CS 5472 - Advanced Topics in Computer Security

Topic 6: Deniable Encryption (2)

Spring 2023 Semester

Instructor: Bo Chen

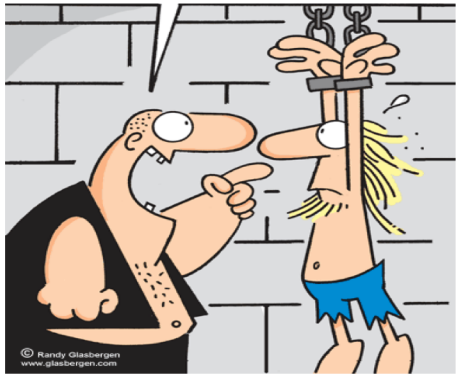
bchen@mtu.edu

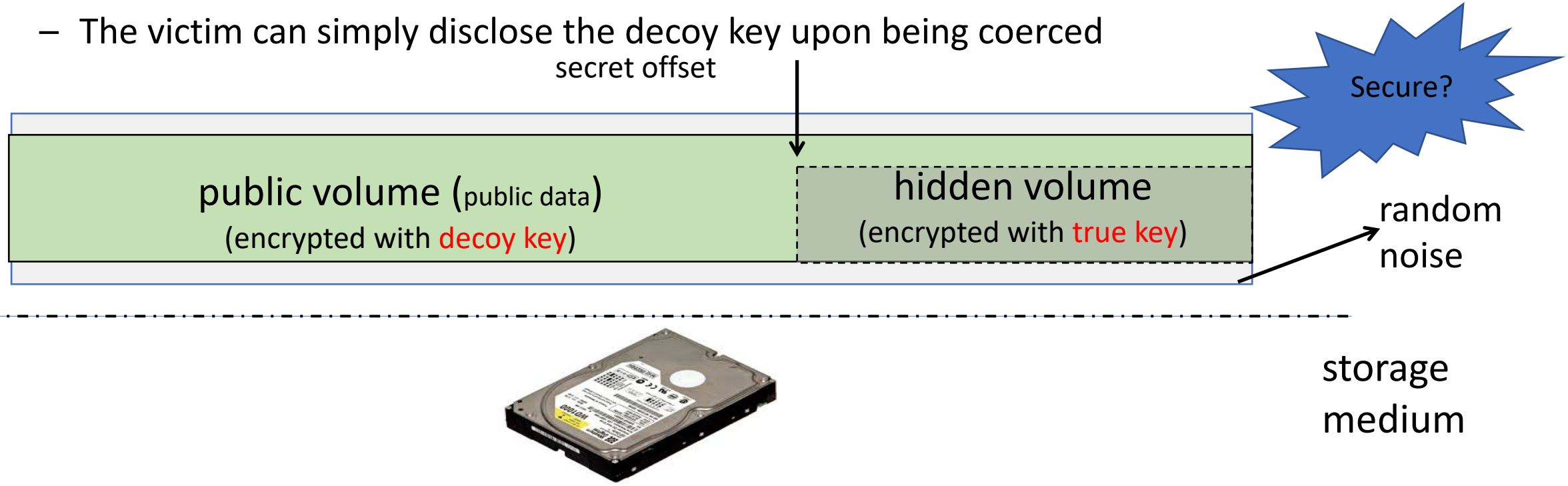
https://cs.mtu.edu/~bchen

Review: Use Hidden Volume to Mitigate Coercive Attacks

- A coercive attacker can enforce the victim to disclose the decryption key
- A hidden volume-based PDE (plausibly deniable encryption) system can be used in mobile devices to mitigate coercive attacks (the design presented on Tuesday's paper presentation)
  - The victim can simply disclose the decoy key upon being coerced

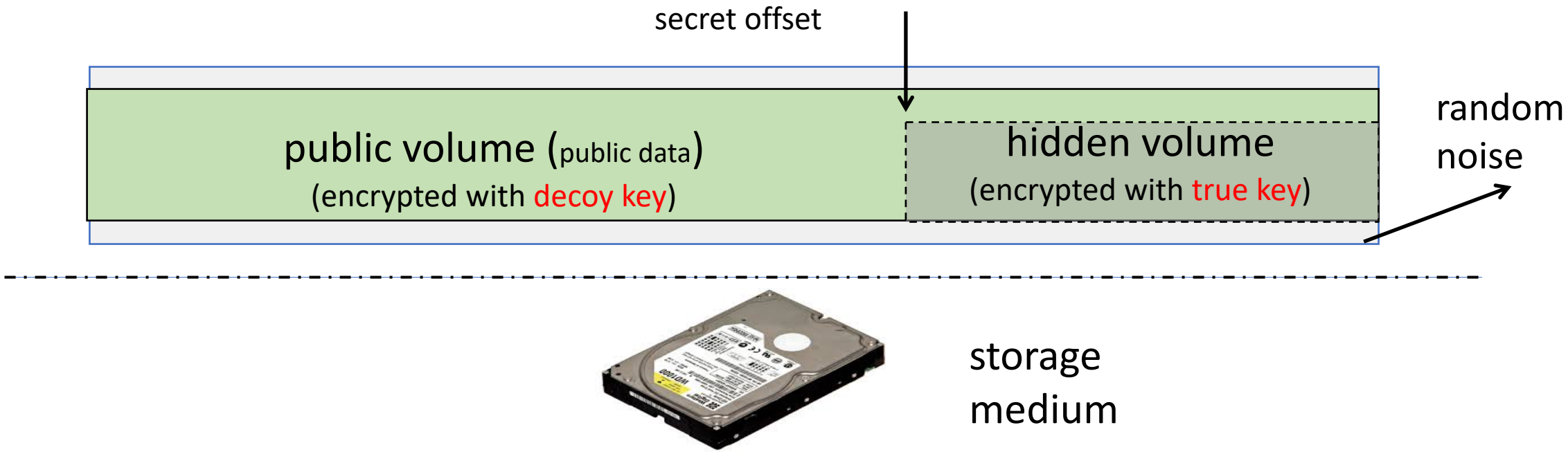
TELL ME YOUR KEY!!!





