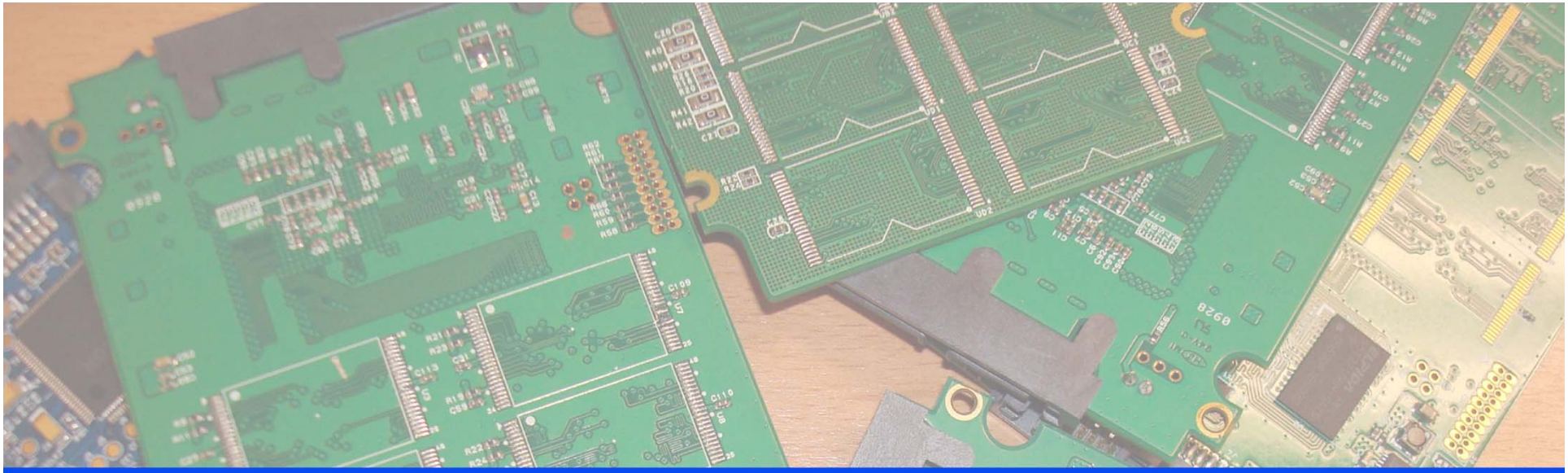
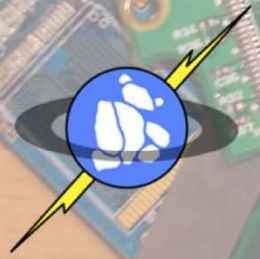


Reliably Erasing Data from Flash-Based Solid State Drives

Michael Wei, Laura Grupp, Steven Swanson

Non-Volatile Systems Laboratory
Department of Computer Science and Engineering
University of California, San Diego



UCSDCSE
Computer Science and Engineering

CMRR
Center for Magnetic Recording Research

Non-Volatile Systems Laboratory
Department of Computer Science and Engineering
University of California, San Diego

Overview

Problem, methods and solutions

- **The Problem -** Confidential data needs to be removed from SSDs
  - How does data get deleted from a SSD
  - How does this cause a problem?
- **Auditing Methodology**
- **Results**
  - Disk-Based
  - File-Based

Motivation

Security of confidential data

- Intentional
  - Credit card numbers
  - Confidential & Proprietary Information
- Unintentional
  - Web browsing history
  - Temporary Files

