CS5740/4740 Spring 2022: Special Topic on Data Security (2)

# Plausibly Deniable Encryption Systems for Mobile Devices


Bo Chen

Department of Computer Science

Michigan Technological University

https://cs.mtu.edu/~bchen

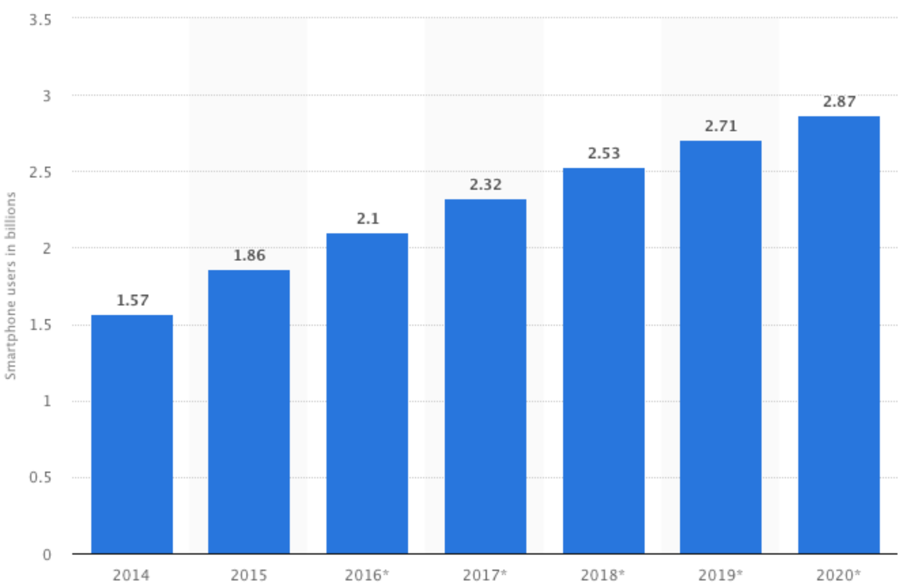
https://snp.cs.mtu.edu

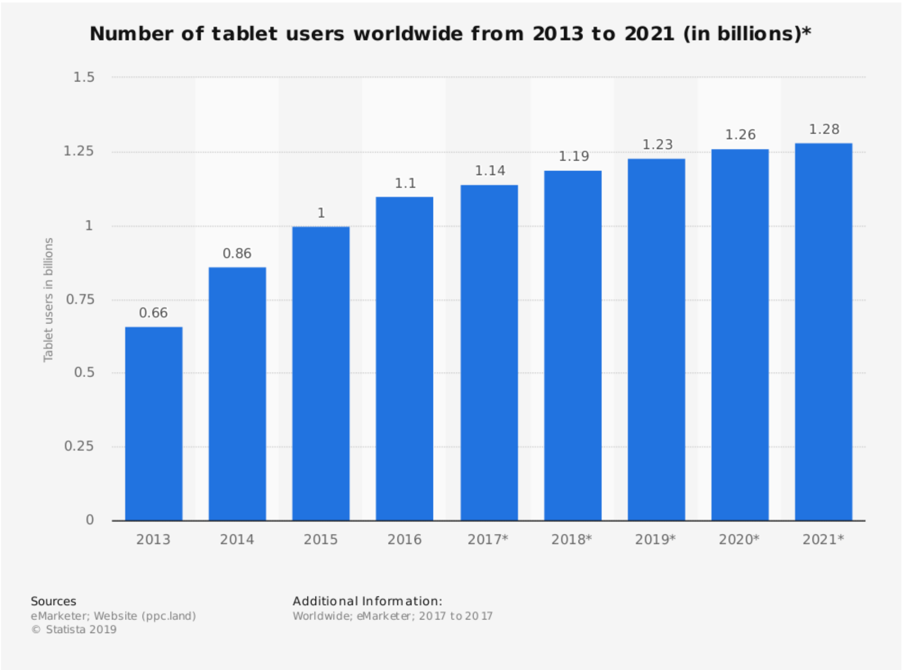
bchen@mtu.edu

# Course Evaluation

- Find a few mins to fill up your course evaluation by the weekend

# Mobile Devices are Turning to Mainstream Computing Devices



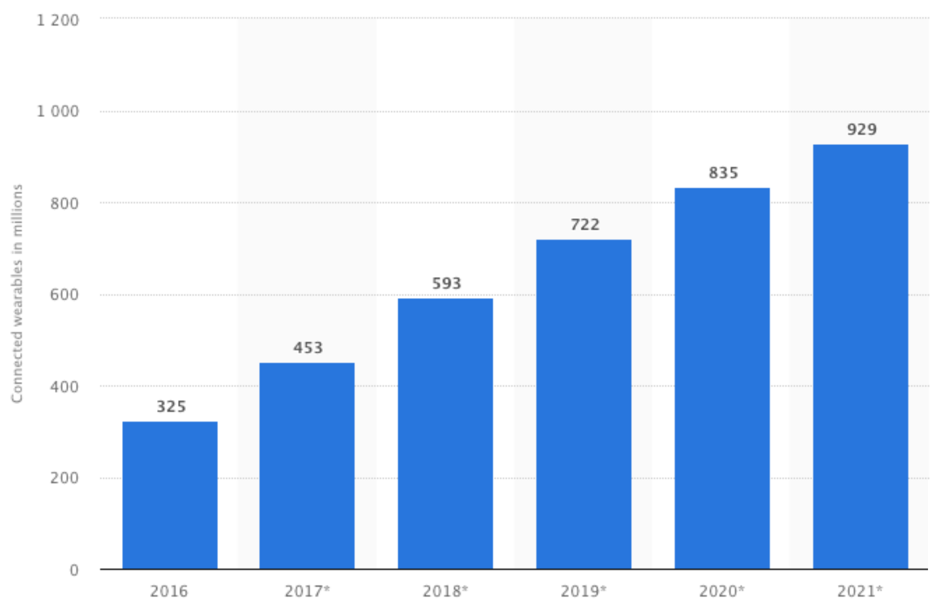




Number of smartphone users worldwide from 2014 to 2020 (in billions)

Number of tablet users worldwide from 2013 to 202

(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
  - Naked photos
  - A human rights worker collects evidence of atrocities in a region of oppre
  - Etc.

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

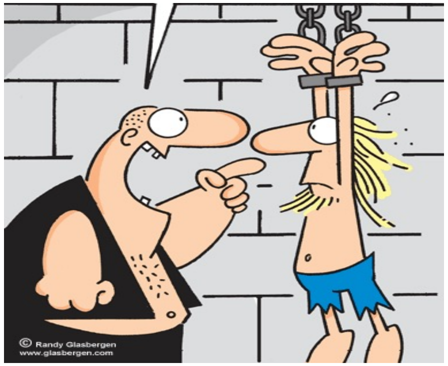
# Coercive Attack against Confidentiality

- To protect confidentiality of sensitive data, we can simply encrypt them
  - AES
  - 3DES

- Conventional encryption is vulnerable to a coercive attack
  - A user captures sensitive data using his/her smart phone, but is captured by an attacker
  - A journalist captured criminal evidence in a country of conflict, tries to cross the boarder, but is stopped by the boarder inspector

