Plausibly Deniable Encryption Systems for Mobile Devices

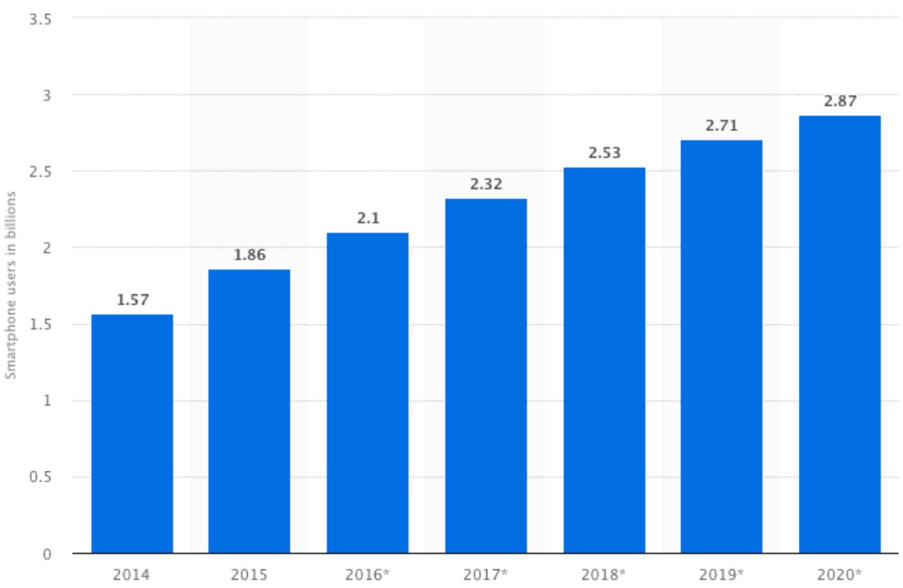
Niusen Chen

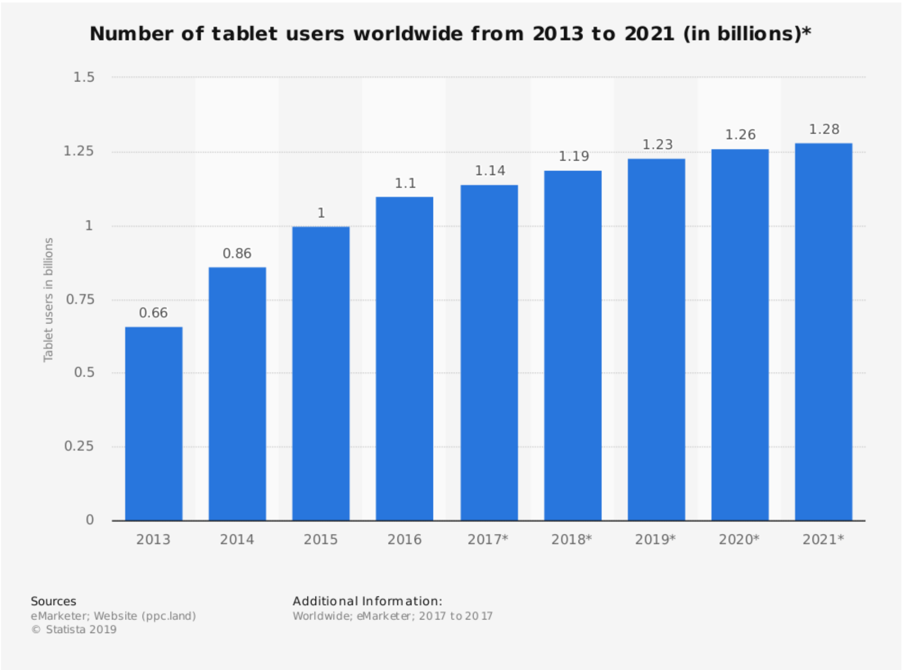
Department of Computer Science

Michigan Technological University

niusenc@mtu.edu

Mobile Devices are Turning to Mainstream Computing Devices

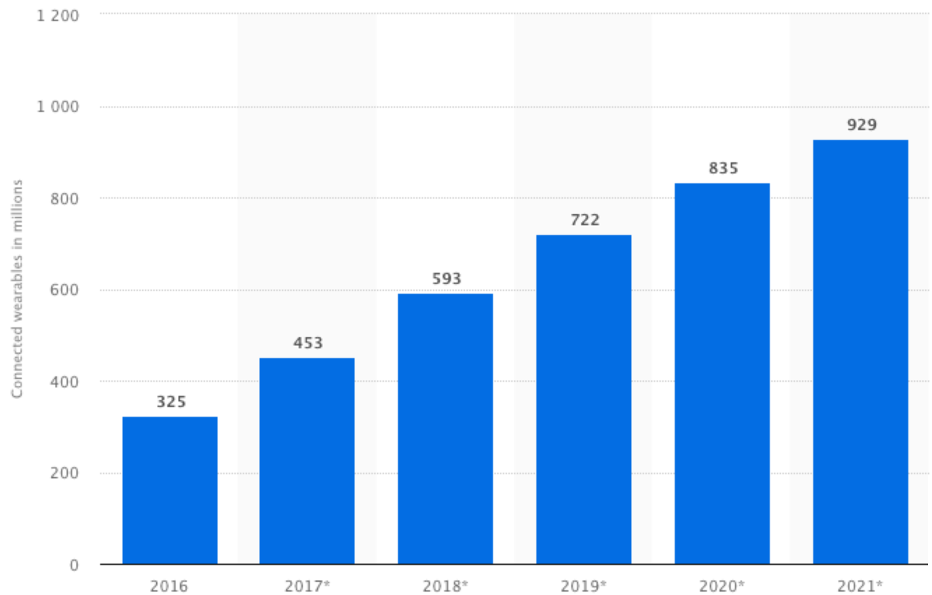




Number of smartphone users worldwide from 2014 to 2020 (in billions)

Number of tablet users worldwide from 2013 to 2021 (in billions)

Mobile Devices are Turning to Mainstream Computing Devices (cont.)



Number of connected wearable devices worldwide from 2016 to 2021 (in millions)

Mobile Devices Are Increasingly Used for Critical Applications

- Mobile devices are increasingly used to handle sensitive data
  - Online banking
  - Ecommerce
  - Cryptocurrency/stock trading
  - Etc.

- Security issues in mobile computing devices
  - Confidentiality
  - Integrity
  - Authentication
  - Access control

Full Disk Encryption (FDE)

1. Everything on disk is encrypted
2. Totally transparent to users
3. Can not defend against coercive attack

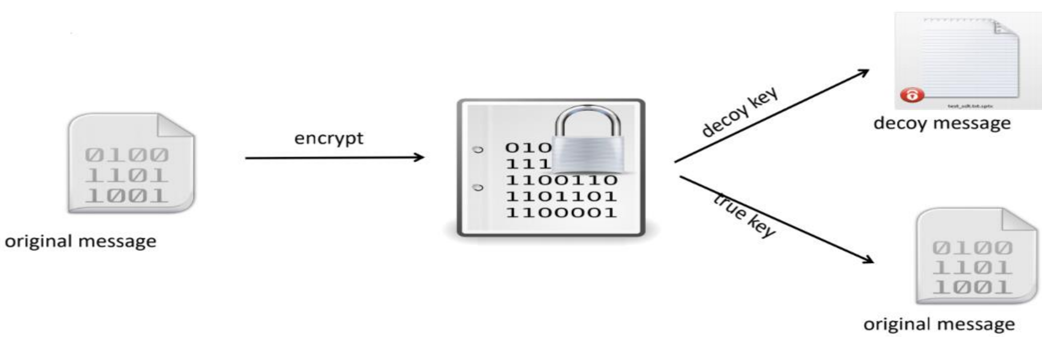
Coercive Attack

An attacker forces the device owner to disclose the decryption key

FDE is vulnerable to a coercive attack

Plausibly Deniable Encryption (PDE)