Deniability Compromise 1: The Attacker Can Have Access to The Disk Multiple Times

- By having multiple snapshots on the storage medium, the attacker can compromise deniability
  - Compare different snapshots and can observe the changes/modifications over the hidden volume, which was not supposed to happen
  - **Hidden volume is hidden in the empty space of the public volume**

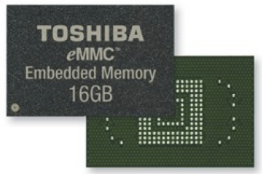


Defending against The Multi-snapshot Adversary

- 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.
- 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) Poster Session, San Francisco, CA, May 2020.
- 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

Deniability Compromise 2: from The Underlying Storage Hardware

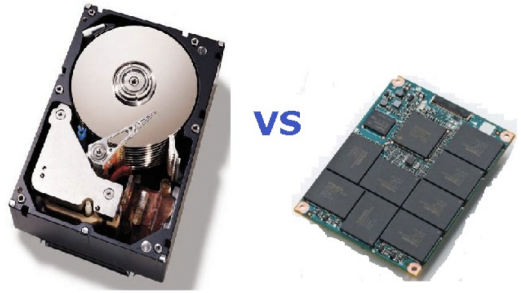
- Mobile devices usually use flash memory as the underlying storage media, rather than mechanical hard disks
  - eMMC cards
  - miniSD cards
  - MicroSD cards



eMMC Chip

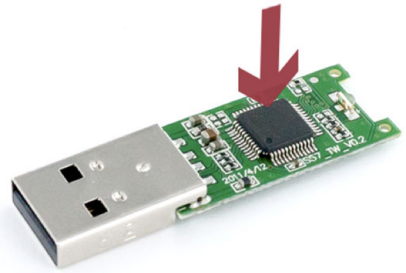

MMC Card

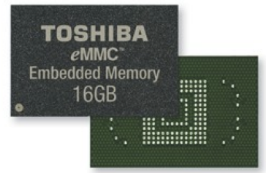
- **Flash memory has significantly different hardware nature compared to mechanical disk drives**, which may cause deniability compromises unknown by the upper layers (application, file system, and block layer)



NAND Flash is Usually Used as Storage Media

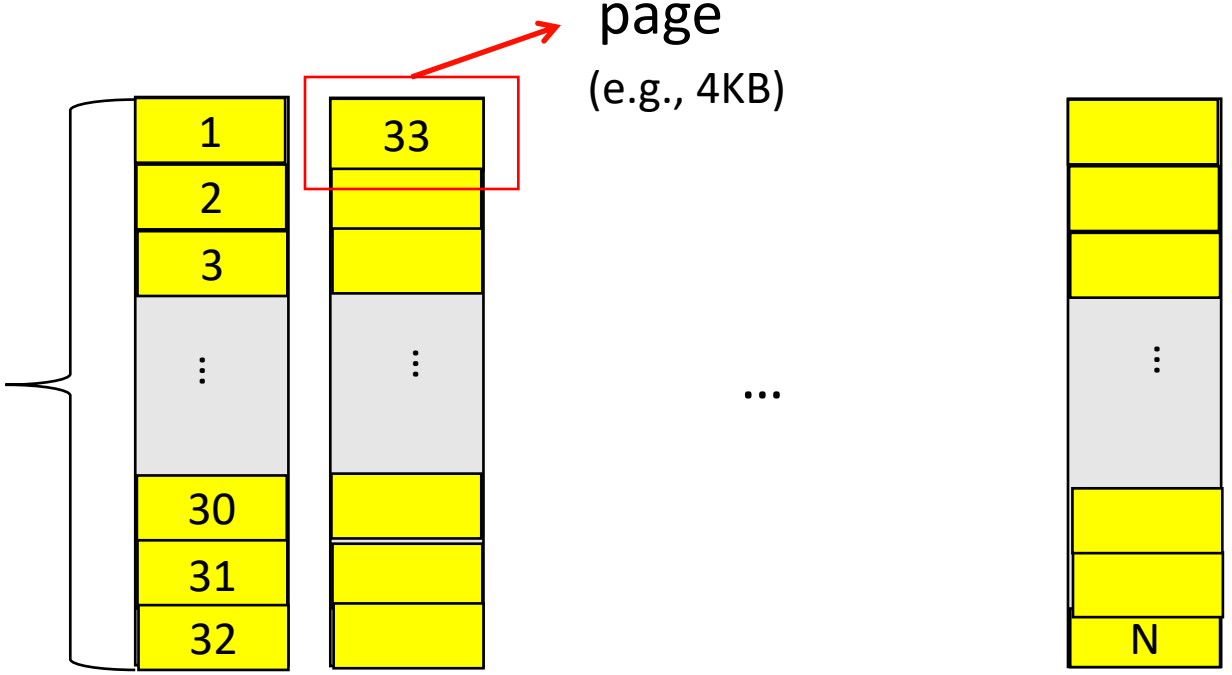
- NAND flash
  - USB sticks
  - Solid state drives (SSD)
  - SD/miniSD/microSD/eMMC