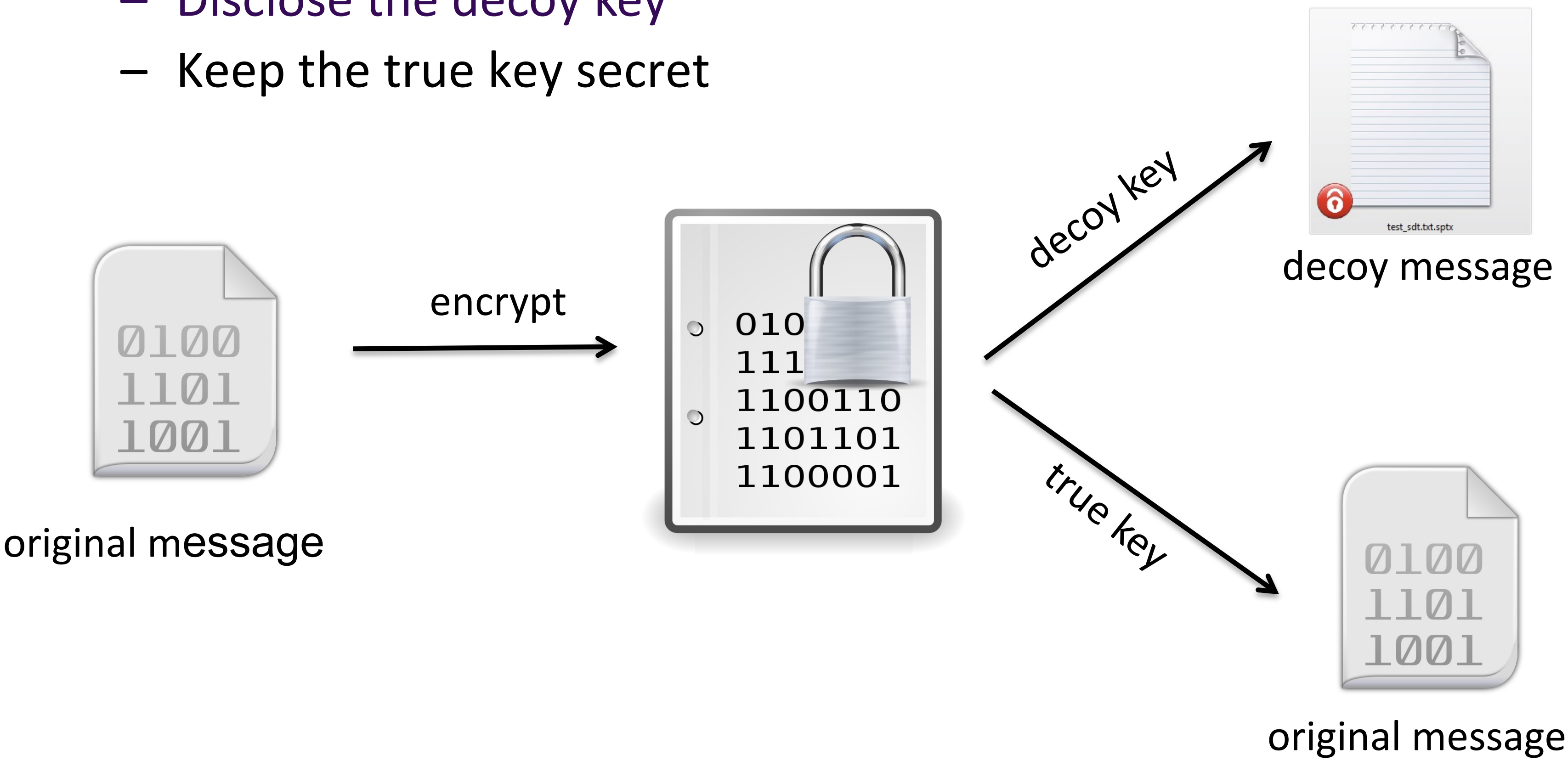
An attacker forces the device's owner to disclose the decryption key

TELL ME YOUR KEY!!!



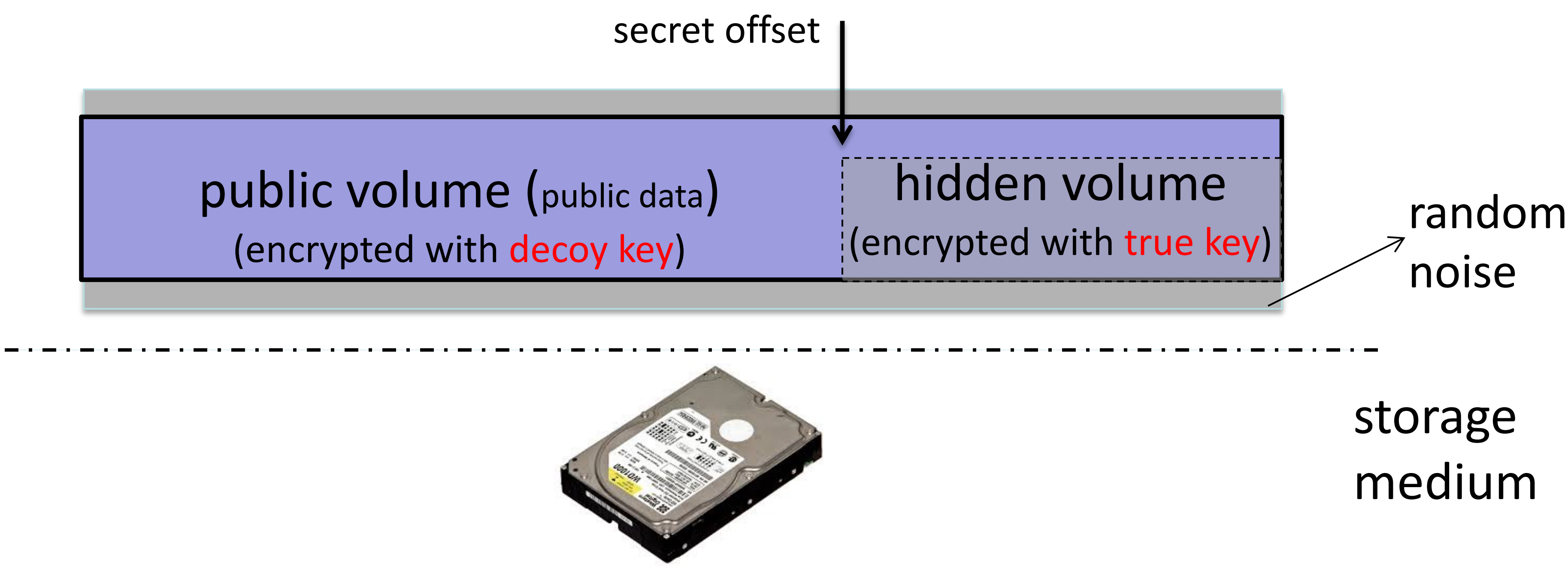
# Plausible Deniable Encryption (PDE)

- Plausible Deniable Encryption (PDE) [Canetti et al., CRYPTO ’97]: a crypto primitive designed for mitigating coercive attacks
  - Disclose the decoy key
  - Keep the true key secret



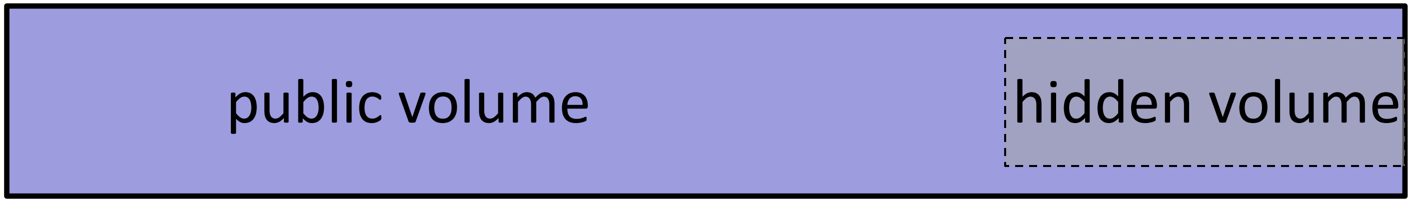
# Implementing PDE in Systems - Hidden Volume