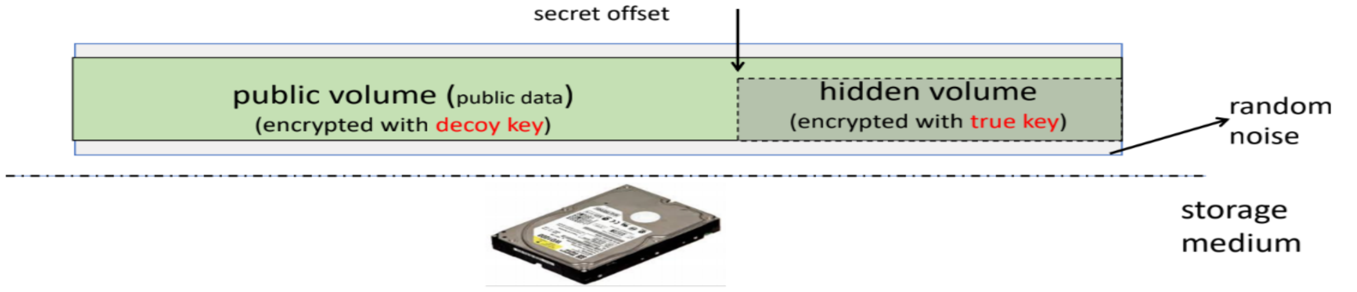
- A crypto primitive designed for mitigating coercive attacks
- Plain-text is encrypted by a true key and a decoy key such that:
  - Decrypt with decoy key → Decoy message
  - Decrypt with true key → True message
- Upon being coerced: disclose decoy key, keep true key
- PDE is hard to be achieved in crypto
- Two techniques to simulate PDE
  - Hidden volume technique
  - Steganography technique



PDE Technique

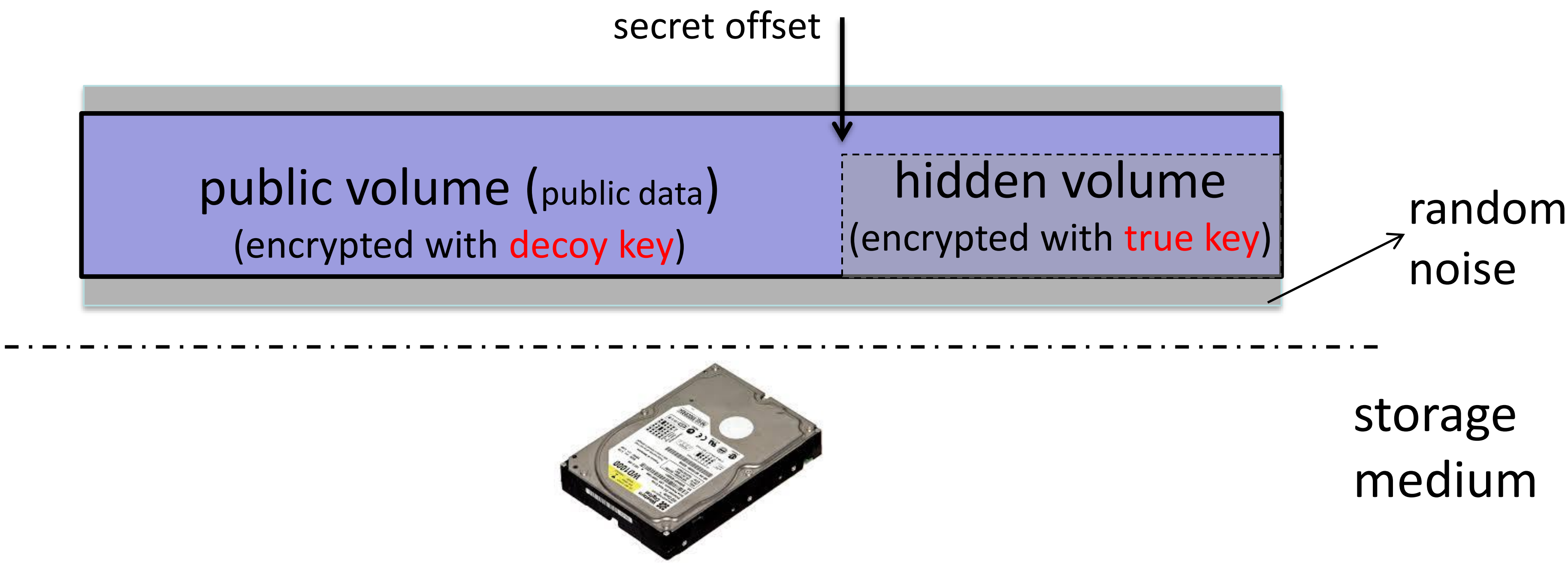
Hidden Volume Technique

- The entire disk is initialized with randomness
- Two volumes: public volume and hidden volume
  - Public volume: encrypted with a **decoy** key; store non-sensitive data
  - Hidden volume: encrypted with **true** key; store sensitive data
- Disclosing the decoy key upon being coerced by attacker



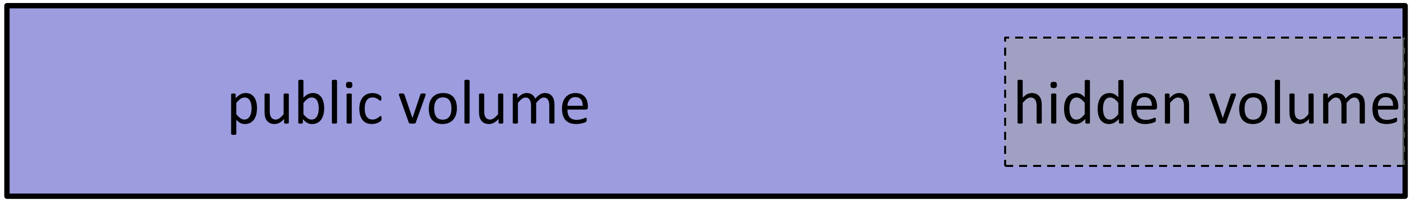
Implementing PDE in Systems - Hidden Volume

- Hidden volume [TRUECRYPT ’04] realizes the concept of PDE in systems
  - Only the decoy key will be disclosed
  - The encrypted hidden volume cannot be differentiated from the random noise



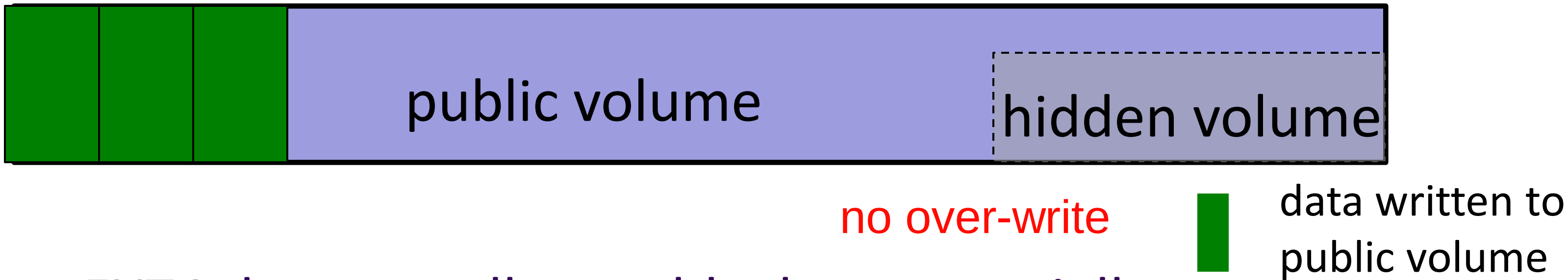
The Challenges: Over-writing Issues

- The data written to the public volume may over-write the data in the hidden volume
  - The hidden volume is part of the public volume