The Problem

How data is deleted: HDD

- 1-1 logical to physical mapping
- Data doesn't move

1: Write "UCSD NVSL" to LBA 8000

2: Write 1s to LBA 8000

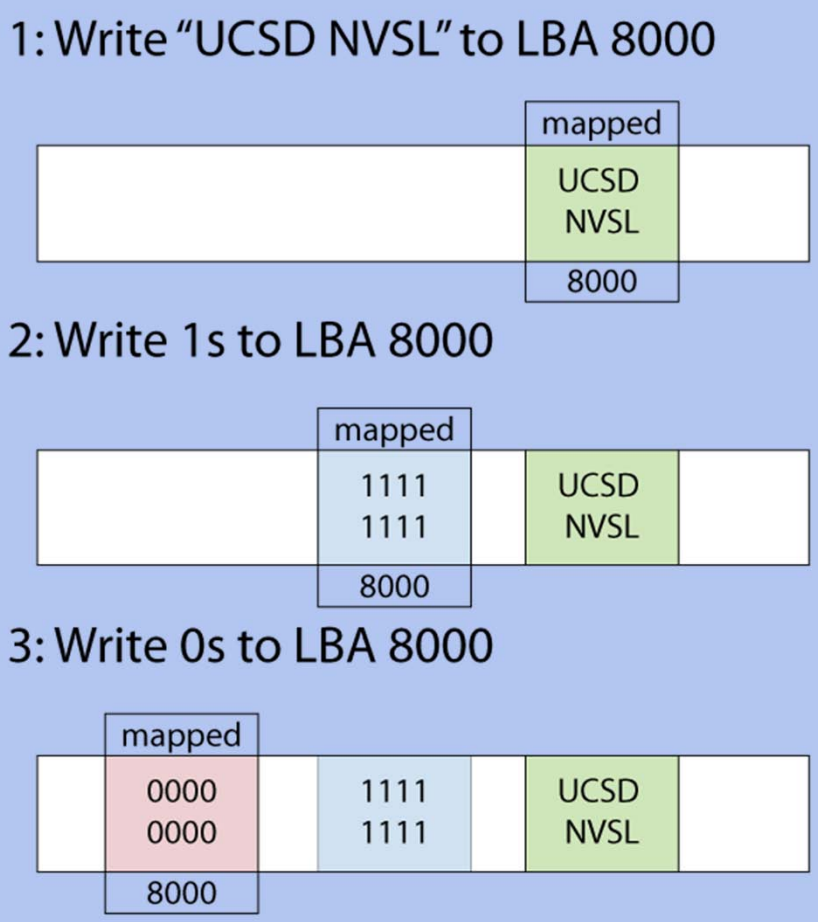
3: Write 0s to LBA 8000

Non-Volatile Systems Laboratory
Department of Computer Science and Engineering
University of California, San Diego

The Problem

How data is deleted: SSD

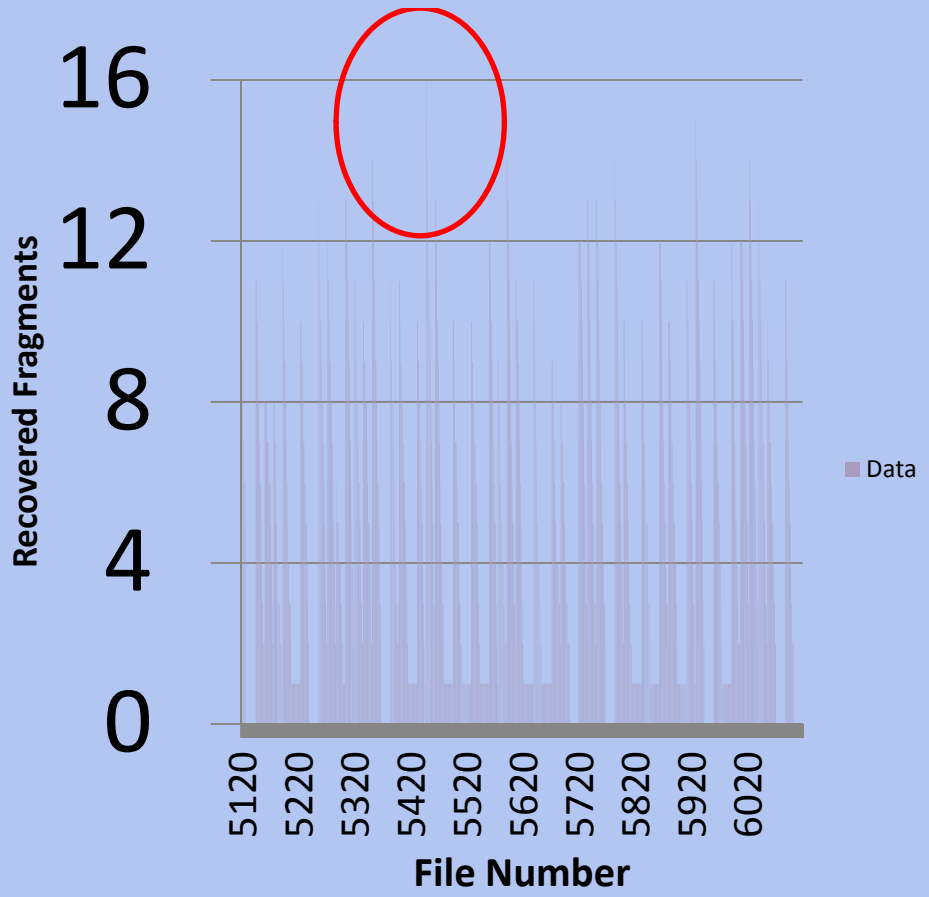
- Flash properties
  - Wears out
  - Page write, block erase
- No 1-1 mapping
- Overprovisioned



