¾s
36 6C A1 8D B8 96 F4 B1 FE F3 60 E8 22 A0 83 E1   6l¡.¸–ô±þó`è" ƒá
F2 B4 20 D2 7B 72 69 3F 1C FE 07 42 A0 BE 24 77   ò´ Ò{ri?.þ.B ¾$w
DD AB 9C 4F DF 9B DB 8A 9F 2A F3 C6 6F 8E 32 3C   Ý«œOß›ÛŠŸ*óÆoŽ2<
D3 8D 58 AD BC 54 CD 88 75 9F 9F C6 10 FF 1E B3   Ó.X-¼TÍˆuŸŸÆ.ÿ.³
5C 3C 3A 20 D4 40 05 05 ED A1 74 93 C6 F5 94 9F   \<: Ô@..í¡t“Æõ”Ÿ
90 71 51 DE 81 C6 E6 DD FA 1F 73 72 44 15 7B 2C   .qQÞ.ÆæÝú.srD.{,
C4 A7 61 CD 3F 05 D8 25 B1 78 8F 7C 50 80 35 D6   Ä§aÍ?.Ø%±x.|P€5Ö
2C E7 7C 6B 89 61 EA 31 EB 46 DB 0D 28 28 9F 5F   ,ç|k‰aê1ëFÛ.((Ÿ_
B4 7C 14 DB BD A6 D0 02 F8 30 30 18 89 A6 67 BA   ´|.Û½¦Ð.ø00.‰¦gº