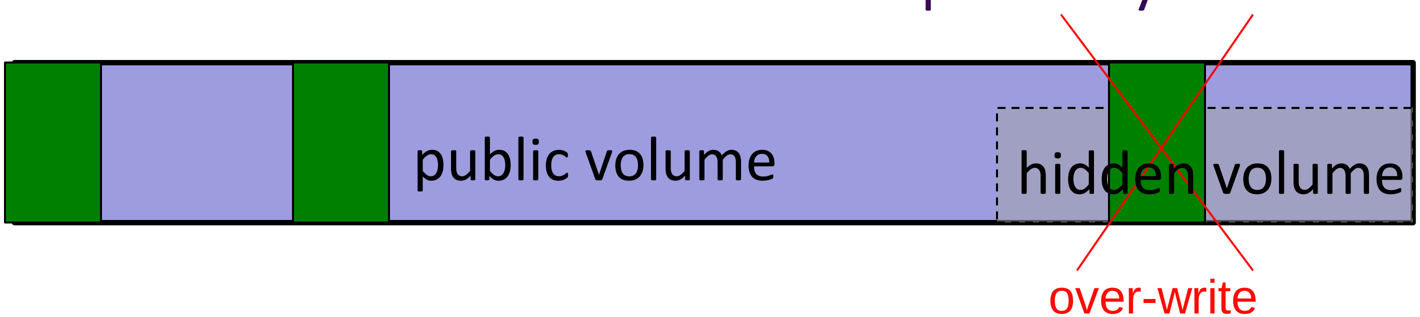


The Challenges: Over-writing Issues (cont.)

- File systems really matter for over-write issues
  - FAT allocates blocks sequentially



  - EXT4 does not allocate blocks sequentially

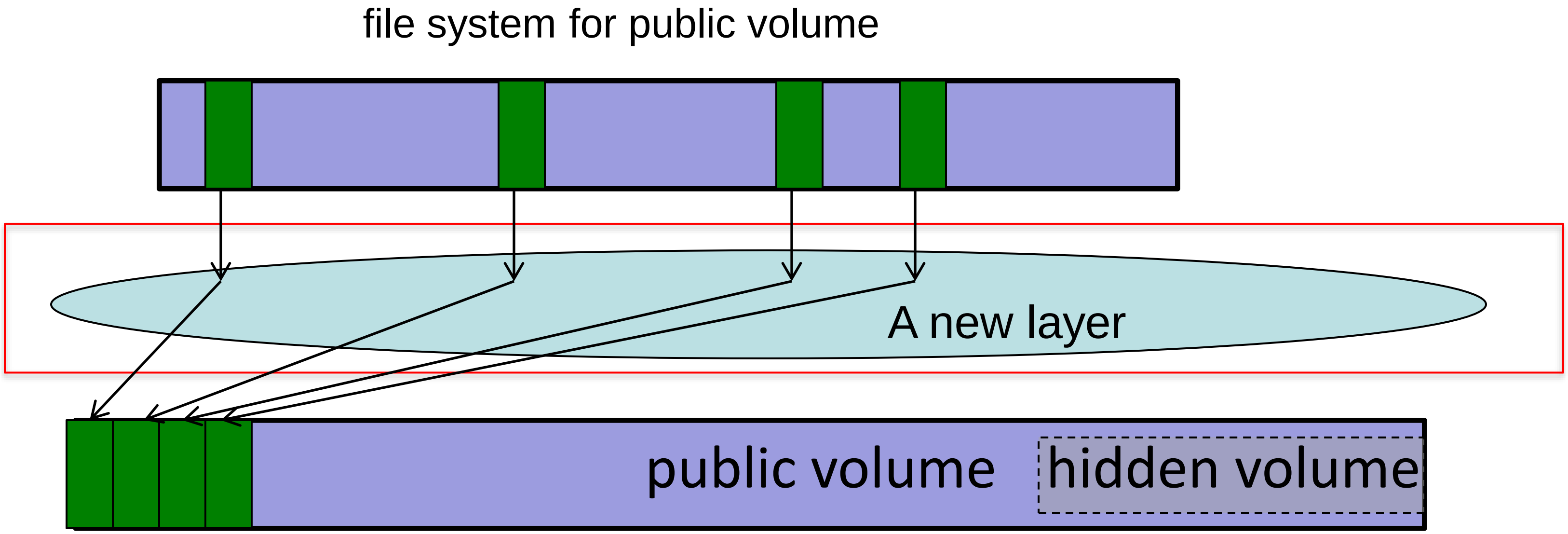


It is challenging to allow any file systems to be deployed while mitigating the over-write issues

MobiPluto – Key Insights [ACSAC ’15]

To realize **file system friendly** design, a new layer is introduced to decouple the file system and the underlying PDE system

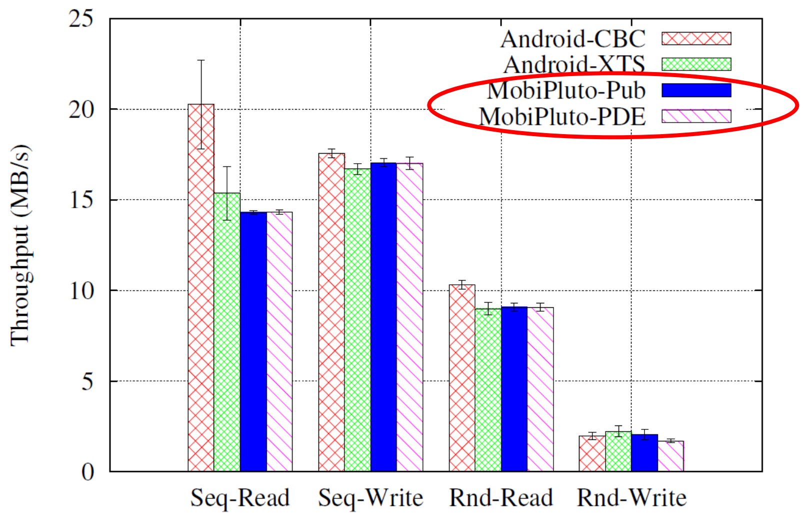
1. Provide virtual volumes to file systems
2. Any block-based file system can be built on a virtual volume
3. Non-sequential allocation on the virtual volume will be converted to sequential allocation on the underlying layer



Bing Chang, Zhan Wang, **Bo Chen**, and Fengwei Zhang. MobiPluto: File System Friendly Deniable Storage for Mobile Devices. 2015 Annual Computer Security Applications Conference (ACSAC '15), Los Angeles, California, USA, December 2015 (Acceptance rate: 24.4%)