- 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



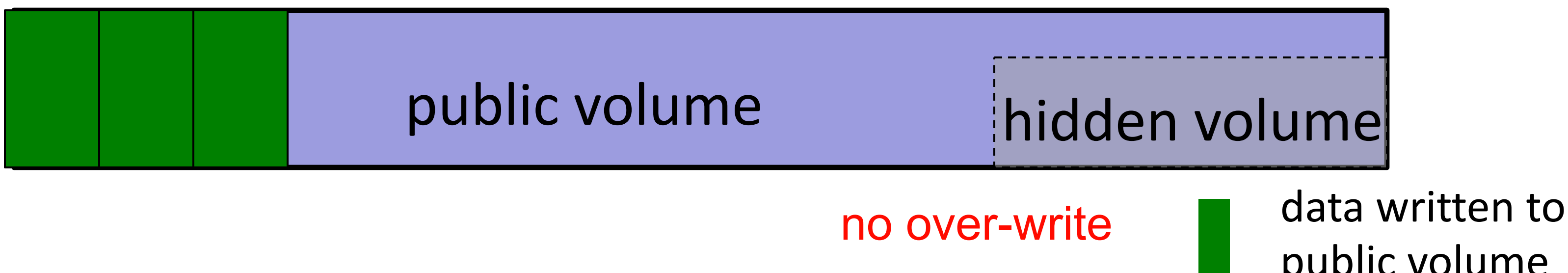
# The Challenges: Over-writing Issues

- 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

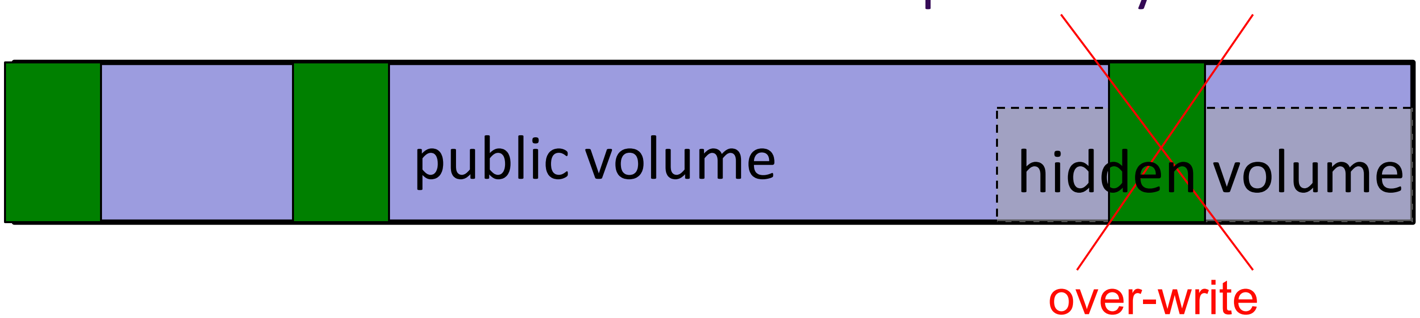


# The Challenges: Over-writing Issues (cont.)

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




  - EXT4 does not allocate blocks sequentially

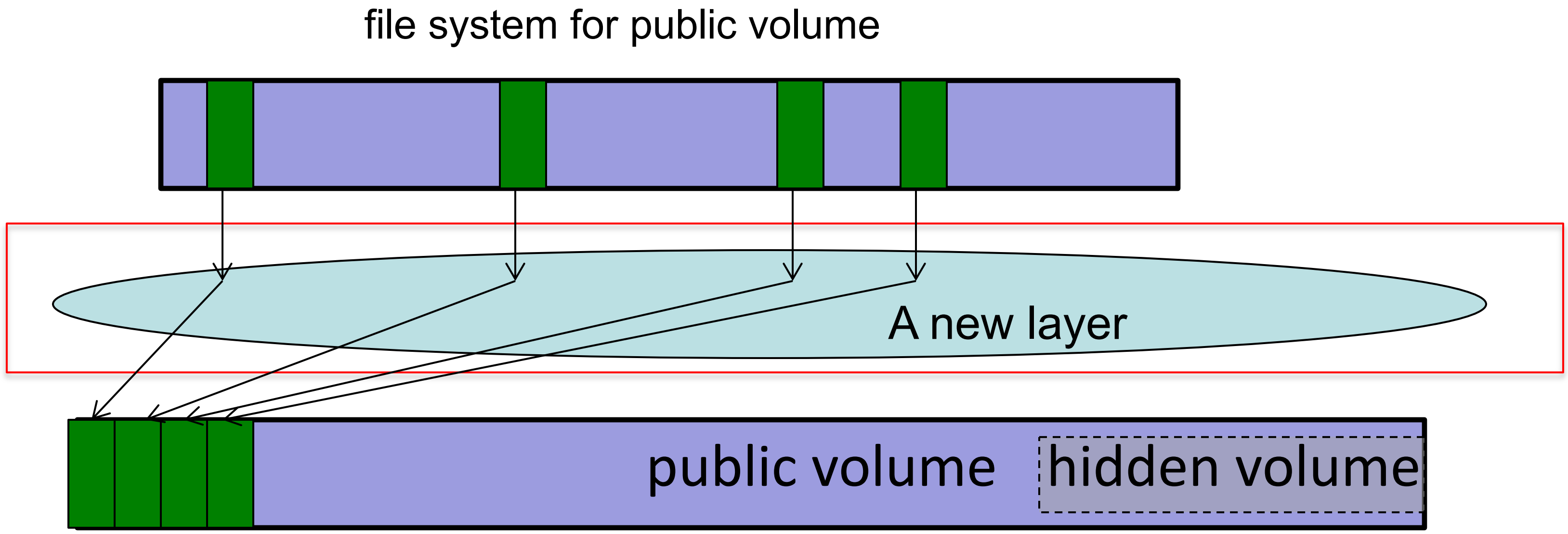



It is challenging to allow any file systems to be deployed while mitigating the over-write issues

# 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

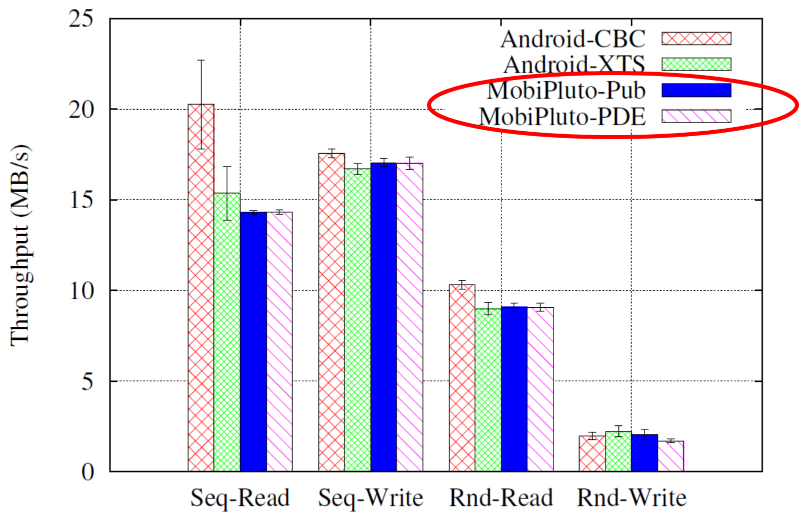
1. Provide virtual volumes to file systems
2. Any block-based file system can be built on a virtual volume
3. Non-sequential allocation on the virtual volume will be converted to sequential allocation on the underlying layer