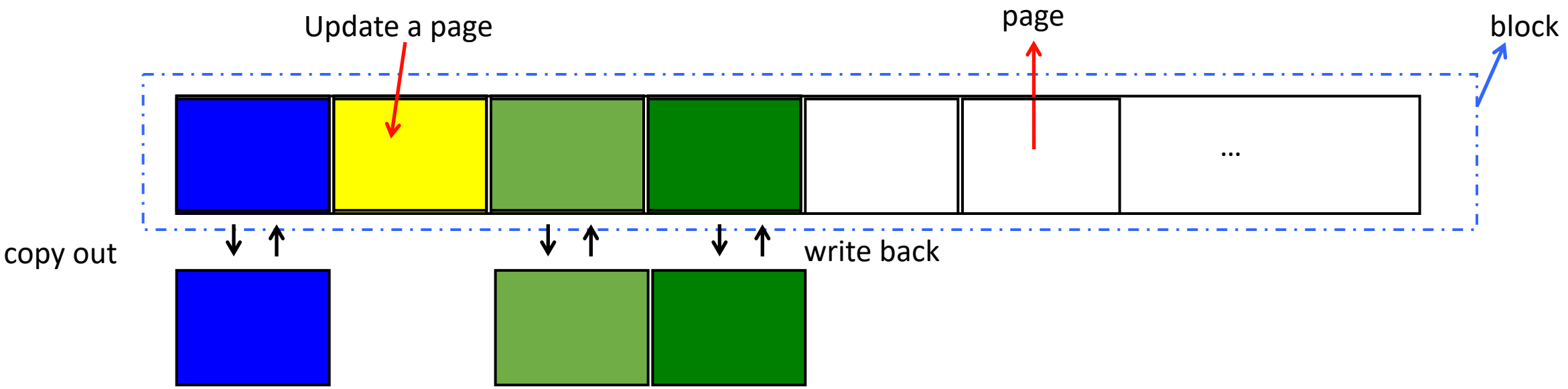
eMMC Chip

MMC Card



Special Characteristics of NAND Flash

- 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)



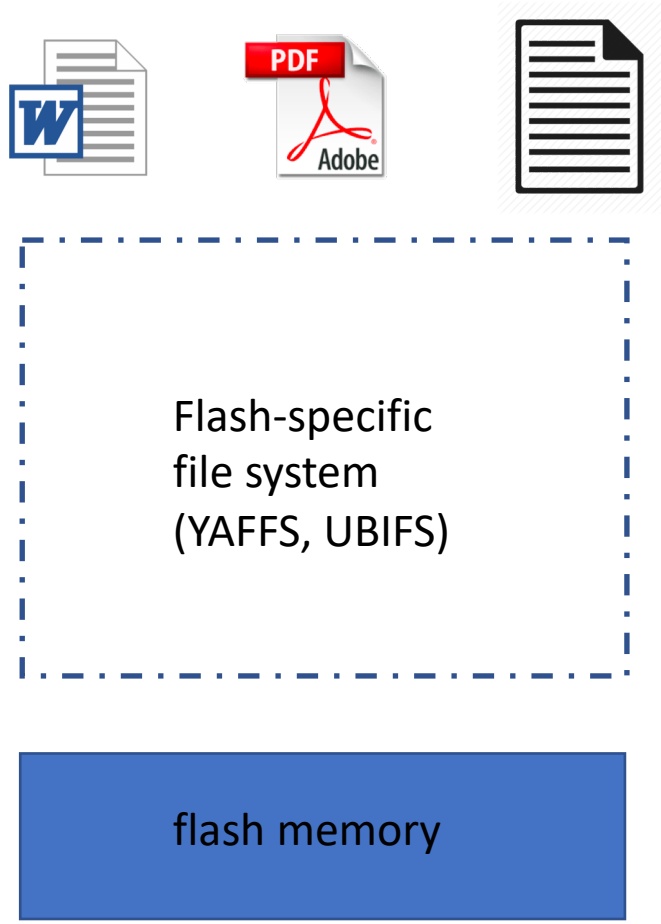
  - Over-write may cause significant write amplification

Special Characteristics of NAND Flash (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)