Evaluation Highlights

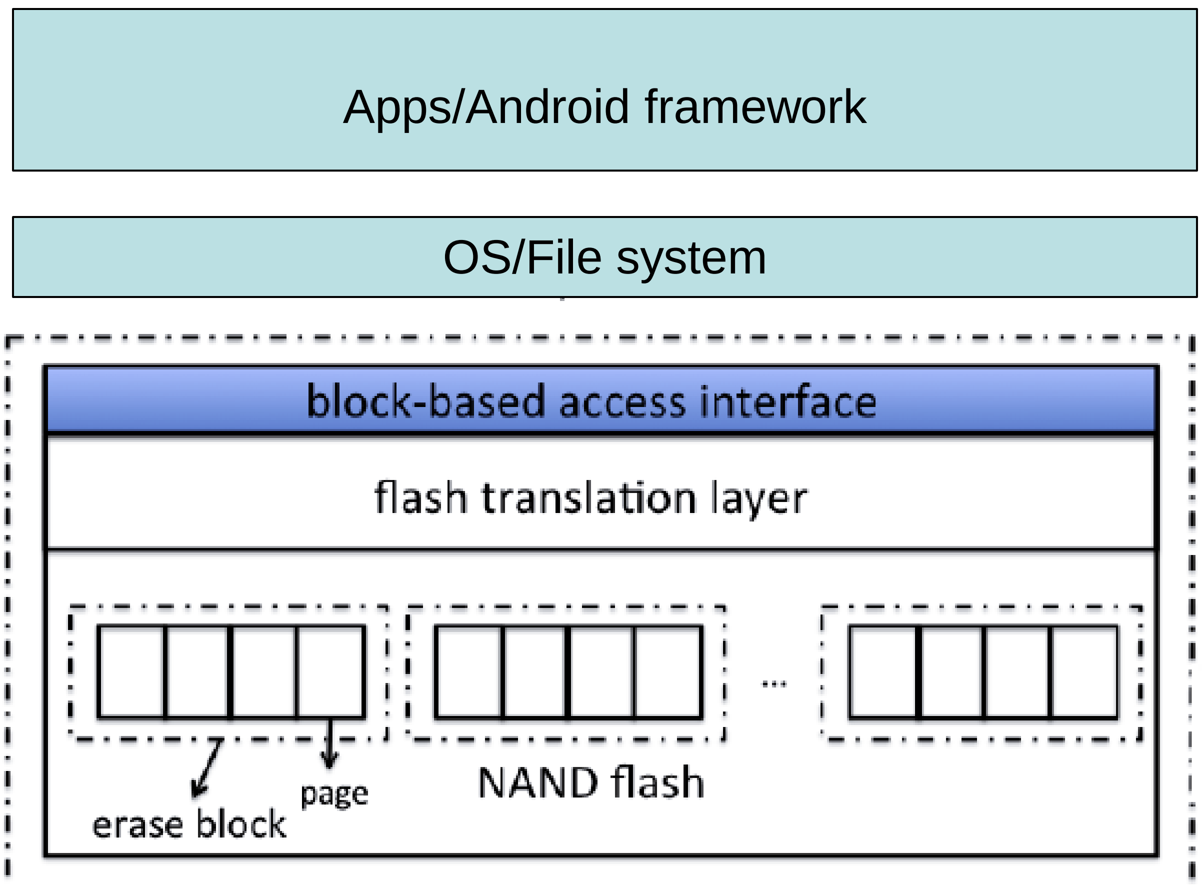
- Implemented a prototype of our solution on LG Nexus 4



Throughput (MB/s) from AndroBench

Deniability Compromise at Lower Storage Layer?

Existing deniable storage systems (e.g., MobiPluto)



deniability compromise

Flash storage (eMMC card/SD card)

A Main-stream Storage Architecture for Mobile Devices

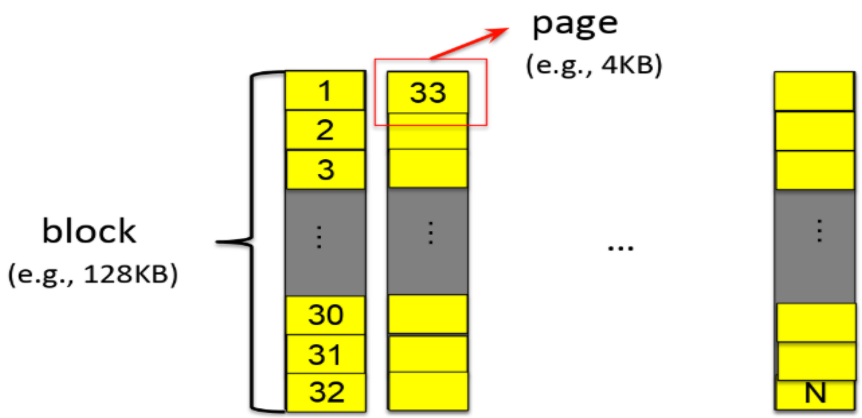
Hardware Characteristics of Flash Memory

Read/Write on pages, but erase on blocks

Erase-before-write

Out-of-place update

Limited number of program-erase(P/E) cycles



Special Functions Incorporated into Flash Storage Device

Garbage Collection: Blocks containing too many invalid pages will be reclaimed by copying valid data out of them, and the reclaimed blocks will be placed to free block pool to be reused

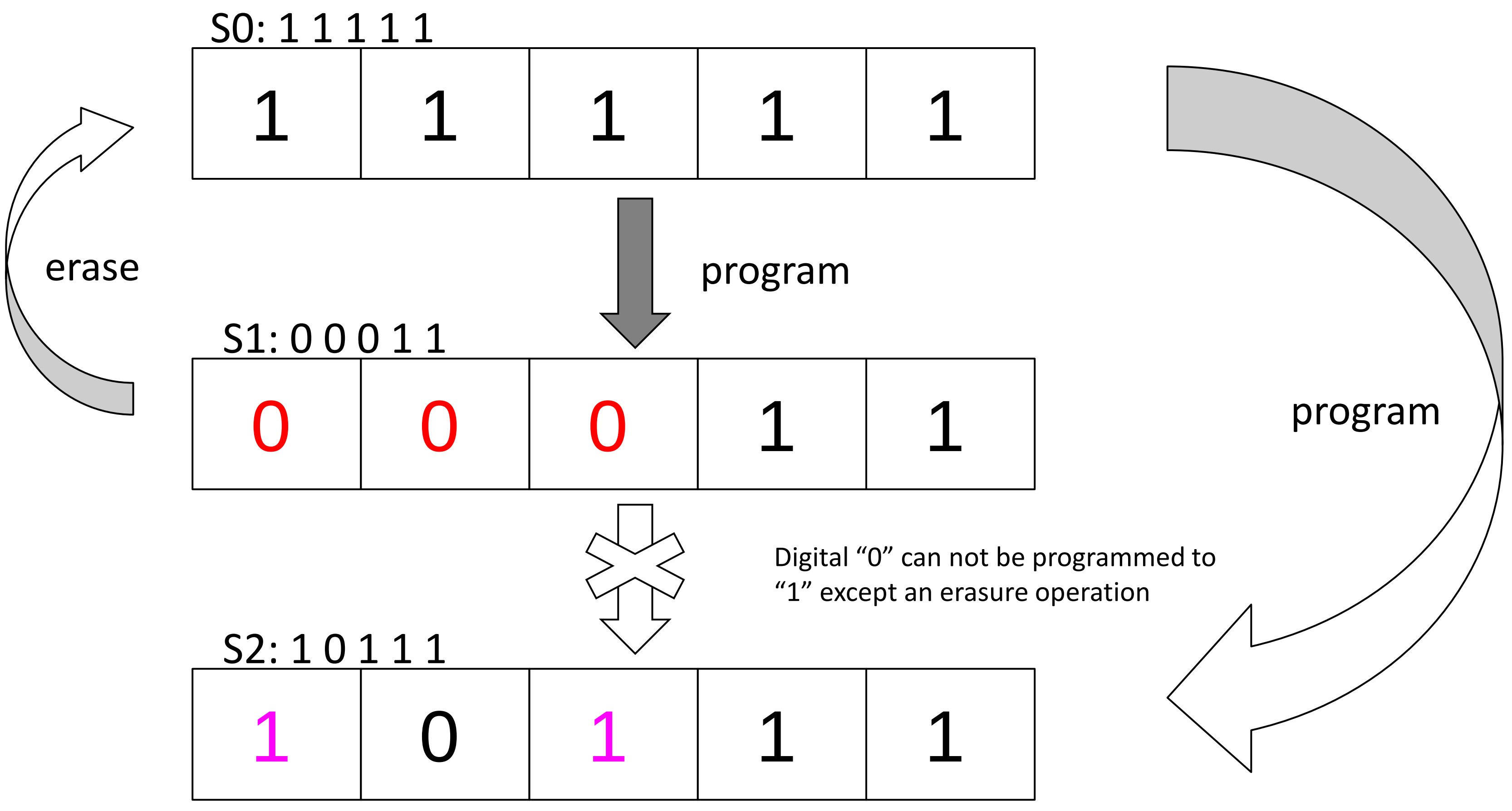
Wear Levelling: Distribute writes/erasures evenly across flash memory

