MobiCeal: Towards Secure and Practical Plausibly Deniable Encryption on Mobile Devices

Bing Chang, Fengwei Zhang, Bo Chen, Yingjiu Li, Wen-Tao Zhu, Yangguang Tian, Zhan Wang and Albert Ching

Presented by : Tanzeer Hossain

Outline

- Introduction
- Background
- Threat model and assumptions
- MobiCeal Design
- Performance Evaluation
- Conclusion

Introduction

- Plausibly Deniable Encryption

  describes encryption techniques where the existence of an encrypted file or message is deniable in the sense that an adversary cannot prove that the plaintext data exists.

- Such denials may or may not be genuine.

Introduction cont.

- Traditional encryption systems does not work well in situations where device owner is captured by the adversary and forced to compromise the encryption key.
- Plausible Deniable Encryption (PDE) scheme can defend this kind of attack.
- Existing PDE solutions for mobile devices have few shortcomings.
  I. Not resilient against attacks where an adversary obtains storage snapshot at different point of time.
  II. Needs to reboot before using PDE functions.

Introduction cont.

- Existing PDE systems that work against multi snapshot adversaries also have few limitations.
  - Unsuitable for mobile environment due to performance overhead. Hive and DataLiar uses write-only oblivious RAM (ORAM) which has poor I/O performance.
  - Vulnerable to side channel attack. HIVE and DEFY do not isolate hidden and public data sufficiently.
  - Not large scale deployable. For example, DEFY is heavily dependent on a specific file system.

Background

- Full-disk encryption (FDE)
  - Full-disk encryption (FDE) is encryption at the hardware level. FDE works by automatically converting data on a hard drive into a form that cannot be understood by anyone who doesn’t have the key to “undo” the conversion.

Background cont.

Plausibly Deniable Encryption

- Two types of techniques are used.
- Hidden volumes technique
  - Two encrypted volumes on the disk.
  - Public volume: encrypted using decoy key.
  - Hidden volume: encrypted using hidden key.

- Steganographic file systems
  - Hide sensitive data among regular file data.
  - Can be achieved by introducing large number of cover files or hiding data into abandoned/dummy file blocks.

Background cont.

- Logical Volume Manager (LVM)
  - LVM is a toolset that provides logical volume management capabilities in Linux.
  - LVM introduces three concepts.
    - Physical volumes (PV) : partitions or entire disk can be initialized as Physical volume
    - Volume Groups (VG) : Physical volumes are combined into volume groups
    - Logical Volumes (LV) : A volume group can be divided into logical groups.

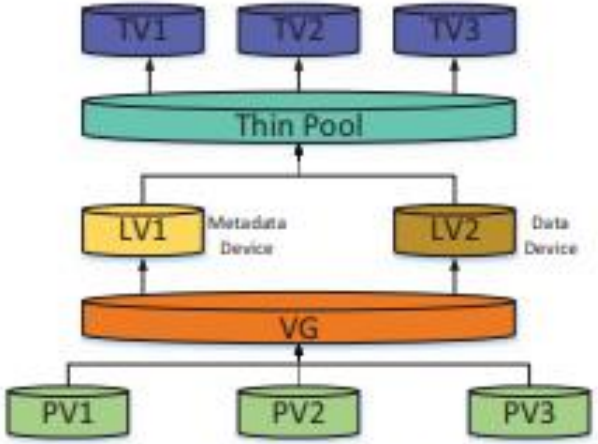
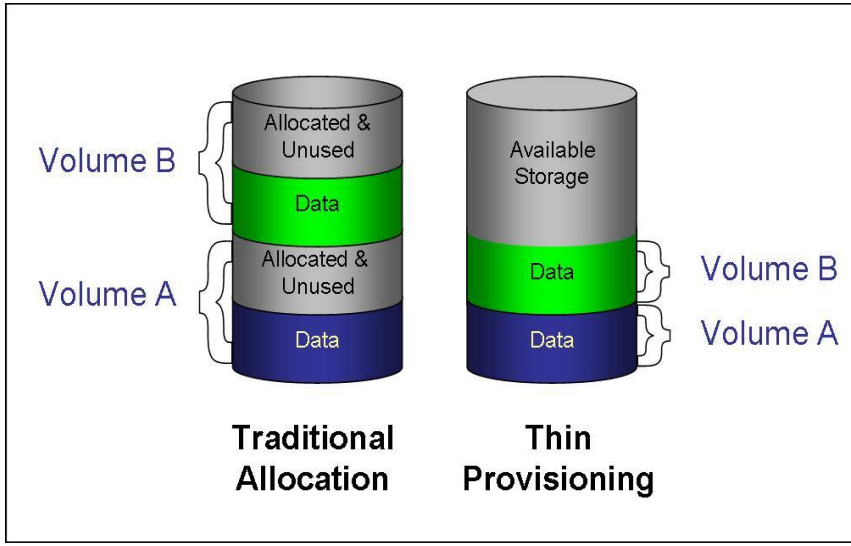


Fig. 1. LVM and thin provisioning architecture.