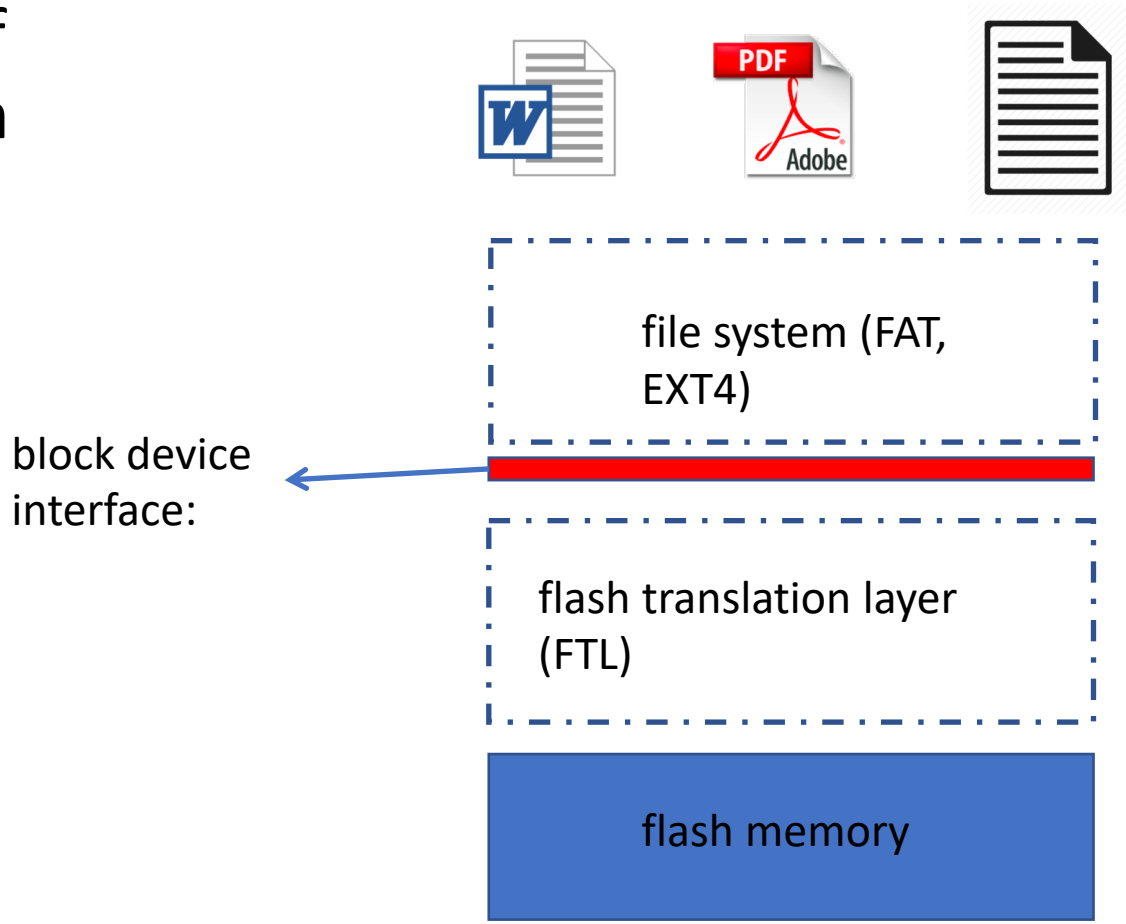
How to Manage NAND Flash

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



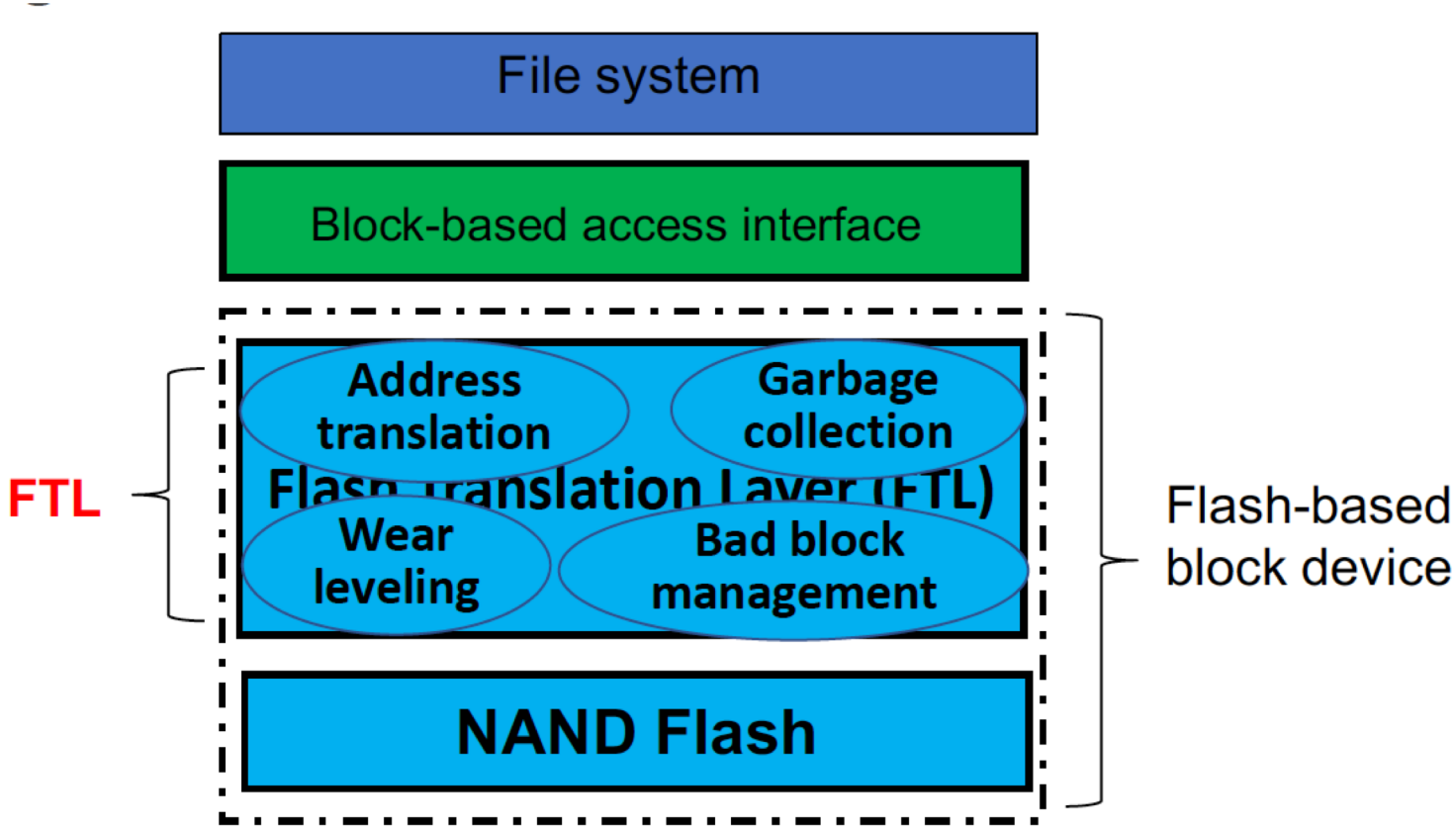
How to Manage NAND Flash (cont.)