Bad Block Management: Bad block management typically introduces a bad block table to keep track of bad blocks. Once a block turns bad, it will be added to the bad block table and will no longer be used

How to Program Data to Flash Memory

Three rules:

- Initially, what in flash memory are all digital “1”s
- Digital “1” can be programmed to digital “0” (write operation)
- Digital “0” cannot be programmed to “1” except a block erasure operation


S0: 1 1 1 1 1
1 1 1 1 1
program
S1: 0 0 0 1 1
0 0 0 1 1
erase
program
Digital “0” can not be programmed to
“1” except an erasure operation
S2: 1 0 1 1 1
1 0 1 1 1

How to Use Flash Memory

File System
(FAT,EXT)

Flash Translation Layer
(FTL)

Flash Memory

Method 1: FTL

Flash-specific File System
(YAFFS, UBIFS)

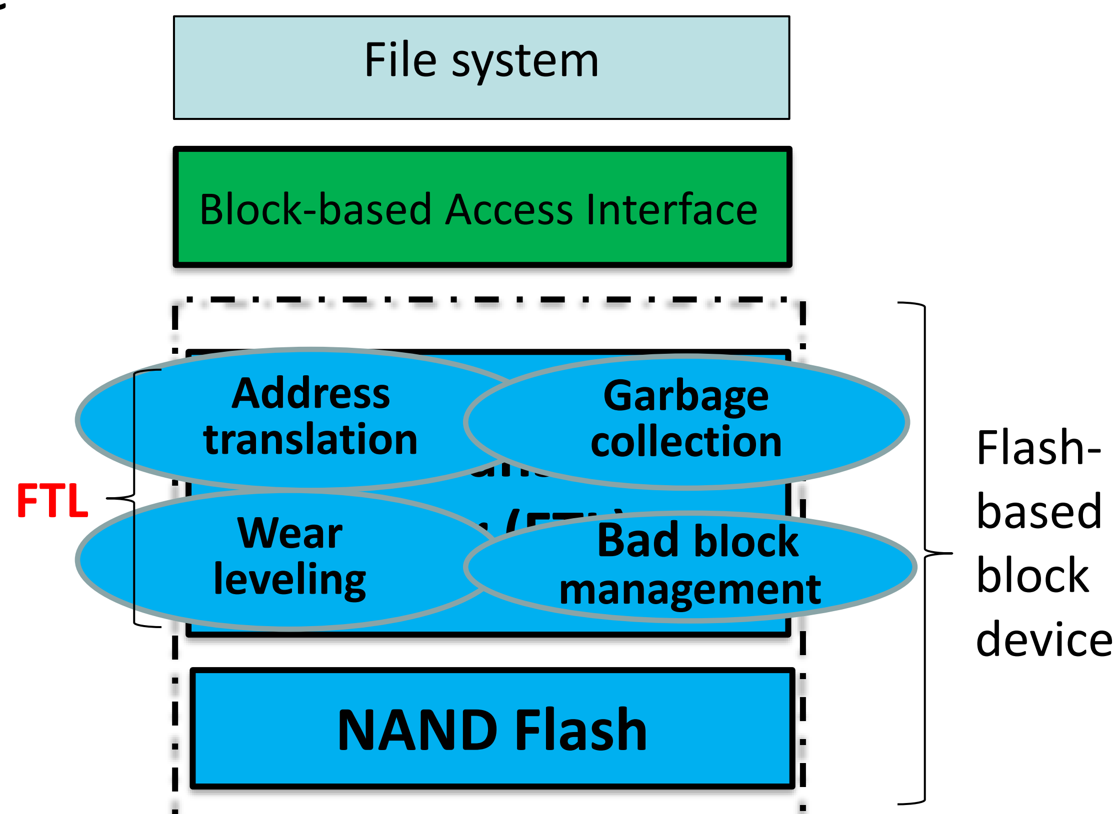
Flash Memory

Method 2: Flash File System

Flash Translation Layer (FTL)

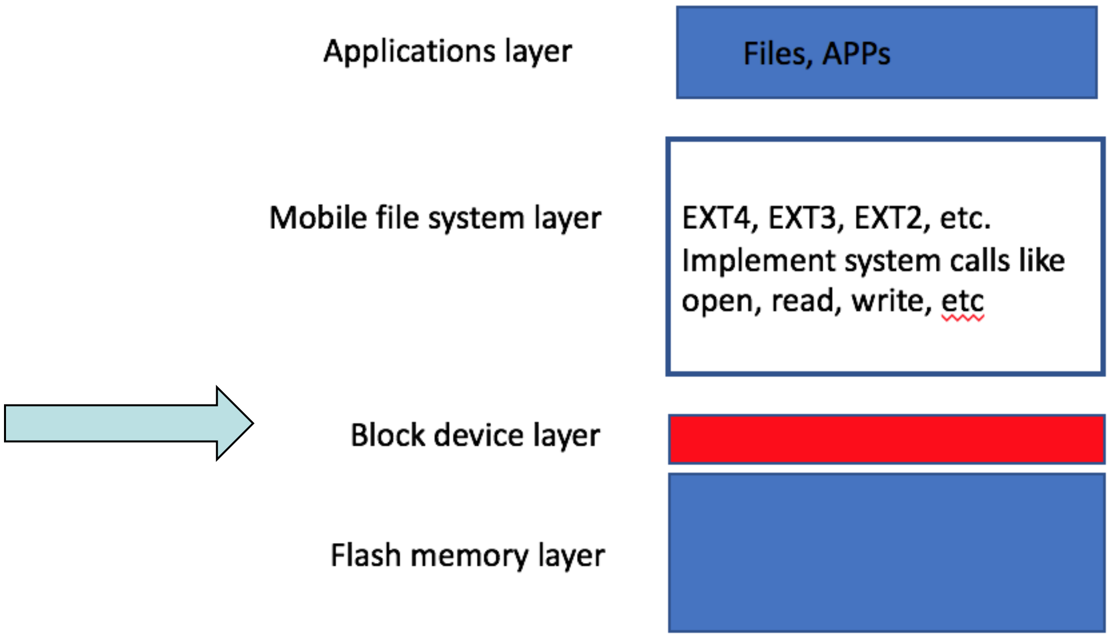
FTL usually provides the following functionality:

- ✓ Address translation
- ✓ Garbage collection (GC)
- ✓ Wear leveling (WL)
- ✓ Bad block management