The Problem

Multiple Copies

- Flash Management = multiple copies
- Our tests
  - Wrote 1000 files
  - Found 16 copies of some files
- Bad for overwrite-based secure erase

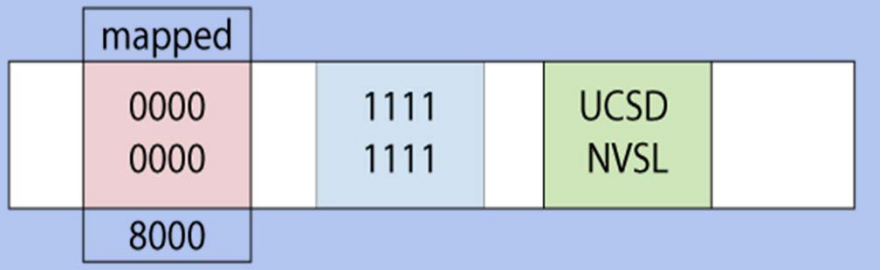


Non-Volatile Systems Laboratory
Department of Computer Science and Engineering
University of California, San Diego

Verification & Auditing

Part I: Recovering Data

- Need to get to "inaccessible data"
- Recover the same way an adversary would
- Remove bare flash chips
- Retrieve data from flash chips



Verification & Auditing

Part II: Generating and destroying data

- Generate specially crafted data that we can recover later
  - Unique ID
  - Checksum
- Write the data to the drive
- Try to get rid of the data

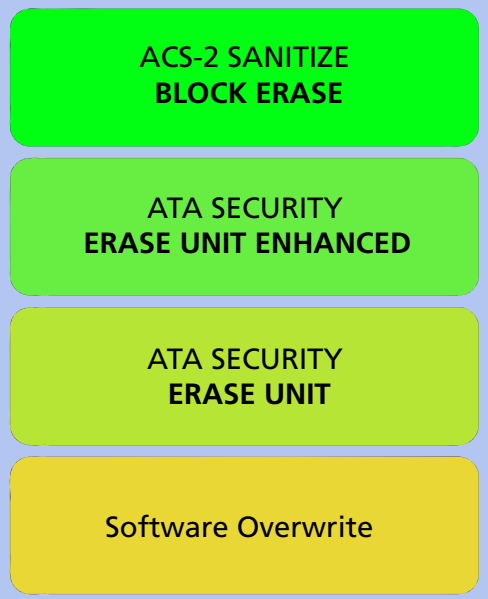
Overview
Problem, methods and solutions

- **The Problem -** Confidential data needs to be removed from SSDs
  - How does data get deleted from a SSD
  - How does this cause a problem?
- **Auditing Methodology**
- **Results**
  - Disk-Based
  - File-Based

Disk-Based Procedure

Overview

- Targets the entire disk
- Built-in commands:
  - "ERASE UNIT"
  - "BLOCK ERASE"
- Software Overwrite



Disk-Based Procedure

Drive Support for ATA Security/ACS-2 Sanitize

SSD Name	Controller	SECURITY ERASE UNIT (ATA-3)	SECURITY ERASE UNIT ENHANCED (ATA-3)	Sanitize BLOCK ERASE EXT (ATA8-ACS2)	Sanitize OVERWRITE EXT (ATA8-ACS2)	Sanitize CRYPTO SCRAMBLE EXT (ATA8-ACS2)
A	1	No	No	No	No	No
B	2	No (Reports yes)	No	No	No	No
C	1	Partial (Bugged)	No	No	No	No
D	3	Partial (Bugged)	No	No	No	No
E	4	Crypto Scrambles	Crypto Scrambles	No	No	No
F	5	Yes	Yes	No	No	No
G	6	Yes	No	No	No	No
H	7	Yes	Yes	No	No	No
I	8	Yes	Yes	No	No	No