- Flash translation layer (FTL) – a piece of 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



Flash Translation Layer (FTL)

- FTL usually provides the following functionality:
  - Address translation
  - Garbage collection
  - Wear leveling
  - Bad block management

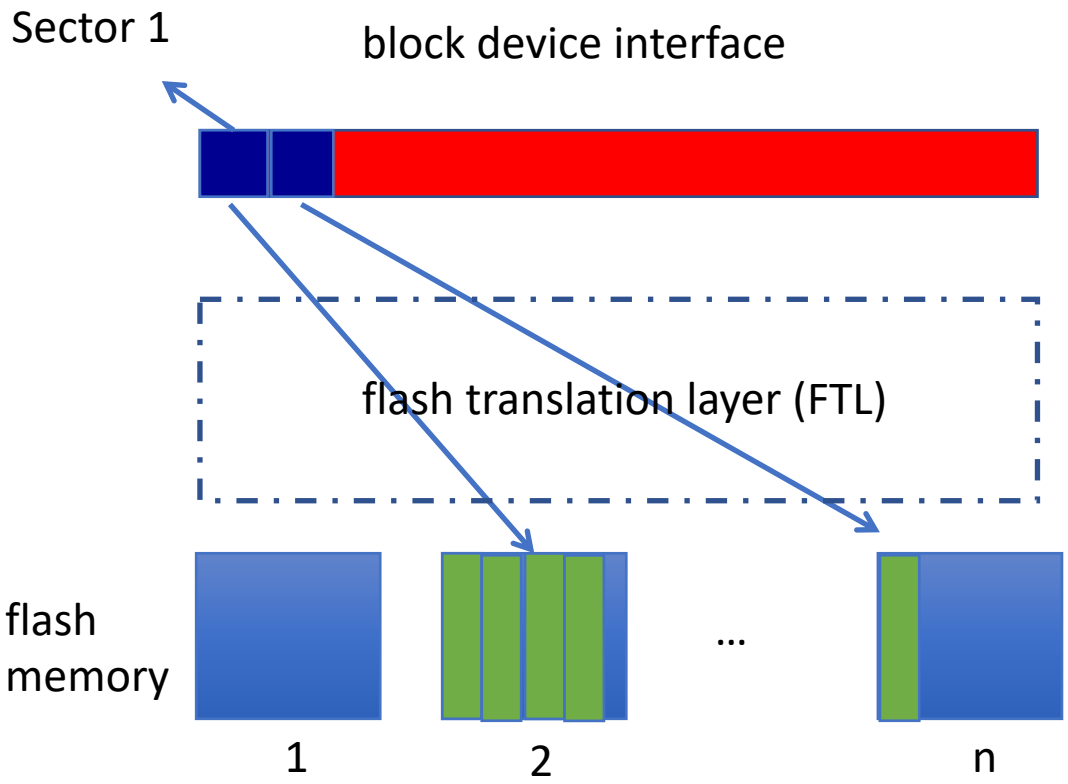


Flash Translation Layer (cont.)

- Address translation
  - Translate address between block addresses and flash memory addresses
  - Need to keep track of mappings between Logical Block Address (LBA) and Physical Block Address (PBA)

