A Secure Plausibly Deniable System for Mobile Devices against Multi-snapshot Adversaries

Bo Chen, Niusen Chen
Department of Computer Science, Michigan Technological University

Introduction

Mobile computing devices have been used broadly to store, manage and process critical data. To protect confidentiality of stored data, major mobile operating systems provide full disk encryption, which relies on traditional encryption and requires keeping the decryption keys secret. This however, may not be true as an active attacker may coerce victims for decryption keys. Plausibly deniable encryption (**PDE**) can defend against such a coercive attacker by disguising the secret keys with decoy keys. Leveraging concept of PDE, various PDE systems have been built for mobile devices. However, a practical PDE system is still missing which can be compatible with mainstream mobile devices and, meanwhile, remains secure when facing a strong *multi-snapshot* adversary.

Background

Flash Memory

- NAND flash
  - USB sticks
  - Solid state drives (SSDs)
  - SD/miniSD/microSD cards
  - MMC cards

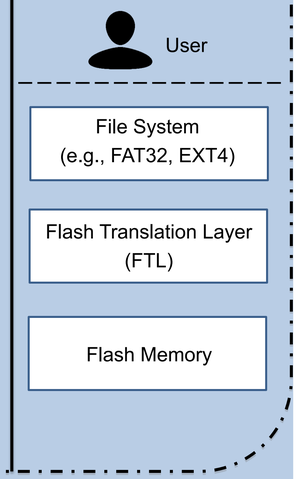
- NAND flash organization
  - Block (unit for erase operations)
  - Page (unit for read/write operations)

Special Characteristics of NAND Flash

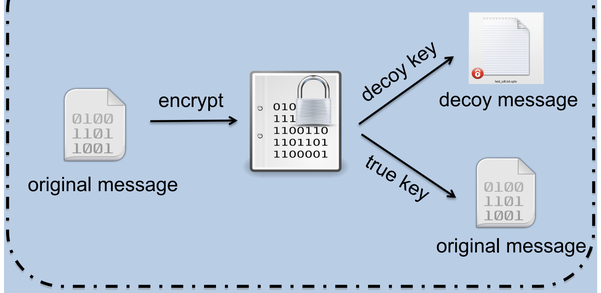
- Update unfriendly (out-of-place updates)
  - Over-writing data stored on a page requires first erasing the entire encompassing block
  - Writing is performed on a page basis, but erasure is performed on a block basis
- A limited number of program/erase (P/E) cycles
  - Each flash block can only be programmed/erased for a limited number of times (e.g., 10K)

How to use NAND Flash

- The most popular form of using flash memory is to emulate it as a block device
- This architecture is commonly found in flash memory cards like eMMC cards, SD cards
- Flash Translation Layer, FTL, is introduced between the block device and the raw flash
- FTL transparently handles unique nature of flash
- FTL implements special functions like garbage collection, wear leveling, and bad block management



Plausibly Deniable Encryption (PDE)



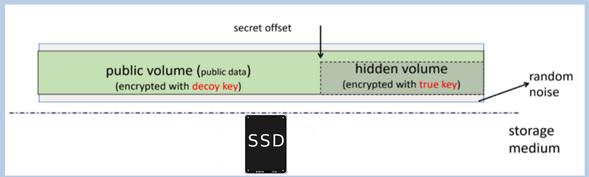
Adversarial Model

- Consider a computationally bounded adversary, which can have access to external storage of a victim mobile device at different points of time, i.e., a *multi-snapshot* adversary
- Each snapshot can be a physical image of raw NAND flash, obtainable by forensic data recovery tools [1]

Design

1. Public Volume & Hidden Volume

- Public volume:
  - Initialized with randomness
  - Encrypted with a decoy key
  - Store public non-sensitive data
- Hidden volume:
  - Stored at a secret location in the public volume
  - Encrypted with a true key
  - Store sensitive data



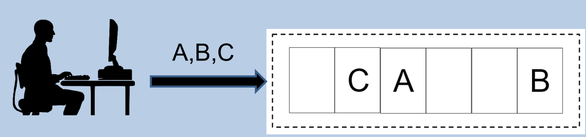
2. Dummy Writes

By comparing two snapshots captured, a multi-snapshot adversary may notice changes among randomness caused by hidden data writes [2]. To avoid this deniability compromise:

- Upon writing the public volume, the FTL will perform additional dummy writes of random data
- The hidden data writes can be denied as the dummy writes

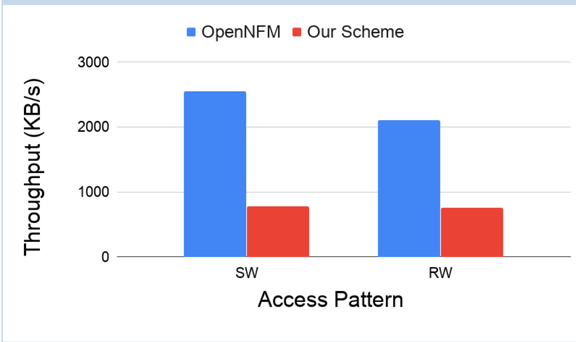
3. Random Writes

- Deniability may be comprised due to conventional log-structured writing used in FTL
- Use random writing to replace log-structure writing, which is exclusively feasible for NAND flash



Preliminary Results

- Implemented random writing and dummy writes into an open-source NAND flash controller framework, OpenNFM
- Ported the prototype to LPC-H3131, an electronic development board equipped with 180MHz ARM micro-controller, 512MB SLCNAND flash
- Used another embedded board, Firefly AIO-3399J, as a host device to read/write the external flash storage provided by LPC-H3131via a USB interface
- A benchmark tool “fio” was run in the host device to assess the write throughput



SW: Sequential Write; RW: Random Write

Acknowledgments

This work was supported by National Science Foundation under grant number 1928349-CNS and 1938130-CNS.

References

[1] M. Breeuwsma, M. D. Jongh, C. Klaver, R. V. D. Knijff, and M. Roeloffs. Forensic data recovery from flash memory. Small Scale Digital Device Forensics Journal, 1(1):1–17, 2007.

[2] B. Chang, F. Zhang, B. Chen, Y. Li, W. Zhu, Y. Tian, Z. Wang, and A. Ching. Mobiceal: Towards secure and practical plausibly deniable encryption on mobile devices. In DSN, pages 454–465. IEEE, 2018.