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

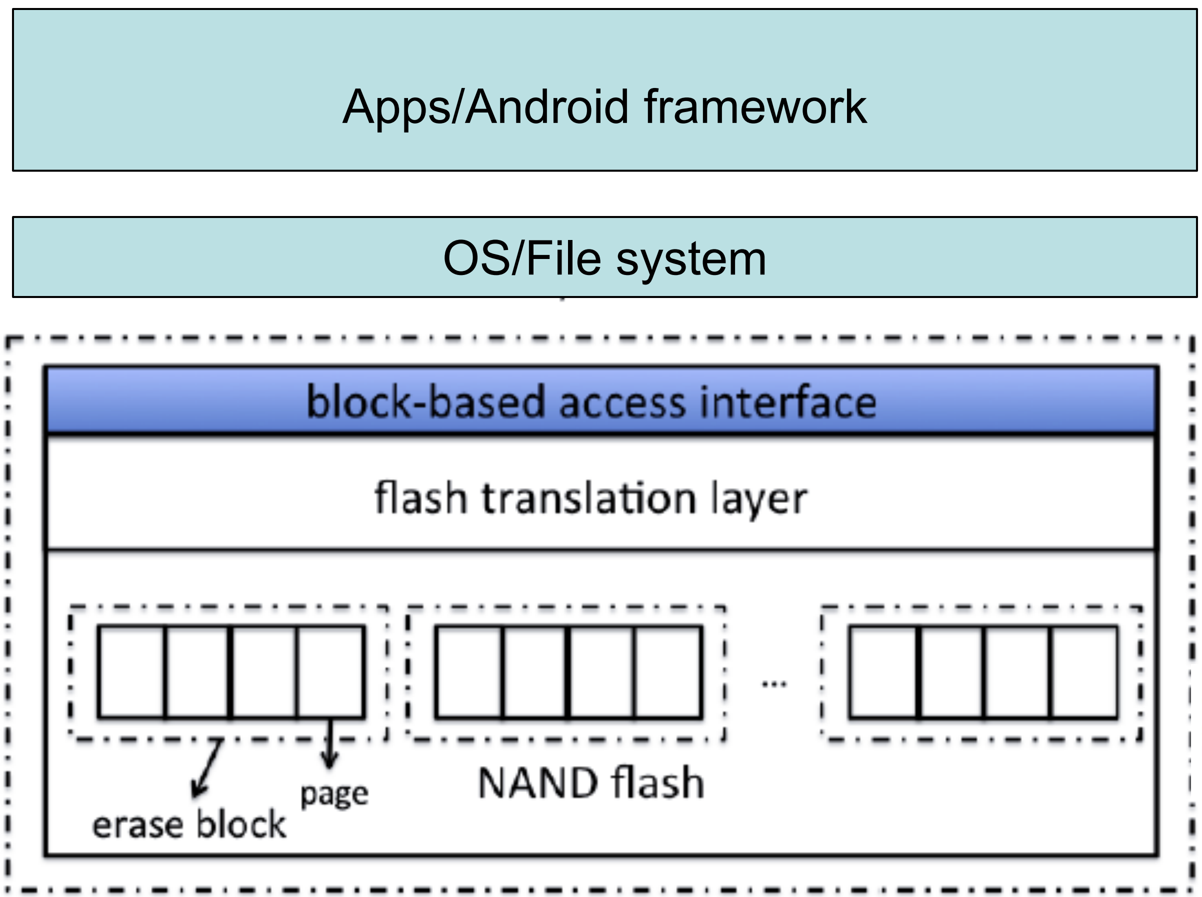
- Implemented a prototype of our solution on LG Nexus 4




Throughput (MB/s) from AndroBench

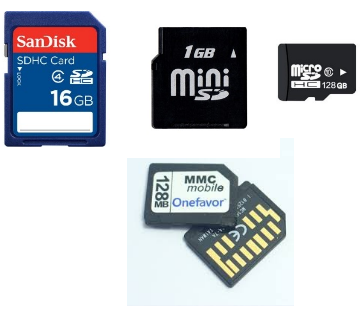
# Deniability Compromise at Lower Storage Layer?

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




deniability compromise

Flash storage (eMMC card/SD card)

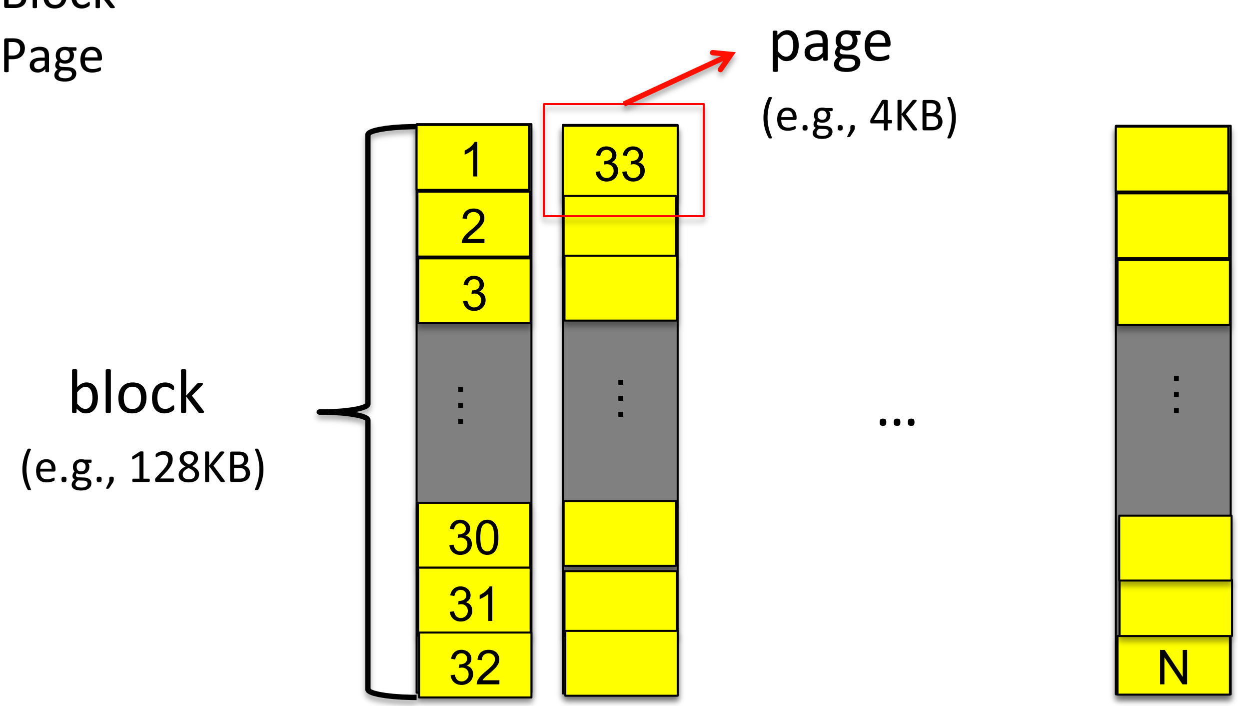



A Main-stream Storage Architecture for Mobile Devices

# NAND Flash Memory

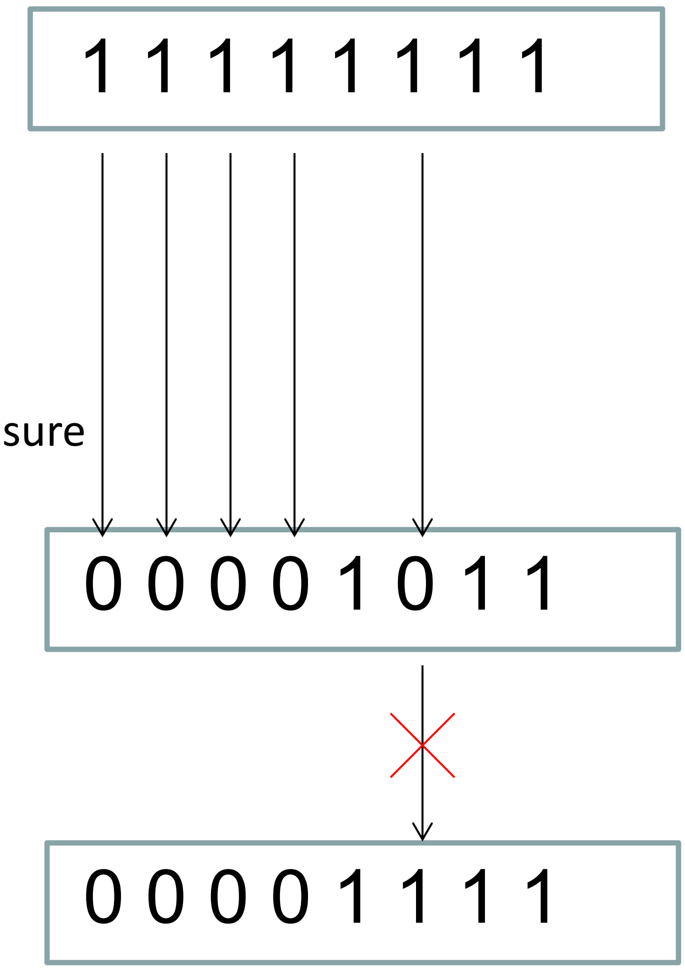

- Flash memory
  - NAND flash (broadly used for mass-storage devices)
  - NOR flash (used for storing program code that rarely needs to be updated, e.g., a computer's BOIS)