Disk-Based Procedure

Drive Support for ATA Security/ACS-2 Sanitize

SSD Name	Controller	SECURITY ERASE UNIT (ATA-3)	SECURITY ERASE UNIT ENHANCED (ATA-3)	Sanitize BLOCK ERASE EXT (ATA8-ACS2)	Sanitize OVERWRITE EXT (ATA8-ACS2)	Sanitize CRYPTO SCRAMBLE EXT (ATA8-ACS2)
A	1	No	No	No	No	No
B	2	No (Reports yes)	No	No	No	No
C	1	Partial (Bugged)	No	No	No	No
D	3	Partial (Bugged)	No	No	No	No
E	4	Crypto Scrambles	Crypto Scrambles	No	No	No
F	5	Yes	Yes	No	No	No
G	6	Yes	No	No	No	No
H	7	Yes	Yes	No	No	No
I	8	Yes	Yes	No	No	No

Disk-Based Procedure

Drive Support for ATA Security/ACS-2 Sanitize

SSD Name	Controller	SECURITY ERASE UNIT (ATA-3)	SECURITY ERASE UNIT ENHANCED (ATA-3)	Sanitize BLOCK ERASE EXT (ATA8-ACS2)	Sanitize OVERWRITE EXT (ATA8-ACS2)	Sanitize CRYPTO SCRAMBLE EXT (ATA8-ACS2)
A	1	No	No	No	No	No
B	2	No (Reports yes)	No	No	No	No
C	1	Partial (Bugged)	No	No	No	No
D	3	Partial (Bugged)	No	No	No	No
E	4	Crypto Scrambles	Crypto Scrambles	No	No	No
F	5	Yes	Yes	No	No	No
G	6	Yes	No	No	No	No
H	7	Yes	Yes	No	No	No
I	8	Yes	Yes	No	No	No

Disk-Based Procedure

Drive Support for ATA Security/ACS-2 Sanitize

SSD Name	Controller	SECURITY ERASE UNIT (ATA-3)	SECURITY ERASE UNIT ENHANCED (ATA-3)	Sanitize BLOCK ERASE EXT (ATA8-ACS2)	Sanitize OVERWRITE EXT (ATA8-ACS2)	Sanitize CRYPTO SCRAMBLE EXT (ATA8-ACS2)
A	1	No	No	No	No	No
B	2	No (Reports yes)	No	No	No	No
C	1	Partial (Bugged)	No	No	No	No
D	3	Partial (Bugged)	No	No	No	No
E	4	Crypto Scrambles	Crypto Scrambles	No	No	No
F	5	Yes	Yes	No	No	No
G	6	Yes	No	No	No	No
H	7	Yes	Yes	No	No	No
I	8	Yes	Yes	No	No	No

Disk-Based Procedure

Drive Support for ATA Security/ACS-2 Sanitize

SSD Name	Controller	SECURITY ERASE UNIT (ATA-3)	SECURITY ERASE UNIT ENHANCED (ATA-3)	Sanitize BLOCK ERASE EXT (ATA8-ACS2)	Sanitize OVERWRITE EXT (ATA8-ACS2)	Sanitize CRYPTO SCRAMBLE EXT (ATA8-ACS2)
A	1	No	No	No	No	No
B	2	No (Reports yes)	No	No	No	No
C	1	Partial (Bugged)	No	No	No	No
D	3	Partial (Bugged)	No	No	No	No
E	4	Crypto Scrambles	Crypto Scrambles	No	No	No
F	5	Yes	Yes	No	No	No
G	6	Yes	No	No	No	No
H	7	Yes	Yes	No	No	No
I	8	Yes	Yes	No	No	No

