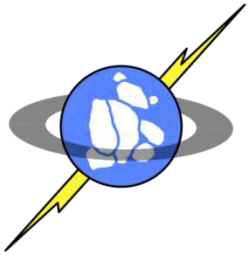
Secure Erasure of Flash Memory

Adrian Caulfield, Laura Grupp,

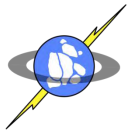
Joel Coburn, Ameen Akel, Steven Swanson

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



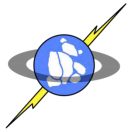
Motivation

- Flash memory has become ubiquitous
  - Laptops, phones, USB devices, SSDs
- Sensitive data is increasingly being stored in flash memory
- Ensuring the safety of our data is a top priority



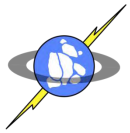
How Secure?

- Security is all about the amount of protection you need
  - Put another way:
    How much time, effort, and money will someone spend to get at your data?
- What data needs protecting?
  - Consumers
    - Sensitive personal information
  - Businesses
    - Legal data retention policies
    - Valuable business data
  - Government
    - top secret, classified data



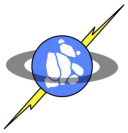
Hard Disks

- Secure erasure is not a new problem
- Much work has already been done for disks
  - Magnetic traces remain when data is overwritten
  - Erasure can be audited by inspecting the platters of a hard disk with an atomic force microscope
- Current solutions
  - SATA and SCSI commands for secure disk erasure
    - Must be correct and verified
  - Overwriting many times with specific patterns
  - Degaussing devices
  - Encryption and key protection



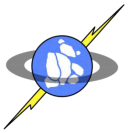
Technology Comparison

Hard Disks	Flash
• Special SATA/SCSI commands for erasure	• Proposed secure erase standards
• Encryption	• Encryption
• Multiple overwrites of same block	• Not possible with flash block address indirection
• Degaussing	• ?
• **Auditable – platter inspection with atomic force microscope**	• **Auditable? Perhaps with a nanoprober?**



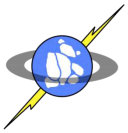
Flash Erasure Requirements

1. Ability to ensure the contents of a single file can be securely erased
2. Guarantee erasure of all blocks on a device
3. Ensure that recovering remnant analog data from the cells would be cost prohibitive
4. Auditable
   - Secure erase features infrequently used, but their proper functioning must be verifiable
   - What is the flash equivalent of pulling out a hard disk platter and looking for analog traces of data



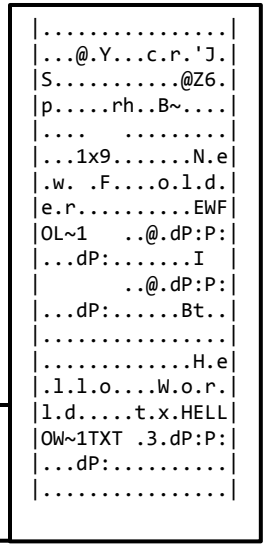
Consumer/Business Data Safety

- **Consumers and Businesses need a way to securely erase small bits of data from a device**
  - Remove personal information from a phone without losing all of the software, etc.
  - Delete a document from an SSD as part of a legal data retention requirement, without requiring reinstalling the operating system
- As with disks, simply deleting a file on a flash device is not enough
- On disks we can simply rewrite the contents of the file with zeros, but on flash its not so simple