- NAND flash organization
  - Block
  - Page



# Flash Memory Programming

All ‘1’ initially:



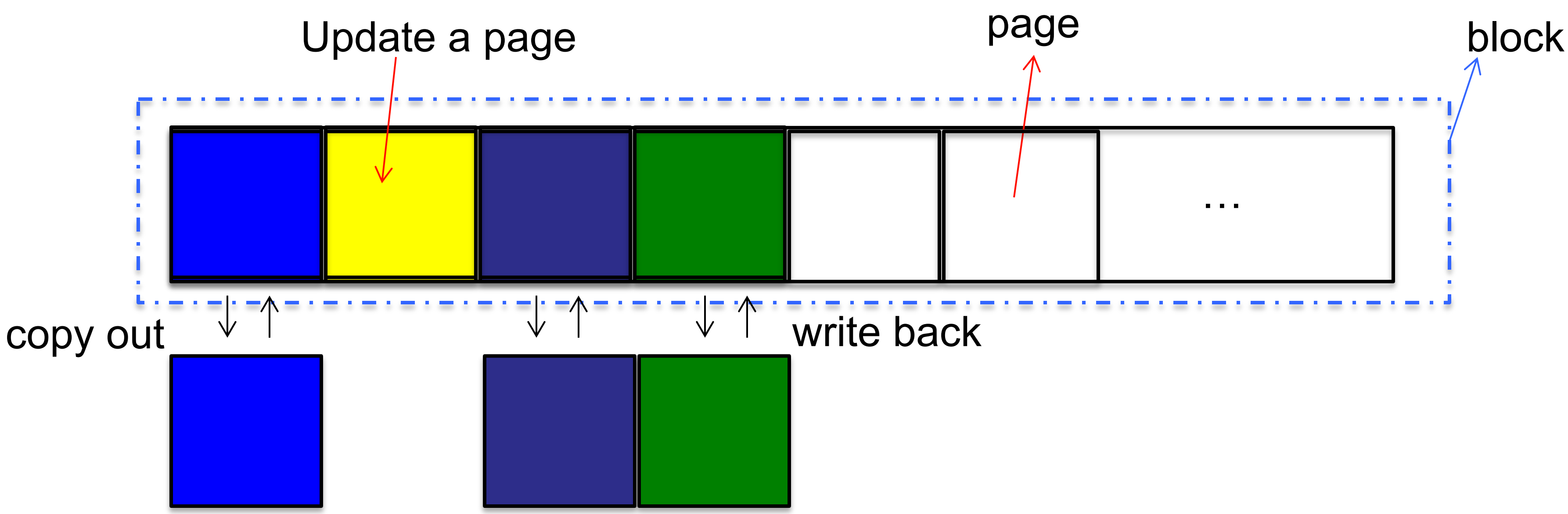

Write 0x0b:
Rule:
1) 1 can be programed to 0
2) 0 cannot be programed to 1 except performing an erasure

Write 0x0f?

Need to erase to all ‘1’ first

# Special Characteristics of Flash Memory

- Update unfriendly
  - Over-writing a page requires first erasing the entire block
  - Write is performed in pages (e.g., 4KB), but erase is performed in blocks (e.g., 128KB)




  - Over-write may cause significant write amplification
  - Usually prefer out-of-place update instead of in-place update

# Special Characteristics of Flash Memory (cont.)

- Support a finite number of program-erase (P/E) cycles
  - Each flash block can only be programmed/erased for a limited number of times (e.g., 10K)
  - Data should be placed evenly across flash (wear leveling)

# How to Manage NAND Flash

- Flash-specific file systems, which can handle the special characteristics of NDND flash
  - YAFFS/YAFFS2, UBIFS, F2FS, JFFS/JFFS2

- Flash translation layer (FTL) – a flash firmware embedded into the flash storage device, which can handle the special characteristics of NAND flash and emulate the flash storage as a regular block device (most popular)
  - SSD
  - USB
  - SD / miniSD/MicroSD
  - MMC cards