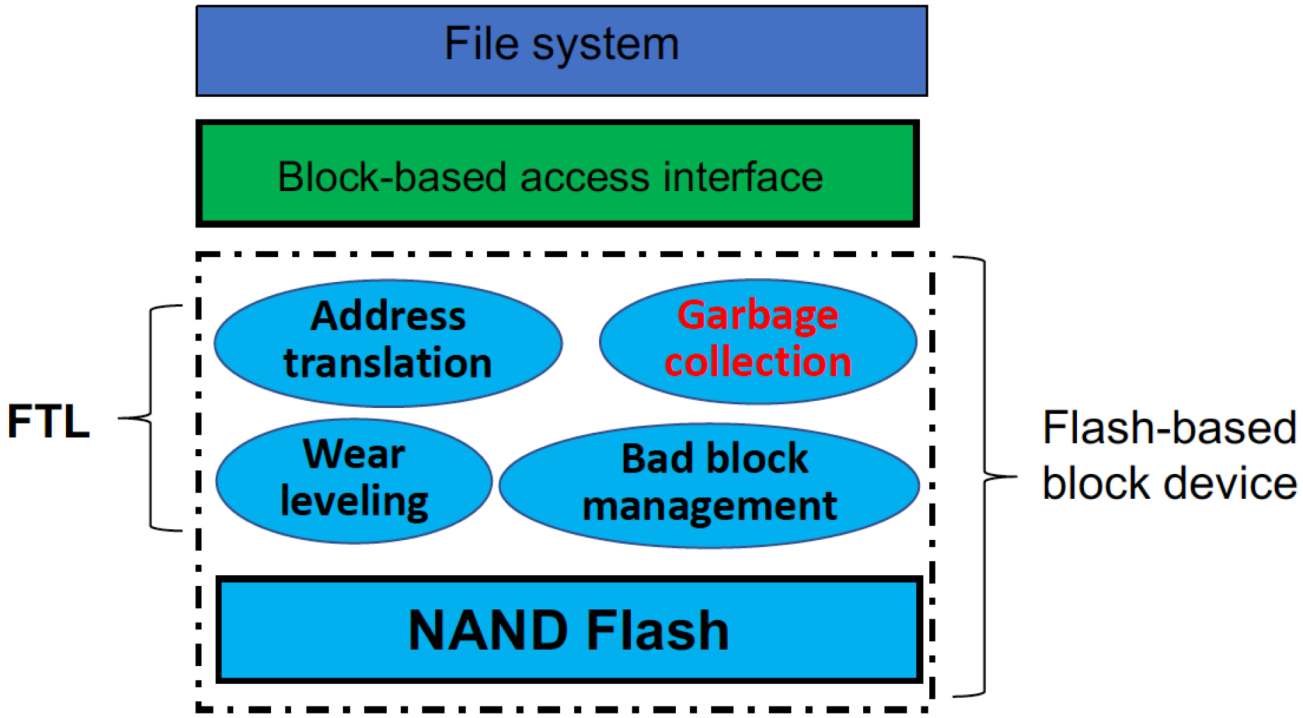
FTL should maintain a mapping table

Block device location	Flash location
Sector 1	(2,3)
Sector 2	(n,1)



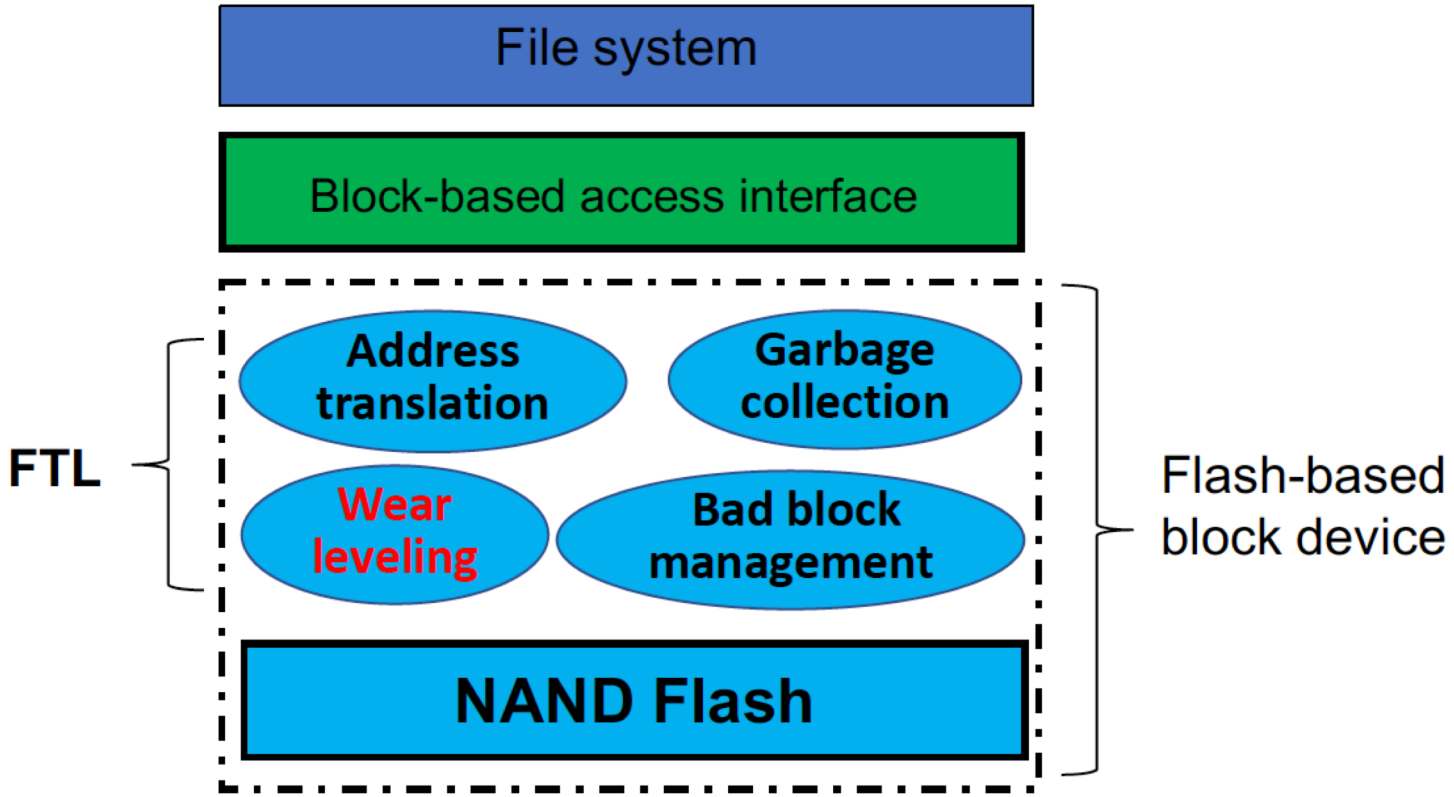
Flash Translation Layer (cont.)