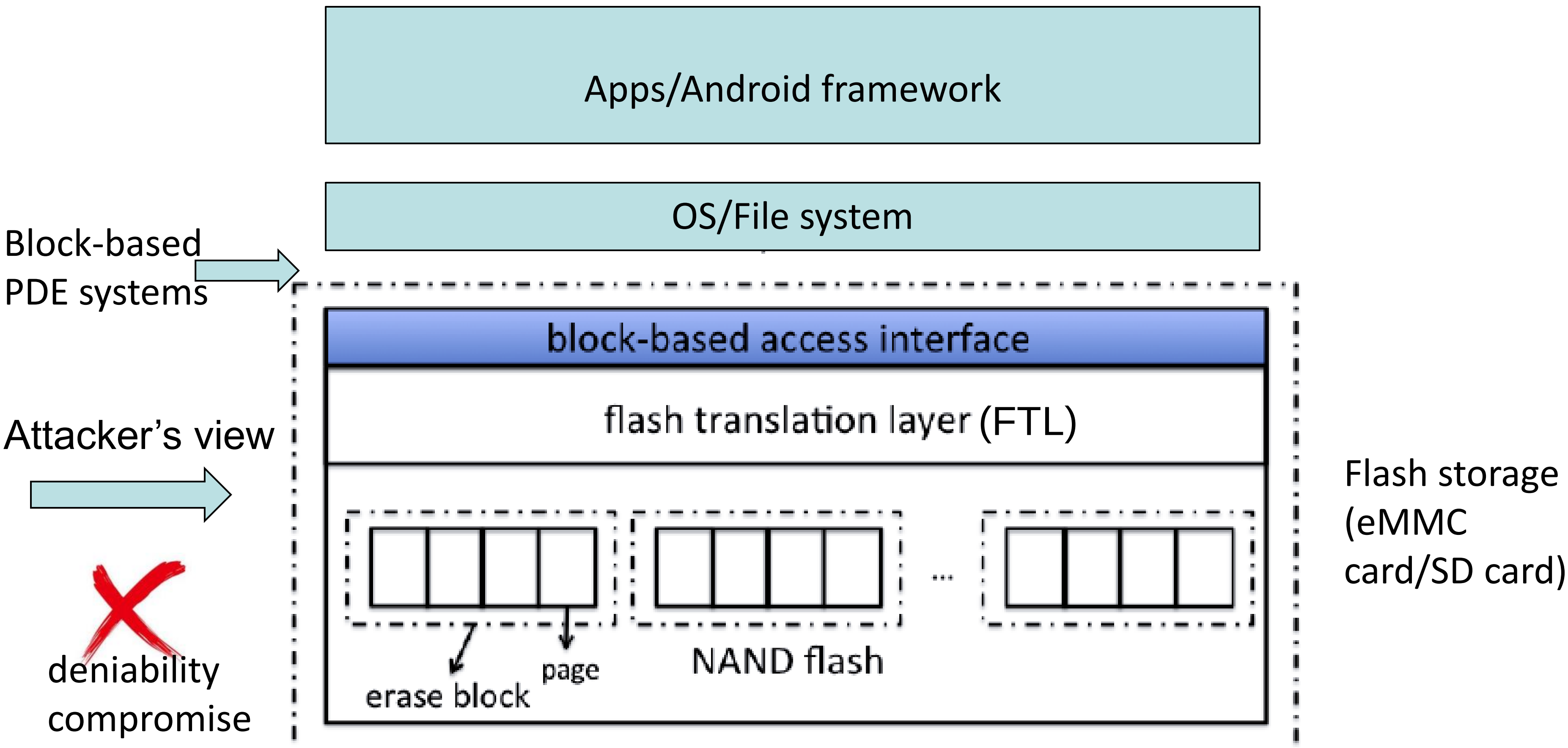


Existing PDE Systems for Mobile Devices

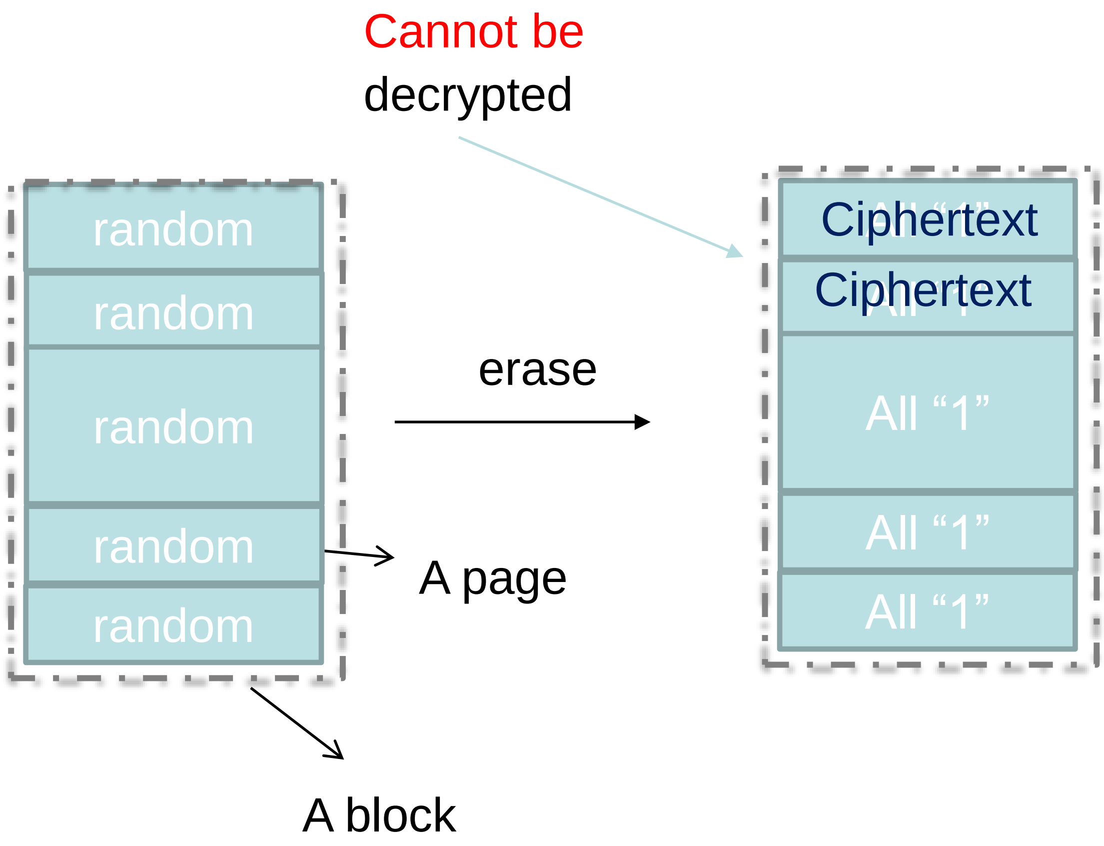
- Most of the existing PDE systems deploy hidden volume on top of the block device
  - Mobiflage [Skillen et al., NDSS ’13]
  - MobiHydra [Yu et al., ISC ’14]
  - MobiPluto [Chang et al., ACSAC ’15]
  - MobiCeal [Chang et al., DSN ’18]