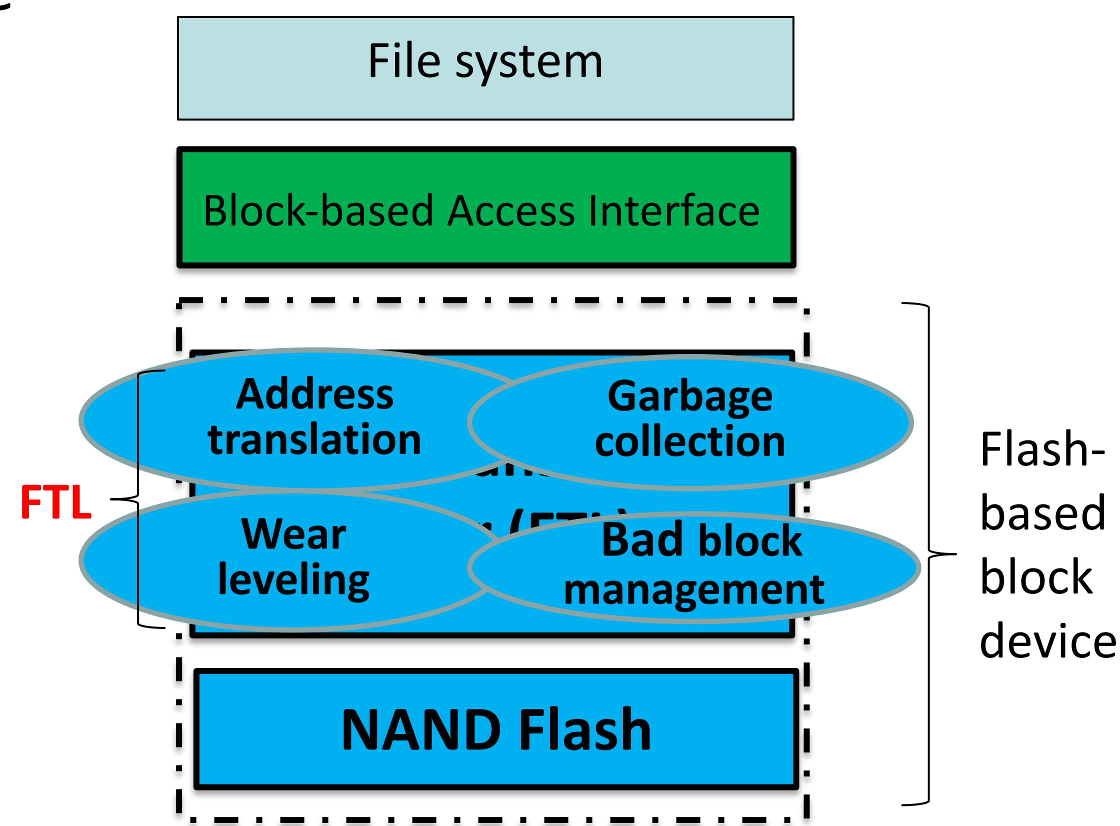



# Flash Translation Layer (FTL)

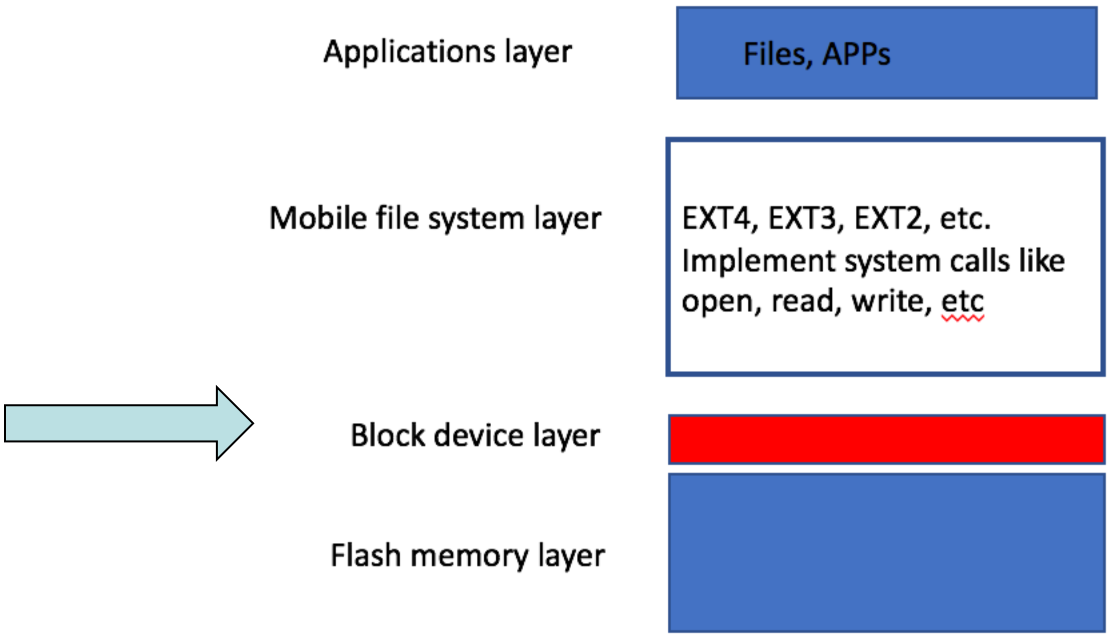
FTL usually provides the following functionality:

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

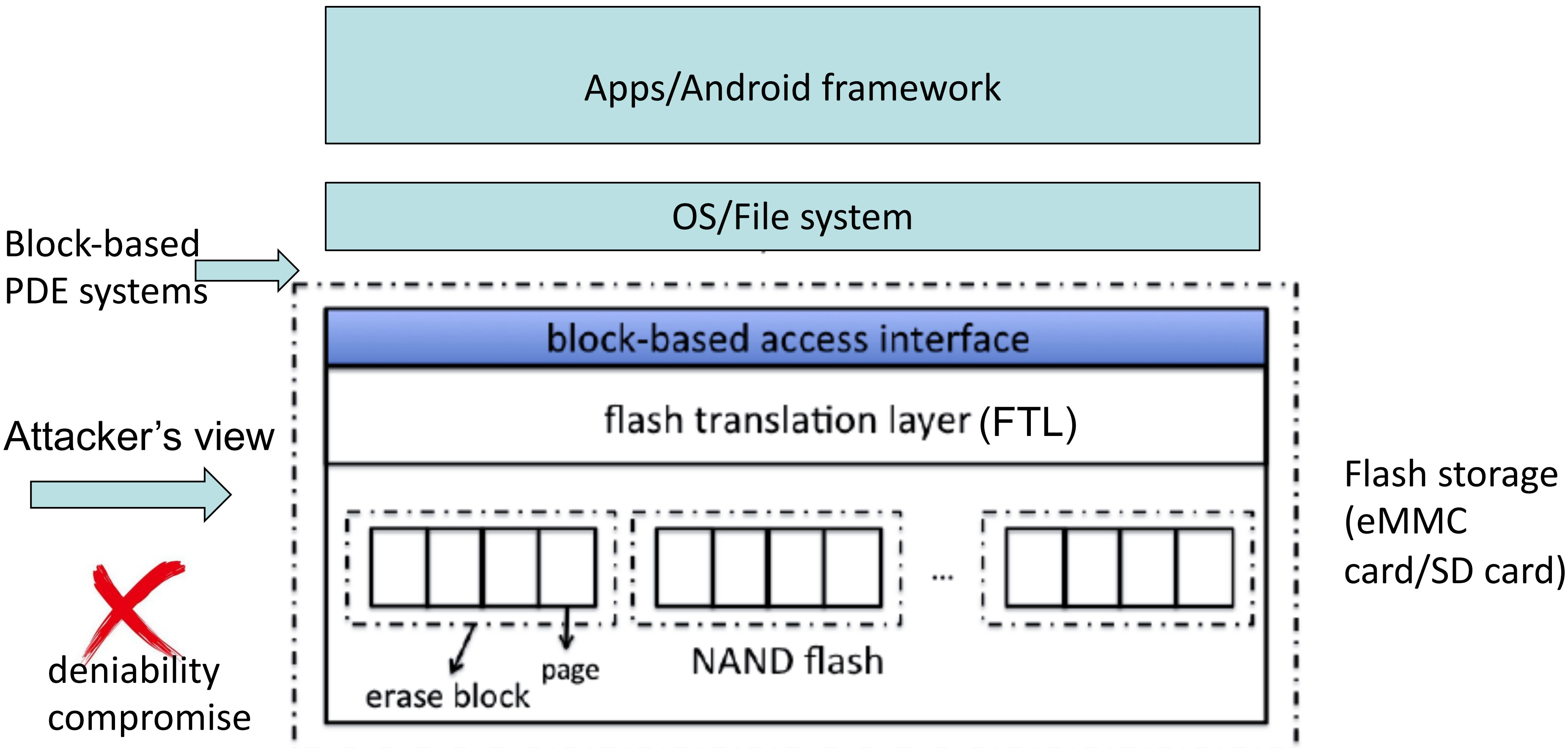


# Existing PDE Systems for Mobile Devices

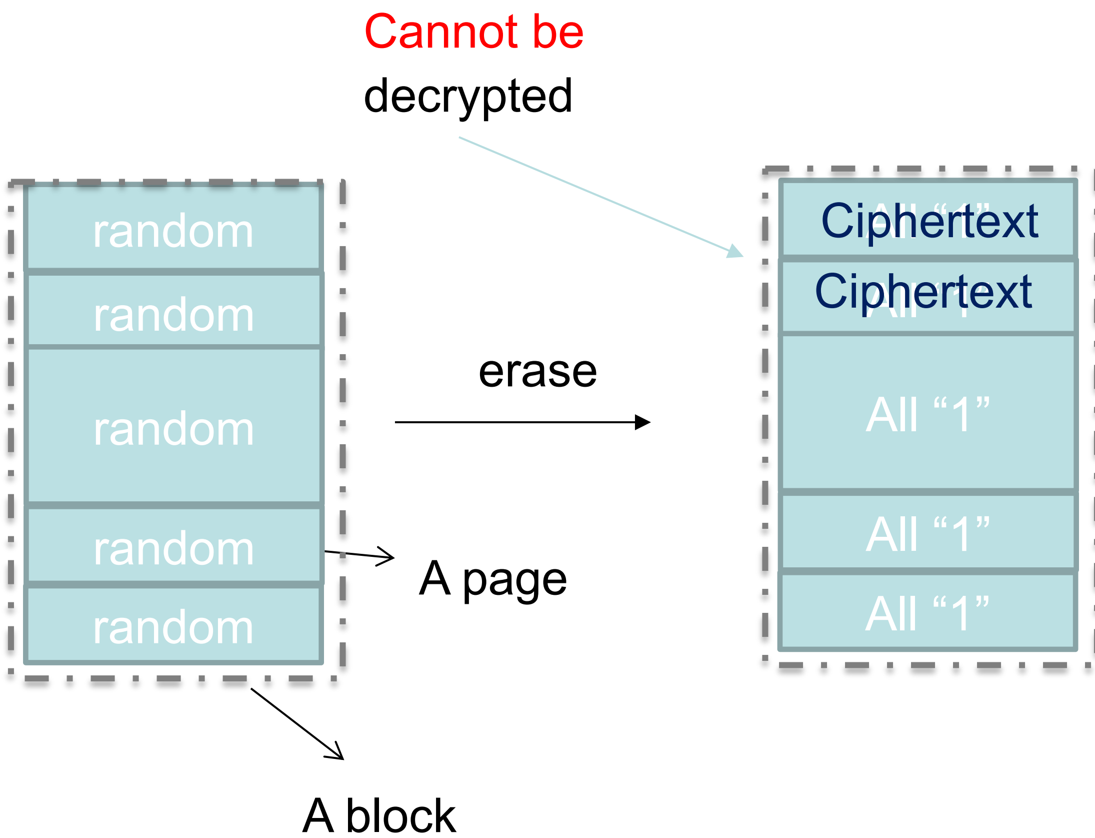
- Most of the existing PDE systems deploy hidden volume on top of the block device
  - Mobiflage [Skillen et al., NDSS '13]
  - MobiHydra [Yu et al., ISC '14]
  - MobiPluto [Chang et al., ACSAC '15]
  - MobiCeal [Chang et al., DSN '18]