Disk-Based Procedure

Software Overwriting

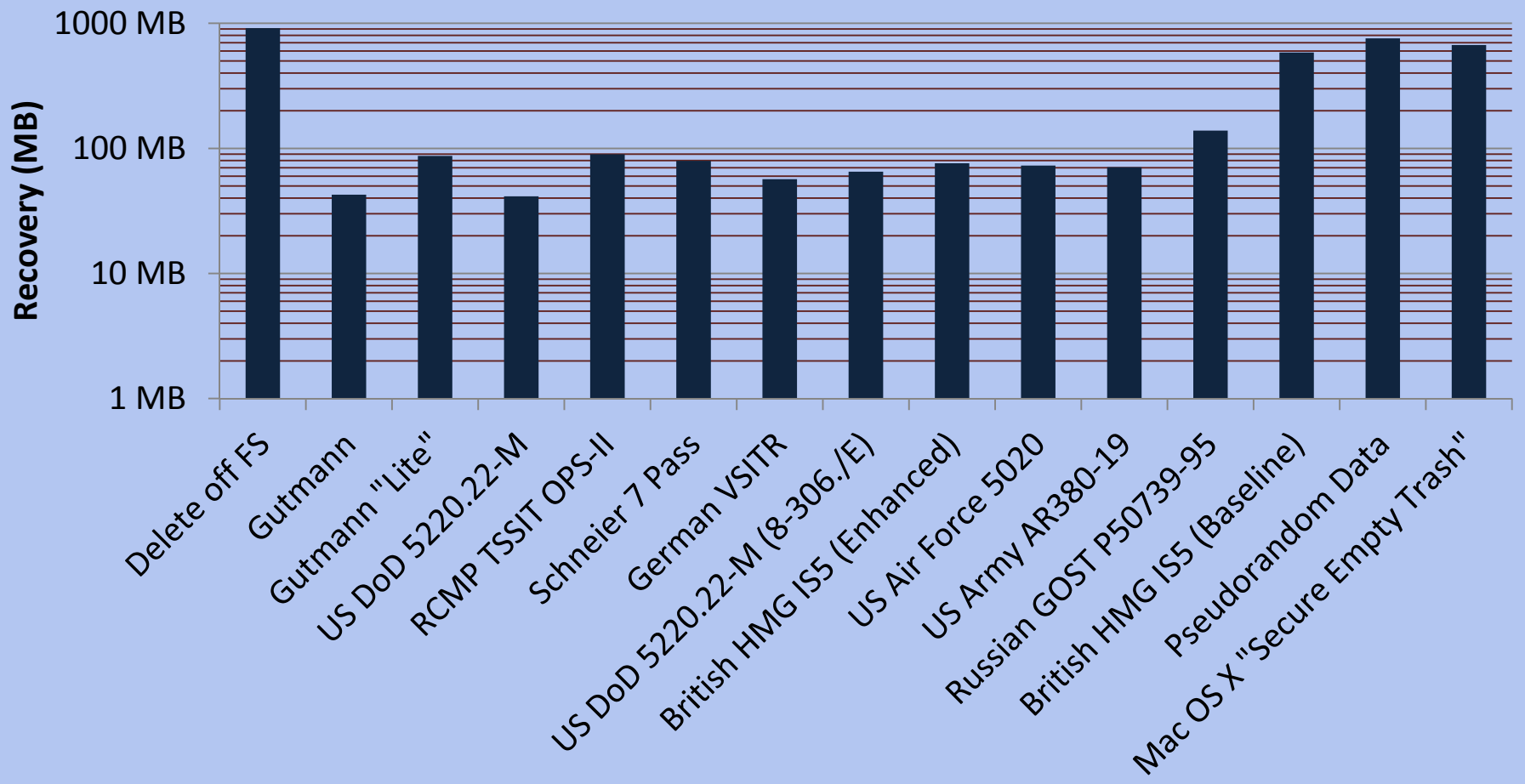
- N-Pass Overwrite
  - Designed to eliminate analog "ghosts" in HDDs
- Our experiments show 2 passes are ***typically*** necessary
  - One case left data after **20 passes**
  - Another left data after **4 passes**
  - Difficult to exhaustively test
    - Depends on previous state of drive

Overview
Problem, methods and solutions

- **The Problem -** Confidential data needs to be removed from SSDs
  - How does data get deleted from a SSD
  - How does this cause a problem?
- **Auditing Methodology**
- **Results**
  - Disk-Based
  - File-Based

File-Based Procedure

Verification



- 14 Procedures tested, all failed

File-Based Procedure

Free space Scrubbing

- Overwrite free space N-passes
  - Gets rid of left over data in filesystem
  - 100 overwrites over free space

- **Result: 80%** of deleted data left

File-Based Procedure

Defragmentation

- Overwrite free space, then defragment
  - Gets rid of "chunks" allocated with other good data
  - Most Aggressive
- **Result: 80%** of deleted data left

Conclusion

- Secure erase is important for SSD adoption
- Need to verify procedures
- We've developed an auditing technique
  - Disk-based secure erase commands are unreliable
  - 14 file-based deletion techniques failed
- Can't assume that HDD techniques work on SSD