Background cont.

Thin Provisioning

- involves using virtualization technology to give the appearance of having more physical resources than are actually available.
- Two logical volumes are needed.
  1. Data device: stores the data blocks.
  2. Meta Data device: stores the space bitmap and the block mappings for thin volumes.



Source: http://wikibon.org

Threat Model and Assumptions

- Adversary can obtain multiple snapshots of the storage device.
- Adversary can have full knowledge of MobiCeal's design.
- Adversary will not capture the device when owner is using PDE functions.
- Adversary will not continue coercing owner when he is convinced encryption keys have been disclosed.
- MobiCeal code will be merged with android code stream.
- The mobile OS, kernel, bootloader, firmware, all the apps and baseband OS are malware free.

MobiCeal Design

- Limitations of existing PDE in mobile devices :
  - Vulnerable to multi-snapshot adversary.
  - Attacker is dynamic, but defense is static
  - Needs dynamic defense to encounter dynamic attack.
- Limitations of dynamic defense based PDE in mobile devices :
  - Expensive in computation and I/O.
  - Designed for more dynamic attacker than our threat model.

MobiCeal Design

- Uses dummy write approach.
- Perform additional artificial writes of randomness.
- Unaccountable changes in random data can be described using dummy writes.
- Number of dummy writes follows exponential distribution.
- Dummy data is created using same encryption algorithm as the hidden data.

MobiCeal Design

- Creates a global bitmap to track blocks allocated for public, hidden and dummy data.
  - Sequential allocation may lead to overwrite issue.
- Current design is still vulnerable to attack when there is occasional large file written in the hidden volume.
  - Adversary may observe that public volume is followed by a large amount of randomness.

MobiCeal Design

- Three types of virtual volumes.
- **Public Volume:** Public volume is encrypted using decoy key via FDE. It is used for daily operations.
- **Hidden Volume:** Public volume is encrypted using hidden key via FDE. Hidden volume is used to store sensitive data.
- **Dummy Volume:** Stores dummy data created by dummy writes. Purpose is to obfuscate the existence of hidden volume.

Block Allocation Strategy in Block layer

- MobiCeal uses random block allocation in the block layer.
- Sequential allocation may compromise deniability.

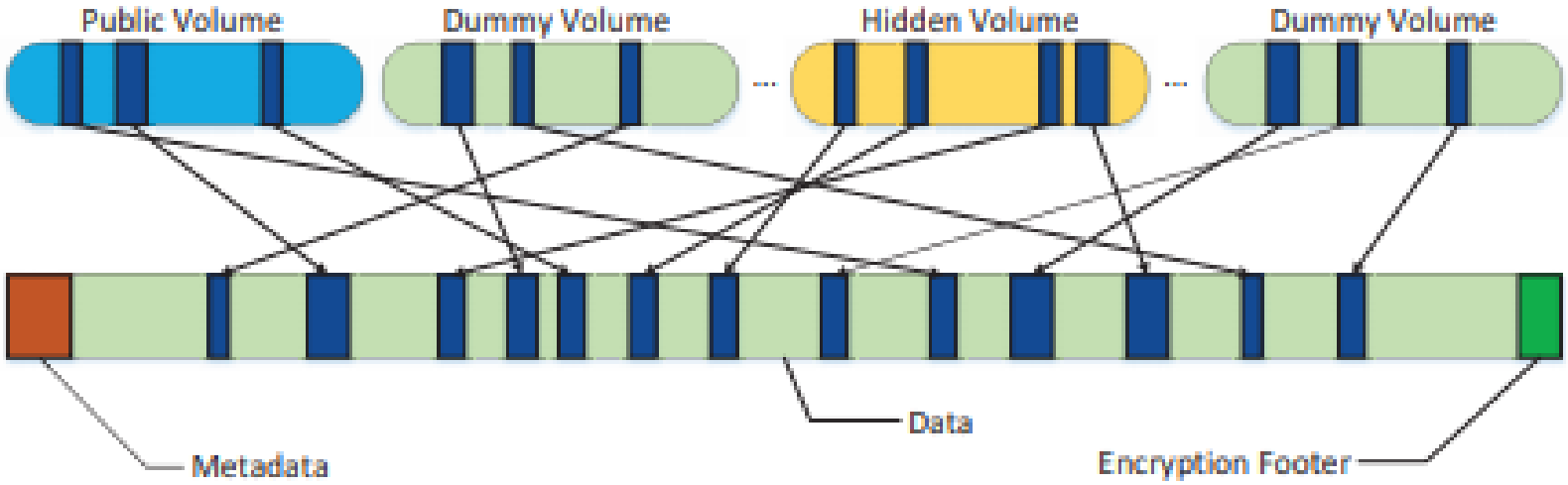
$$D_{v_2}||D_{v_1}||D_{v_2}||D_{v_2}||D_{v_2}||D_{v_2}||D_{v_2}||D_{v_2}||D_{v_2}||D_{v_1}$$

Dv1 represents data blocks allocated for public volume and ***Dv2*** represents data blocks allocated to hidden volume.