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

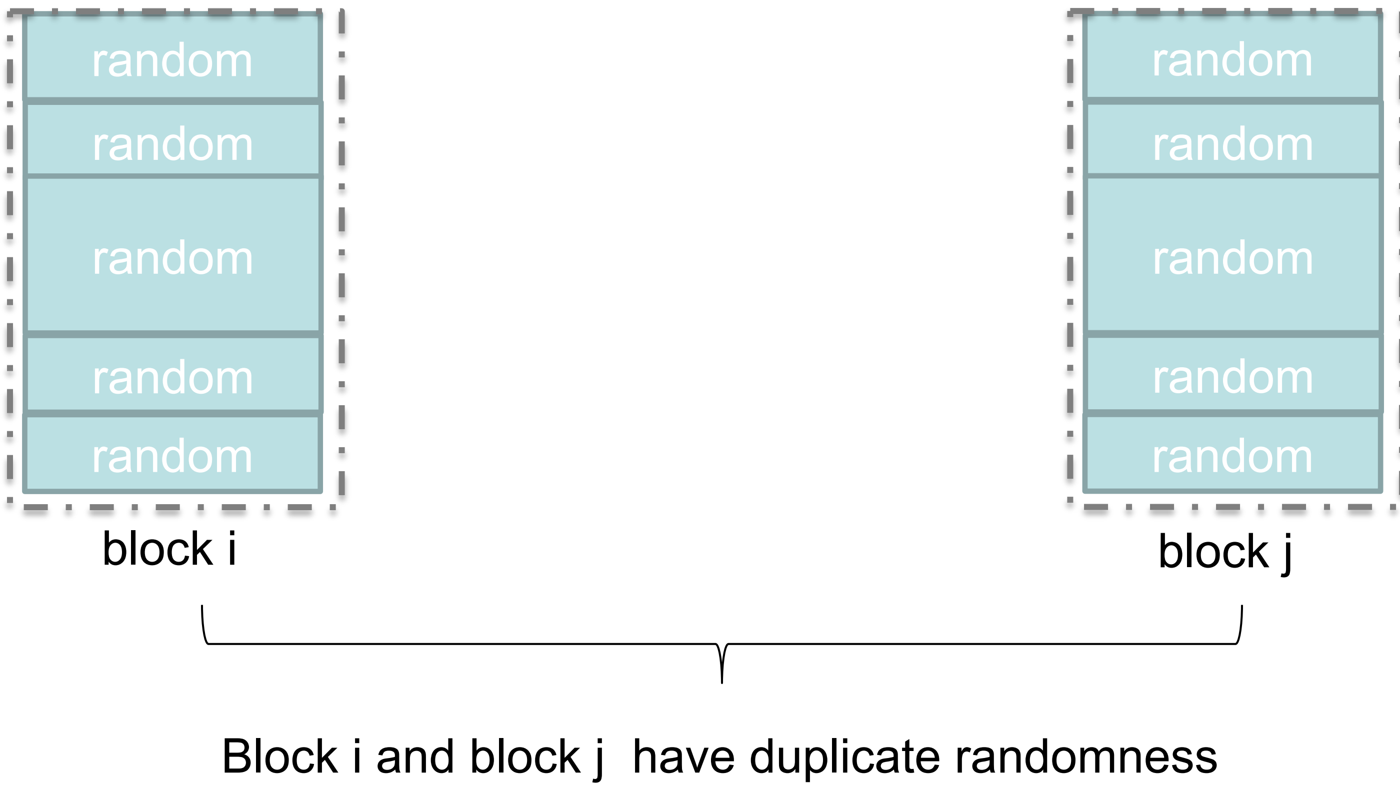


# Compromise of Existing PDEs Built on top of the block device (1)




**A flash block partially used by the hidden volume**

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



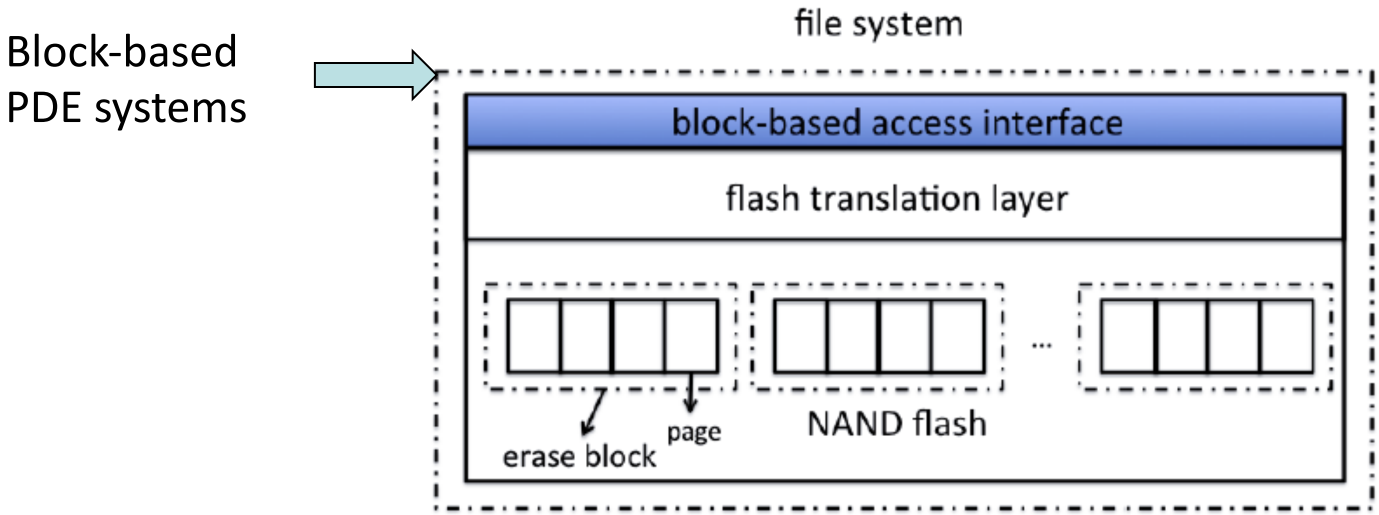

**Special flash memory operations (wear leveling, garbage collection, bad block management) on the hidden volume will create duplicate randomness**



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%)