Deniability May be Compromised When Deploying Hidden Volume on The Block Layer

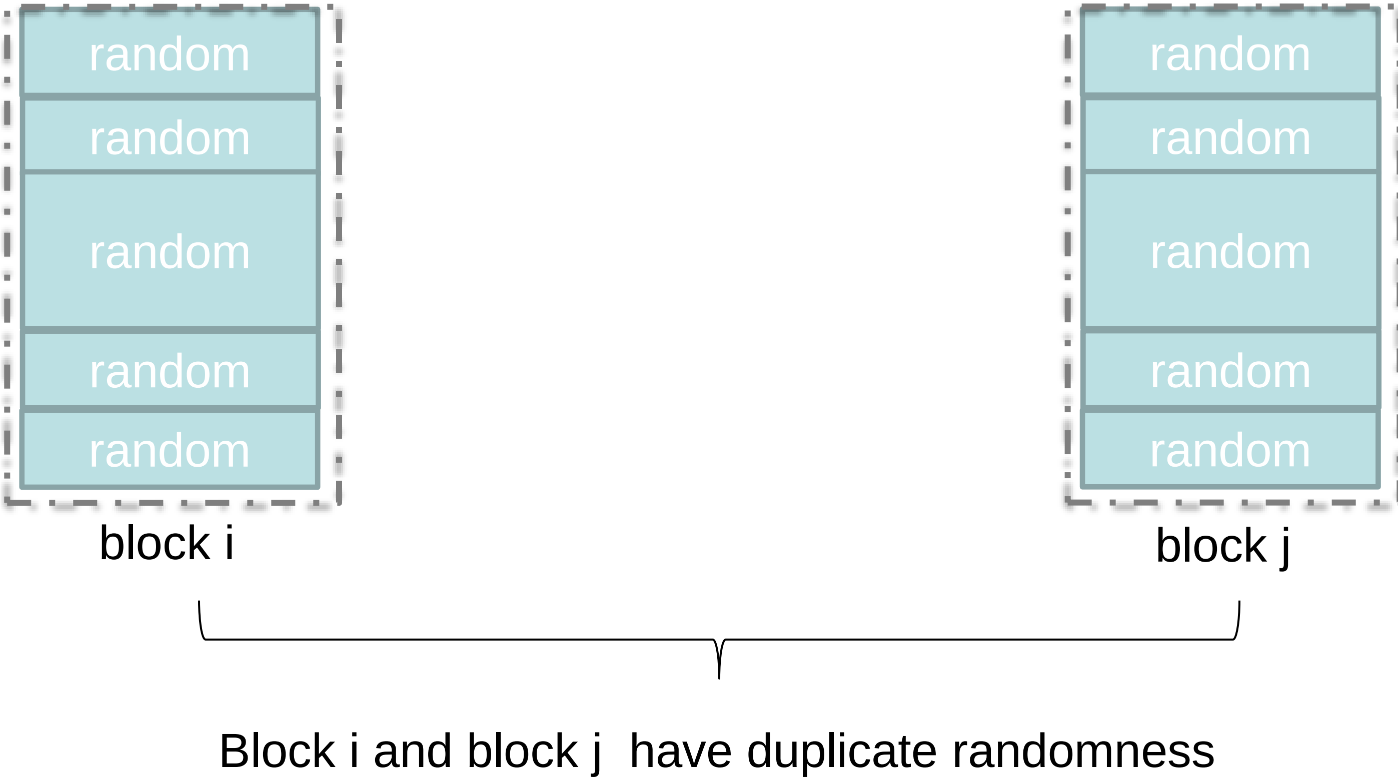


Compromise of Existing PDEs Built on top of the block device (1)



A flash block partially used by the hidden volume

Compromise of Existing PDEs Built on top of the block device (2)

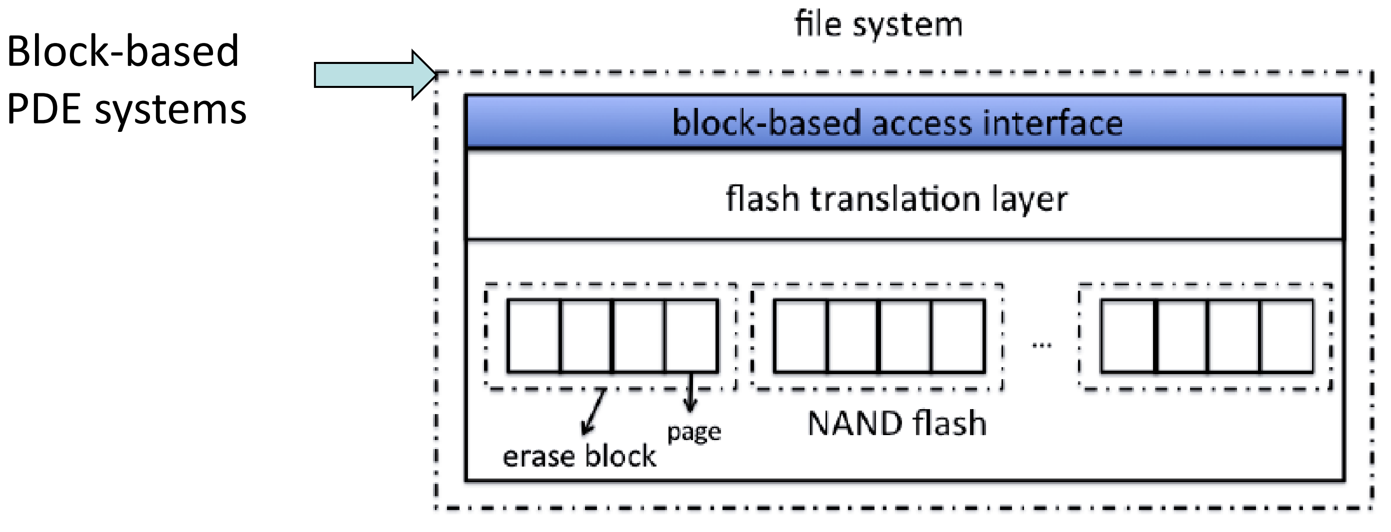


Special flash memory operations (wear leveling, garbage collection, bad block management) on the hidden volume will create duplicate randomness

Shijie Jia, Luning Xia**, Bo Chen**, and Peng Liu. DEFTL: Implementing Plausibly Deniable Encryption in Flash Translation Layer. 2017 ACM Conference on Computer and Communications Security (CCS '17), Dallas, Texas, USA, Oct 30 - Nov 3, 2017 (Acceptance rate: 18%)

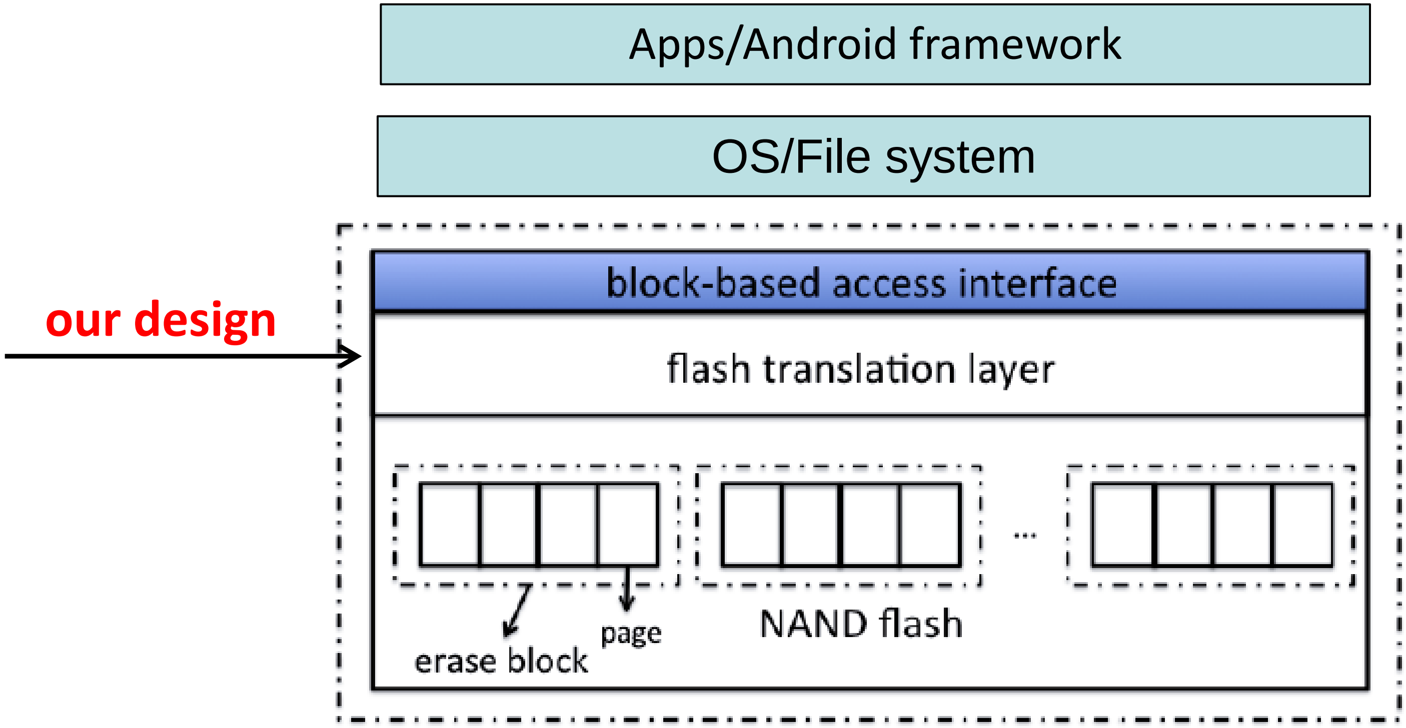
Fundamental Reasons for Compromises of The Existing Block-based PDE Systems

- Built on top of block device (outside the black box of flash memory), and cannot manage the internal flash memory
- Unexpected ``traces'' of hidden sensitive data could be created in the flash memory which is out of the control of the block-based PDE



FTL-based PDE System [CCS ’17]

Key insight 1: move the public/hidden volume design down to the flash translation layer (FTL) and strictly isolation them.