- Garbage collection
  - Flash memory is update unfriendly
  - Not prefer in-place update, but prefer out-of-place update
  - The blocks storing obsolete data should be reclaimed periodically by garbage collection



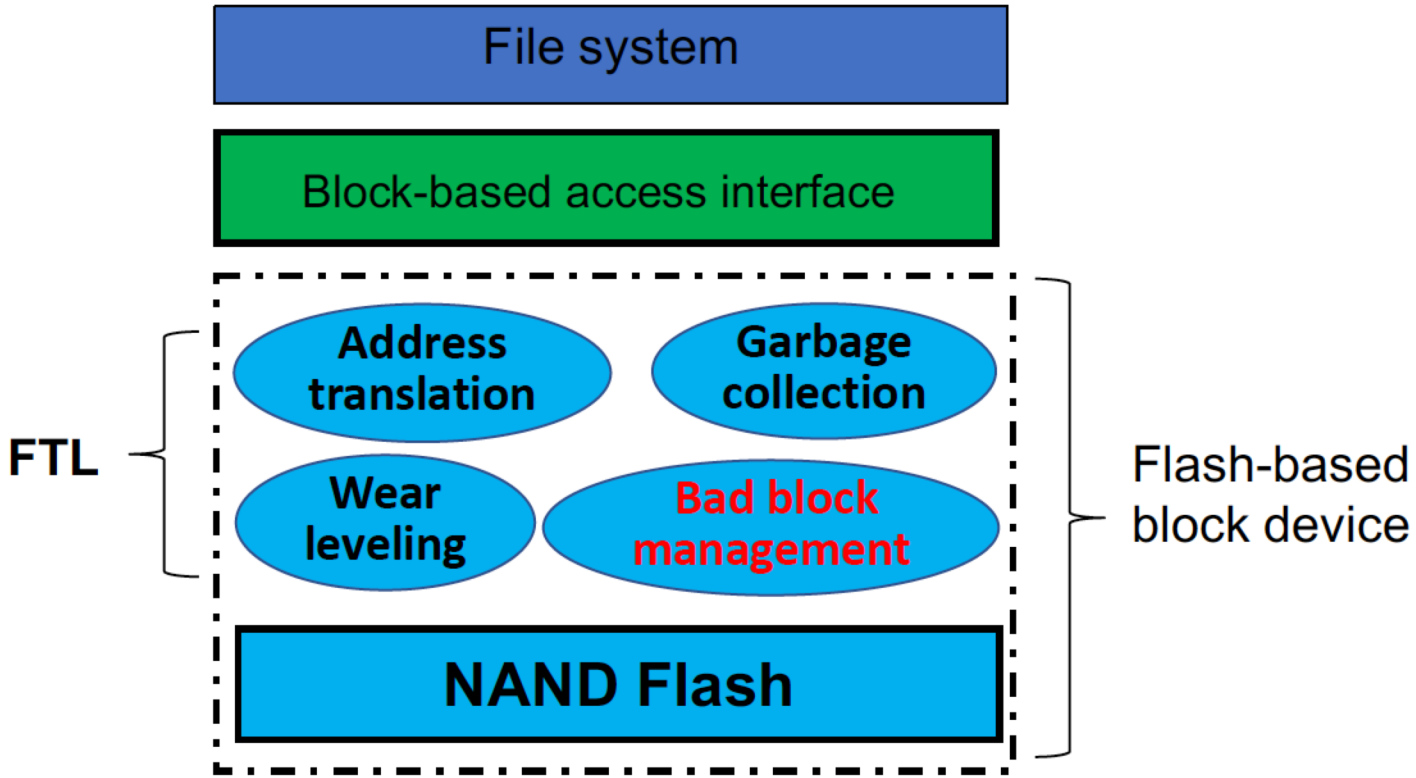
Flash Translation Layer (cont.)

- Wear leveling
  - Each flash block can be programmed/erased for a limited number of times
  - Distribute writes evenly across the flash to prolong its lifetime