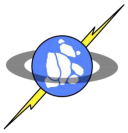


Erasing a Single File

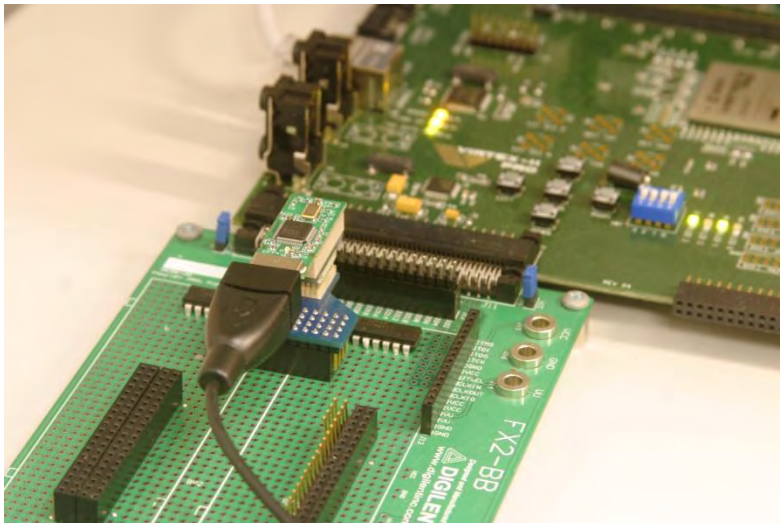
- Flash Translation Layers (FTL) make it impossible for higher level applications to know if a page of flash memory has been erased
  - FTLs remap the location of blocks of data to spread wear out across the device
  - Deleting or overwriting a file does not necessarily mean all of its pages have been overwritten
  - FTL and file system/operating system support will be necessary to securely erase single files



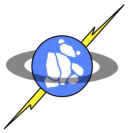
Old copy of file system metadata
Recovered by reading raw device



Auditing with the Flash Drag Tester

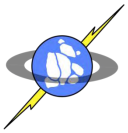


- Provides a real time trace of all of the commands and data sent to a set of flash chips
- Allows us to track the lifetime of a piece of data



Securely Erasing the Entire Device

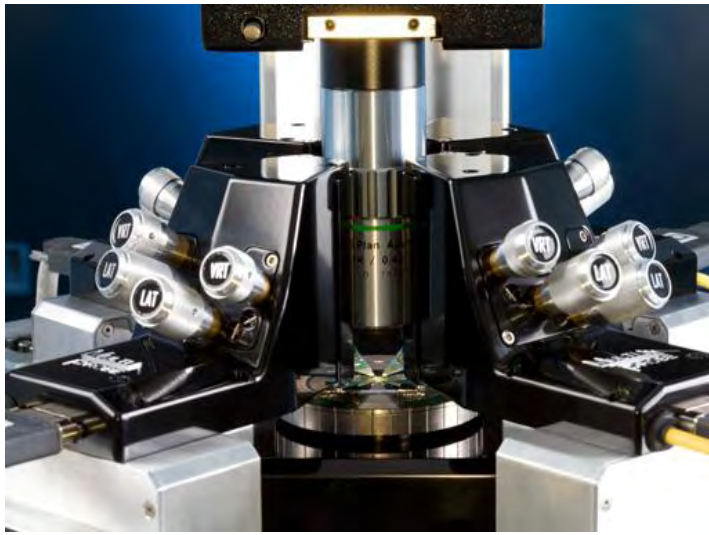
- Existing flash security and erasure standards propose that:
  - Security be provided by specific erase commands, overwriting data, or through cryptography
  - Whole device erases will continue, even after a power failure, until completed
- Auditability and verification should be a significant part of any future standards
  - As with hard disks this is a critical characteristic that can influence device selection



Physical Security

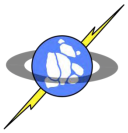
- Data security through the normal interface is adequate for most users, but physical security is important as well

- Can we audit to verify that even a nanoprober will not reveal anything about the past contents of the cells?
  - Similar to looking at platters with an atomic force microscope



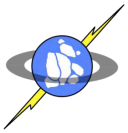
Current Flash Destruction Techniques

- Current techniques
  - Grinding up the chip into millions of pieces
  - Melting in acid
- These are done for disks as well
- Destruction tools must be fast and portable
  - As an example, embassies under siege and military forces need to be able to quickly destroy data
  - Transporting the device before destruction is a security risk



The Future

- An auditable, secure solution for the erasure of flash devices is needed
  - Standards are a good first step
  - Single file erasure is important too
  - Needs to pass physical probing as well
- A study of what can be recovered through physical probing of the cells would be valuable
  - something similar to disk platters with the atomic force microscope



Thank You

Questions?