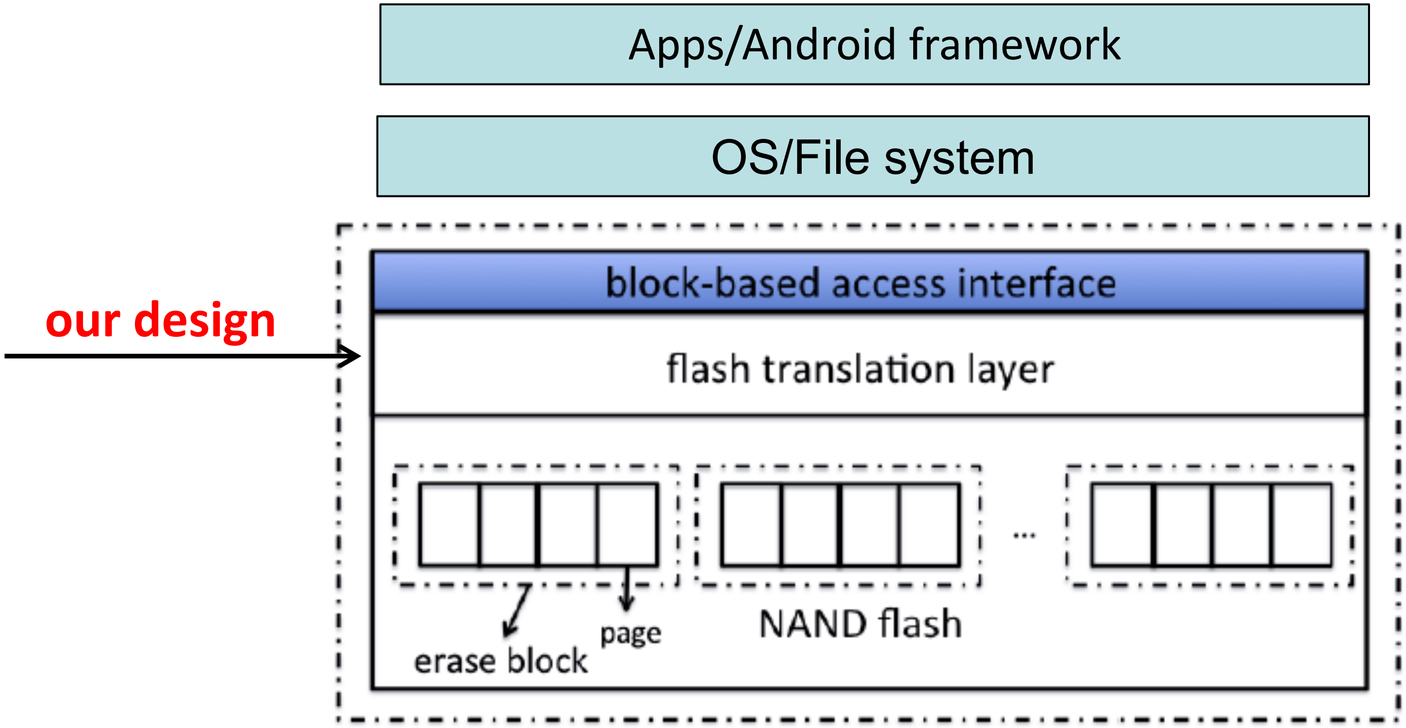
# Fundamental Reasons for Compromises of The Existing Block-based PDE Systems

- 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



# Our 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.)

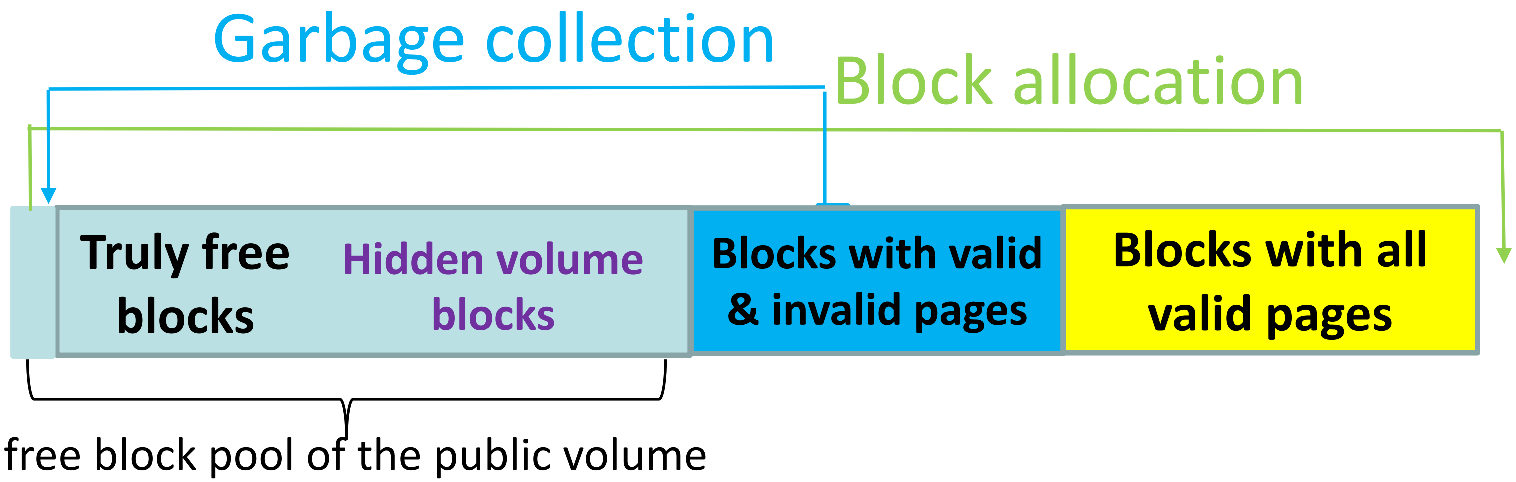
Key insight 1: move the public/hidden volume design down to the flash translation layer (FTL) and strictly isolate them.

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**.

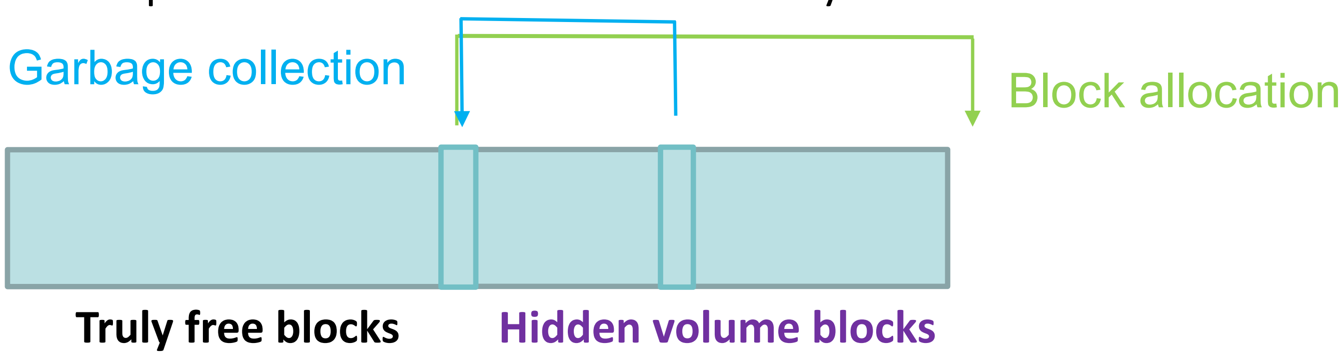
# Our FTL-based PDE System (cont.)

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

- How to defend against multi-snapshot adversaries [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 integrate the PDE system in both the upper layers (file system, block device) and the flash memory layer
- How to adapt PDE systems for wearable devices [AC3 '21]


[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).

[S&P '20] **Bo Chen**, and Niusen Chen. A Secure Plausibly Deniable System for Mobile Devices against Multi-snapshot Adversaries. 2020 IEEE Symposium on Security and Privacy (S&P '20), San Francisco, CA, May 2020 (extended abstract).

[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