Shijie Jia, Luning Xia**, Bo Chen**, and Peng Liu. DEFTL: Implementing Plausibly Deniable Encryption in Flash Translation Layer. 2017 ACM Conference on Computer and Communications Security (CCS '17), Dallas, Texas, USA, Oct 30 - Nov 3, 2017 (Acceptance rate: 18%)

Our FTL-based PDE System (cont.)

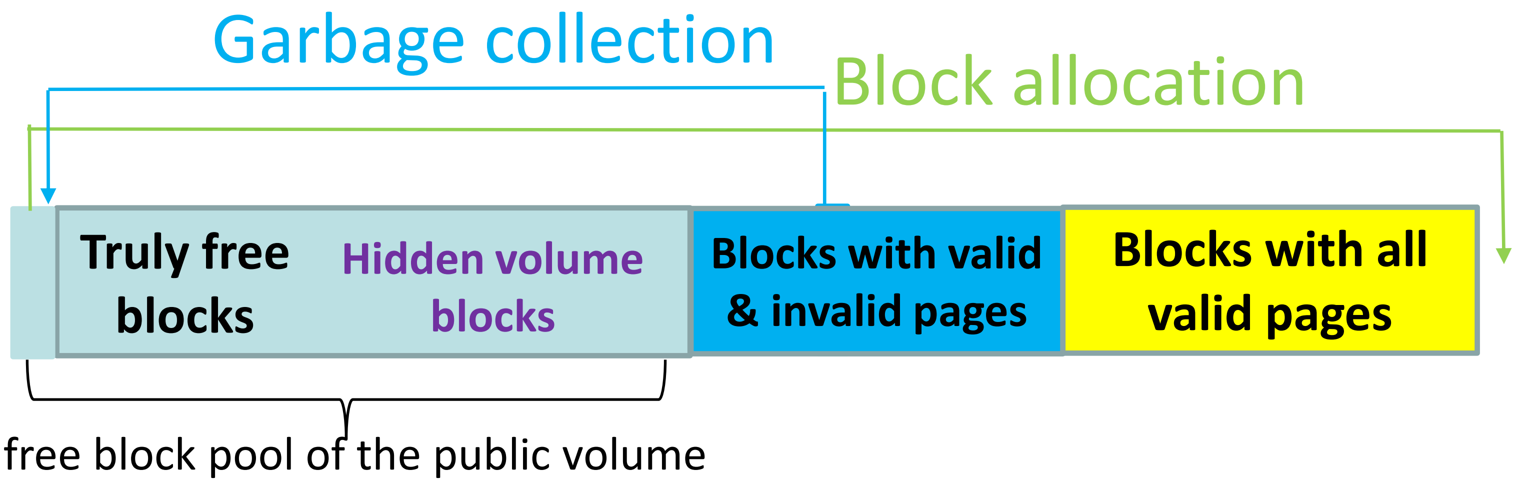
Key insight 1: move the public/hidden volume design down to the flash translation layer (FTL) and strictly isolate them.

1. Strict isolation between the public volume and the hidden volume: **Public data and hidden data will not share flash blocks**; Upon quitting the device, if any flash blocks have hidden data written at the beginning but have empty pages not yet filled, those pages should be filled with randomness
2. Manipulating the special functions (wear leveling, garbage collection, bad block management) of the FTL, **so that they will avoid producing duplicated randomness for the hidden data**.

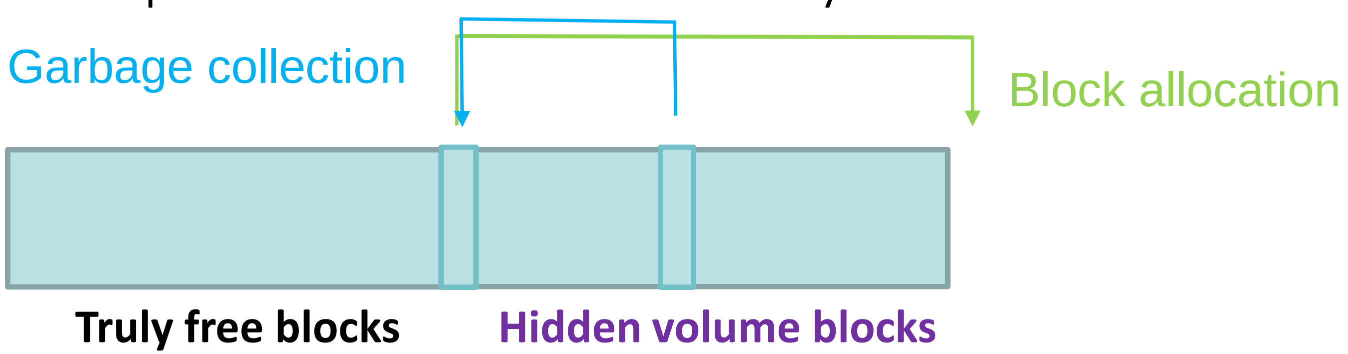
Our FTL-based PDE System (cont.)

Key insight 2: to mitigate the over-write issue, **the public volume should void using blocks occupied by the hidden sensitive data**:

1) The public volume will allocate blocks from the head of the free block pool; active garbage collection will be performed to fill the head of the free block pool.



2) The hidden volume will allocate blocks from the tail of the truly free blocks; active garbage collection will be performed to fill the tail of the truly free blocks.



Other Issues We Having Been Exploring Recently

- How to defend against multi-snapshot adversaries [TIFS, EdgeSP ’21, S&P ’20, DSN ’18]
  - The adversary may have access to the victim device multiple times
- How to avoid deniability compromise in the memory [EdgeSP '21] ?
- How to build a cross-layer PDE system (file system, block device, flash memory layer) [SecureCom ’22]
- How to adapt PDE systems for wearable devices [AC3 '21]

[TIFS] **Niusen Chen**, and Bo Chen. HiPDS: A Storage Hardware-independent Plausibly Deniable Storage System. IEEE Transactions on Information Forensics & Security (TIFS), 2023.

[SecureComm '22] **Niusen Chen**, Bo Chen, and Weisong Shi. A Cross-layer Plausibly Deniable Encryption System for Mobile Devices. 18th EAI International Conference on Security and Privacy in Communication Networks (SecureComm '22), Kansas City, Missouri, October 2022

[AC3 ’22] **Niusen Chen**, Bo Chen, and Weisong Shi. The Block-based Mobile PDE Systems Are Not Secure – Experimental Attacks. 2022 EAI International Conference on Applied Cryptography in Computer and Communications (AC3 '22), Nanjing, China, May 2022

[EdgeSP '21] Jinghui Liao, Bo Chen, and Weisong Shi. TrustZone Enhanced Plausibly Deniable Encryption System for Mobile Devices. The Fourth ACM/IEEE Workshop on Security and Privacy in Edge Computing (EdgeSP '21), San Jose, CA, December 2021.

[AC3 '21] **Niusen Chen**, Bo Chen, and Weisong Shi. MobiWear: A Plausibly Deniable Encryption System for Wearable Mobile Devices. The First EAI International Conference on Applied Cryptography in Computer and Communications (AC3 '21), Xiamen, China, May 2021 (Best Paper Award).

[DSN ’18] Bing Chang, Fengwei Zhang, Bo Chen, Yingjiu Li, Wen Tao Zhu, Yangguang Tian, Zhan Wang, and Albert Ching. MobiCeal: Towards Secure and Practical Plausibly Deniable Encryption on Mobile Devices. The 48th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN ’18), June 2018 (Acceptance rate: 28%)

Acknowledgments

- The PDE project has been supported by US National Science Foundation under grant number 1928349-CNS

https://snp.cs.mtu.edu/research/cloudsec.html