62 AA DD BA 03 2B B3 53 9D 61 39 A1 88 DE 57 CC   bªÝº.+³S.a9¡ˆÞWÌ
A3 80 57 B1 F1 64 B5 EC 58 26 59 C1 05 83 8E DF   £€W±ñdµìX&YÁ.ƒŽß
A9 19 3F 90 8A 3C 5C C8 12 62 93 0E 38 55 0D 30   ©.?.Š<\È.b“.8U.0
75 0F 1C 81 C3 61 34 0F 56 E9 CD A0 6D CB 29 36   u...Ãa4.VéÍ mË)6
9E 59 9C FF 31 39 0A 4C 1E C0 AE E3 E0 FA 8D 24   žYœÿ19.L.À®ãàú.$
```

- Drive was 99% erased
- 1% of the drive contained data patterns
- Could have been an encrypted version of the fingerprint

- Went to manufacturer
- Engineers produced a report documenting that the patterns were metadata and firmware

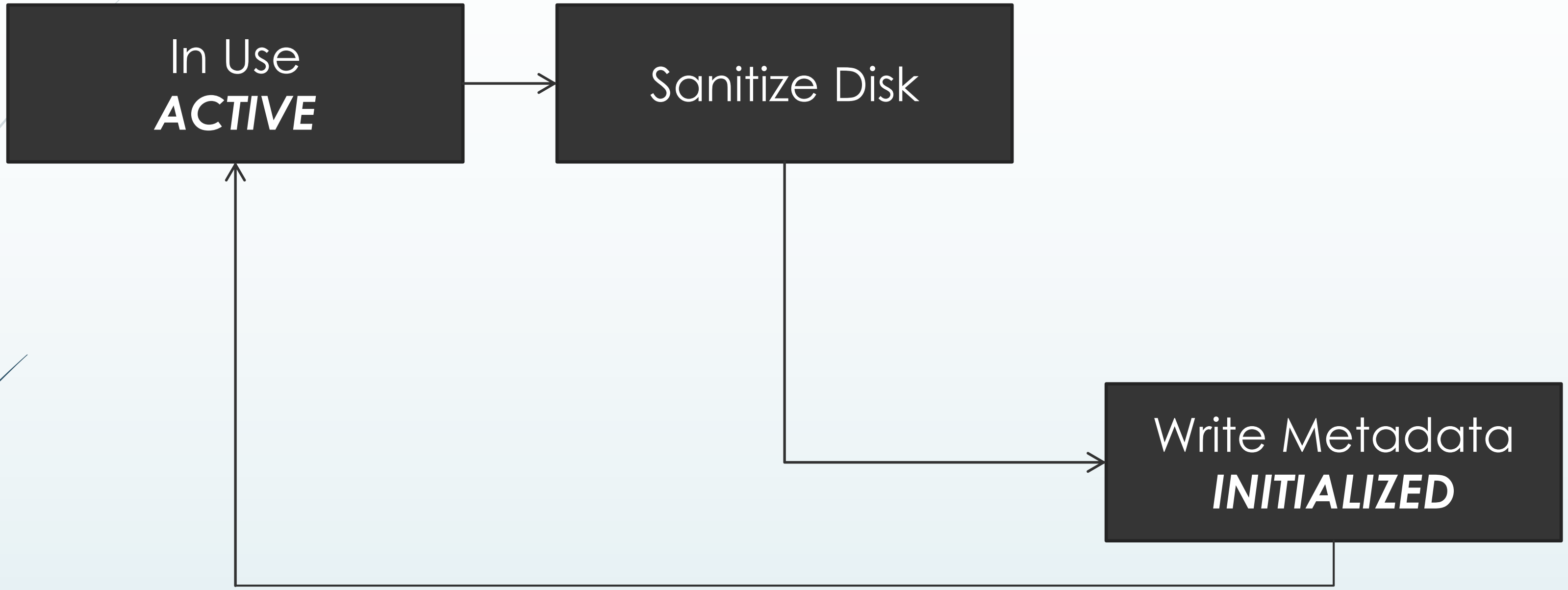
Problems

- Don’t want to contact the manufacturer every time
- Talking to the manufacturer is expensive and time consuming
  - Manufacturer has to allocate engineers
  - Engineers take time to produce a report
  - Manufacturer might not have designed the controller
  - Somebody has to interpret to manufacturers report
- Easiest to verify a drive that is all 0s

Overview

- Past work in sanitizing disks
- US Coast Guard RMMs
  - Introduction
  - Sanitization & Evaluation
  - Report
- **Scramble and Finally Erase (SAFE)**

SAFE: Scramble and Finally Erase