- If adversary observe that seven data blocks are allocated for dummy writes between two data blocks for public voulume, he may suspect the existance of hidden volume.
- It may happen if large file is written in the hidden volume.

Storage Layout

- The entire disk is divided into three parts.
- Meta Data: stores information of the virtual volumes (global bitmap, sizes and mappings of virtual bitmap)
- Data : Stores the data block for the virtual volumes.
- Encryption Footer: Encrypted decopy key and salt are stored.

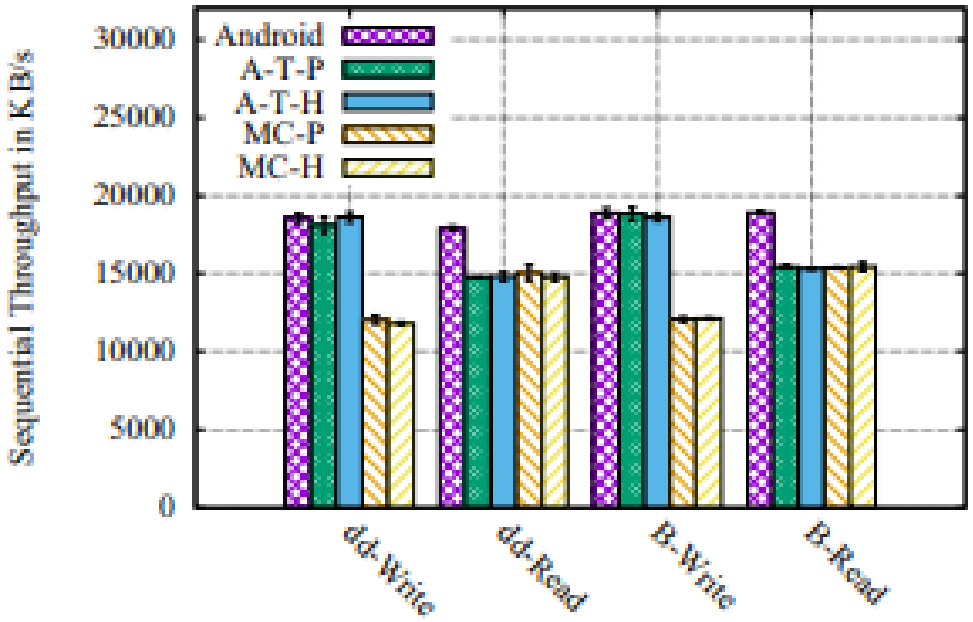


Side Channel Attacks

- Existing PDE system (e.g., HIVE and DEFY) vulnerable to side channel attacks.
- MobiCeal guards four possible leakage paths for side channel attacks.
- The public volume, logs at /devlogs, /cache and RAM are four possible leakage paths.
- To prevent side channel attacks, when hidden password is confirmed, the MobiCeal system unmounts three partitions and mounts two tmpfs RAM disks to /devlog and /cache.
- To make sure that RAM is cleared after using hidden volume, reboot is mandatory for switching to public volume.

Performance Evaluation

- Throughput Performance



Performance Evaluation

- Overhead Comparison

TABLE I

OVERHEAD COMPARISON. THE VALUES OF DEFY ARE FROM THE FIGURE 6 IN [33]. TEST ENVIRONMENT: DEFY: UBUNTU 13.04, SINGLE PROCESSOR, 4GB RAM, SIMULATED FLASH DEVICE; HIVE: ARCH LINUX X86-64, I7-930, 9GB RAM, SAMSUNG 840 EVO SSD; MOBICEAL: ANDROID 4.2.2, SNAPDRAGON APQ 8064, 2GB RAM, NEXUS 4 INTERNAL STORAGE.

	Ext4 (MB/s)	Encrypted (MB/s)	Overhead
DEFY	800	50	93.75%
HIVE	216.04	0.97	99.55%
MobiCeal	19.5	15.2	22.05%

Performance Evaluation

- Timing Measurement

TABLE II
INITIALIZATION TIME, BOOTING TIME, AND SWITCHING TIME.

	Initialization	booting time (decoy pwd)	switching time (enter hid-mod)	switching time (exit hid-mod)
Android FDE	18min23s±1s	0.29±0.02s	N/A	N/A
MobiPluto	37min2s±2s	1.36±0.02s	68±4s	64±5s
MobiCeal	2min16s±3s	1.68±0.04s	9.27±0.28s	63±6s

Conclusion

- MobiCeal is first block layer PDE scheme that is resilient to multi-snapshot adversaries in mobile devices.
- It is file system friendly and supports first switching.
- Performance overhead is significantly lower comparing to other existing PDE solutions.

Thank You