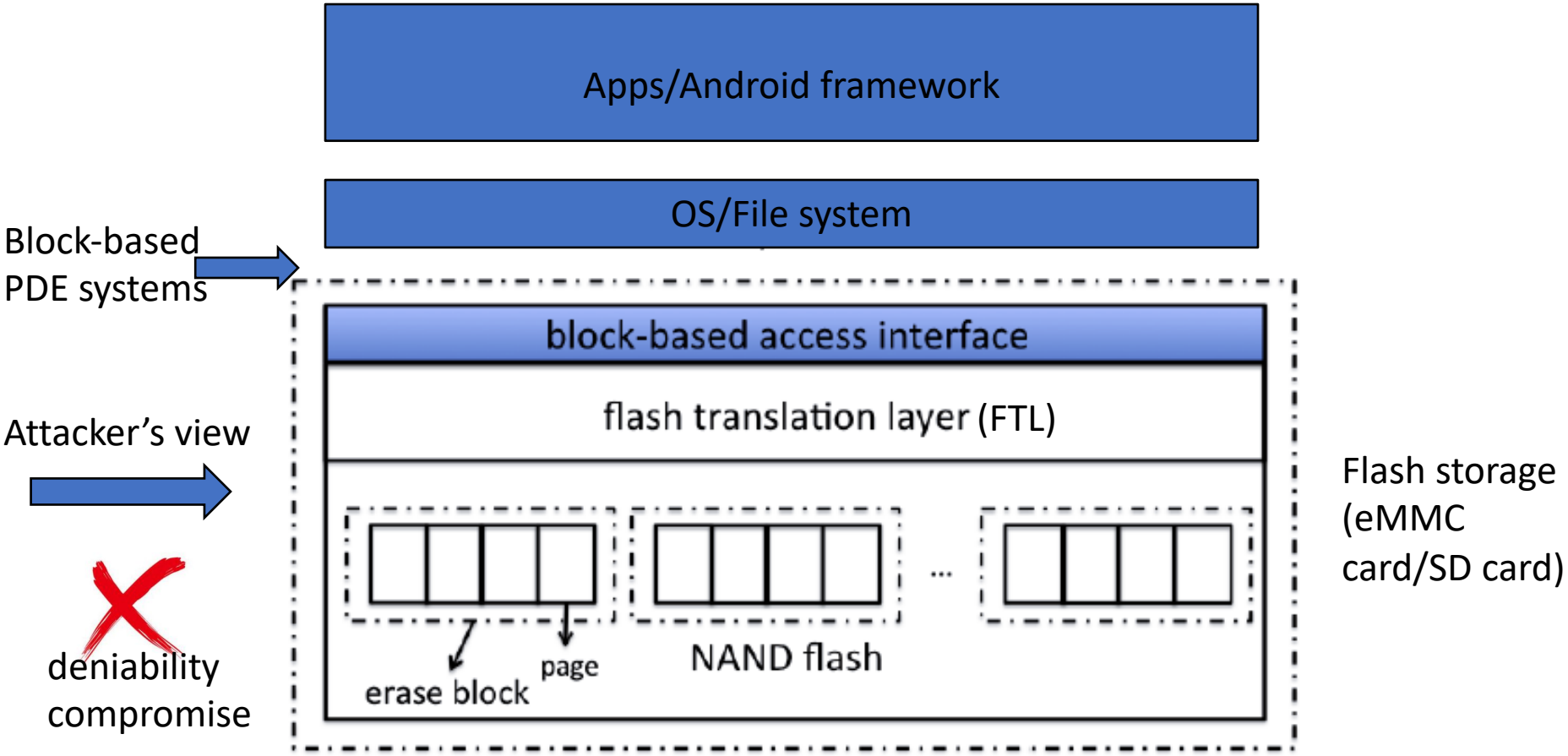


Flash Translation Layer (cont.)

- Bad block management
  - Regardless how good is the wear leveling, some flash blocks will eventually turn “bad” and cannot reliably store data
  - Bad block management is to manage these bad blocks



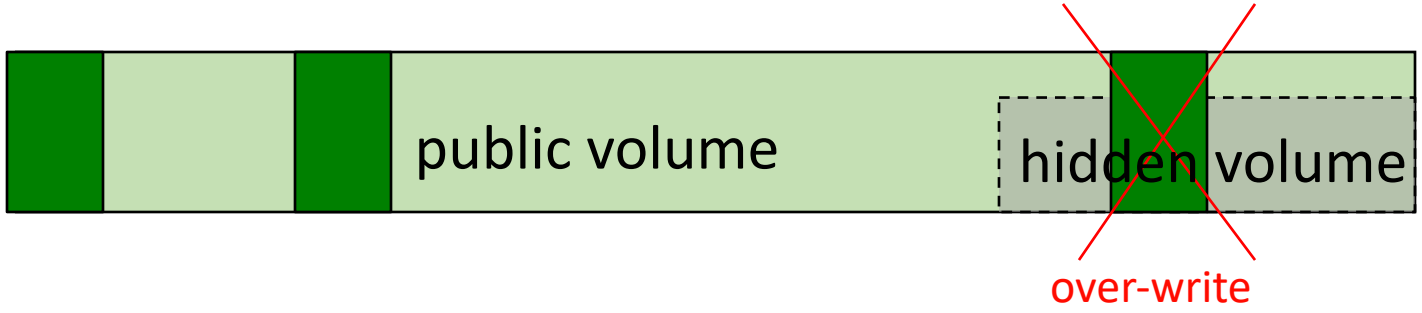
Deniability May be Compromised When Deploying Hidden Volume on The Block Layer



By obtaining a view in the flash memory, the adversary may be able to observe those unexpected "traces" of the hidden sensitive data (The trace are due to handling the special nature of ash memory)

Any Other Issues?

- The data written to the public volume (if not written sequentially) may over-write the data in the hidden volume
  - The hidden volume is part of the public volume



Paper Presentation

- DEFTL: Implementing Plausibly Deniable Encryption in Flash Translation Layer

- Presented by Niusen Chen (guest presenter from MTU Security and Privacy lab)