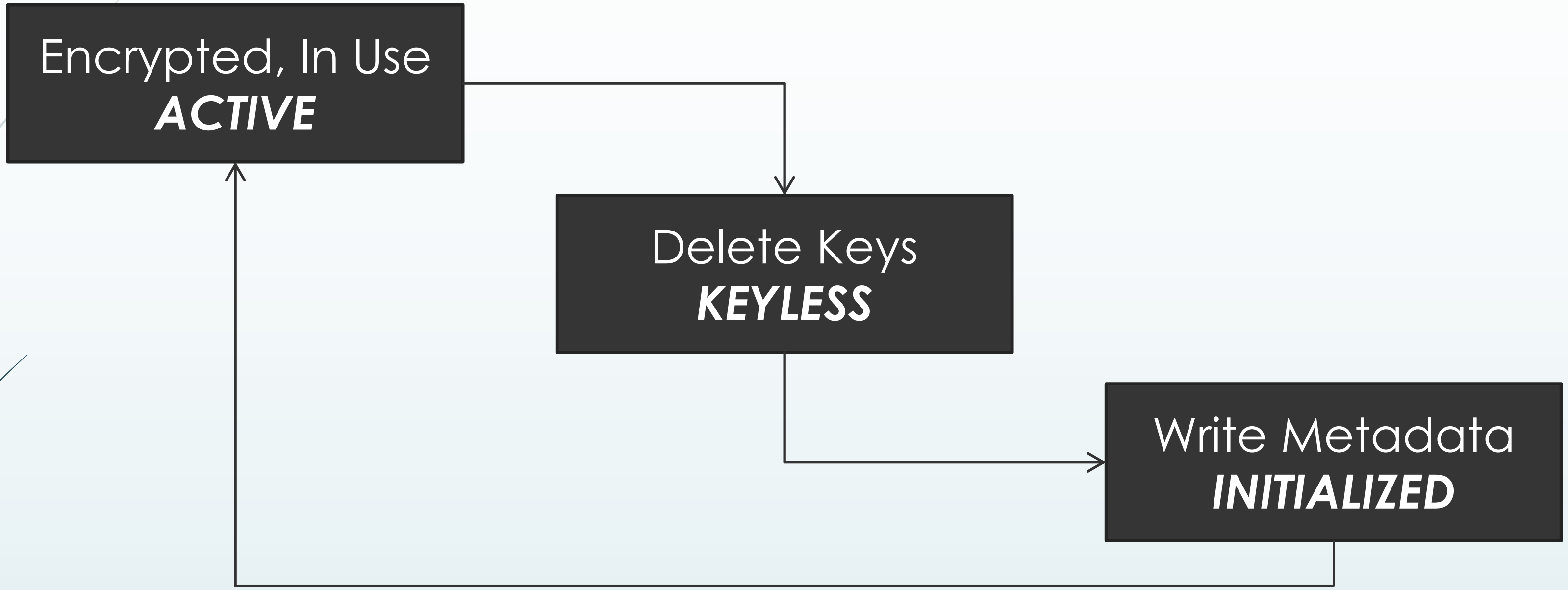
In Use
ACTIVE

Sanitize Disk

Write Metadata
INITIALIZED

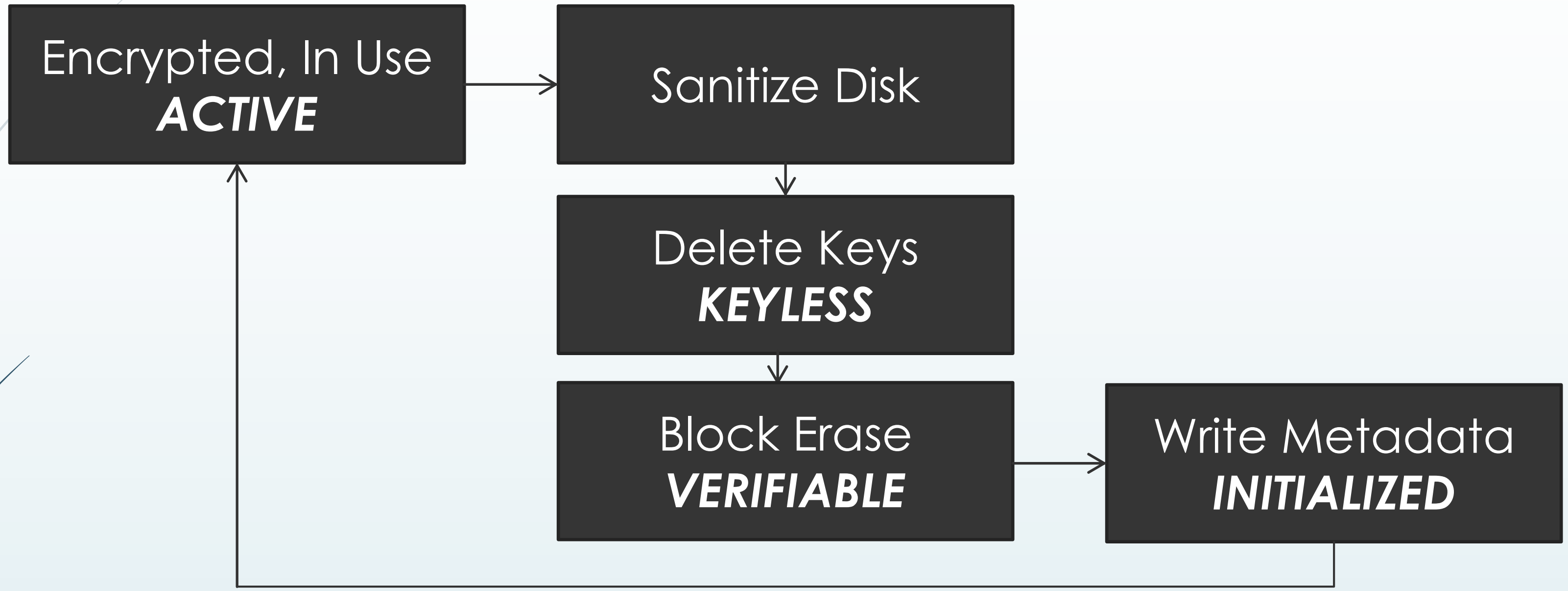
- Traditional Sanitization Process
  - Sanitize and Initialize in a single step
  - Drive is *INITIALIZED* after a sanitize

SAFE: Scramble and Finally Erase



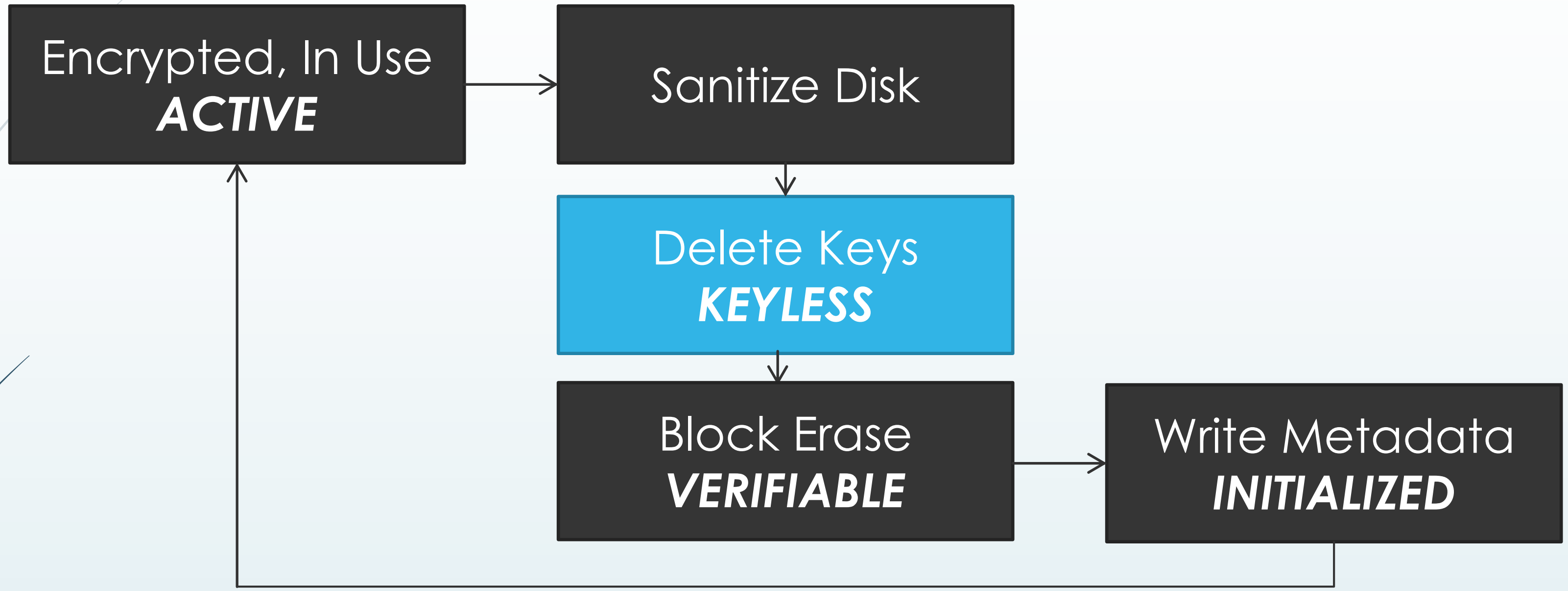
- Crypto-Erase "Sanitization" Process
  - Delete keys
  - Drive is *INITIALIZED* after a sanitize

SAFE: Scramble and Finally Erase



SAFE breaks this up and adds two new states: *KEYLESS and VERIFIABLE*

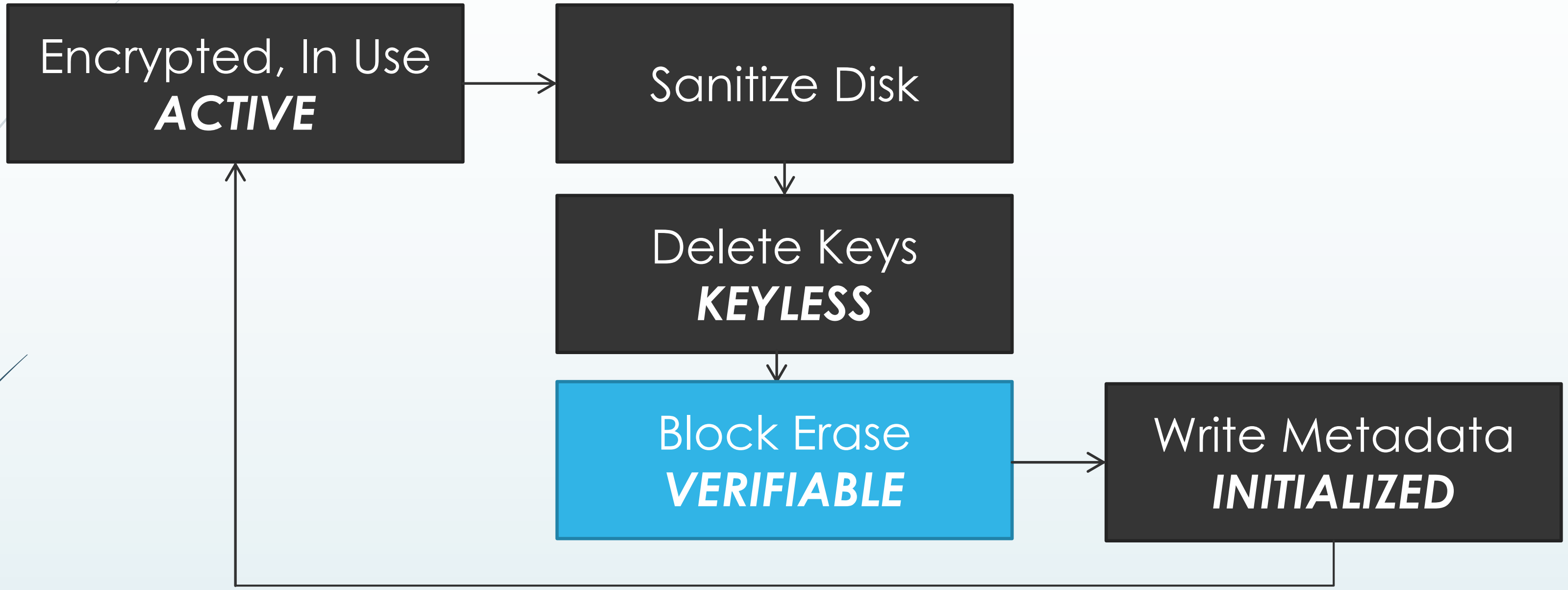
SAFE: Scramble and Finally Erase



Scramble: Drive is actively being encrypted

- On sanitize, delete the keys (*KEYLESS*)
- This step takes milliseconds

SAFE: Scramble and Finally Erase



Erase: Perform a block erase after scramble

- We can easily verify the drive (*VERIFIABLE)*
- This step takes minutes

Conclusion

- Sanitizing storage media is essential for data security
- Need to **verify** sanitization effectiveness
- Metadata and encryption can make verification difficult
- SAFE is a system that allows us to verify drives with the protection of encryption