CS 5472 - Advanced Topics in Computer Security

Topic 10: Secure Hardware and Quantum Cryptography (1)

Spring 2026 Semester
Instructor: Bo Chen
bchen@mtu.edu
https://cs.mtu.edu/~bchen
https://snp.cs.mtu.edu

Notes

- Start to prepare your exam early which will be on next Thursday and close book
  - Open book
  - Will review everything on next Tuesday

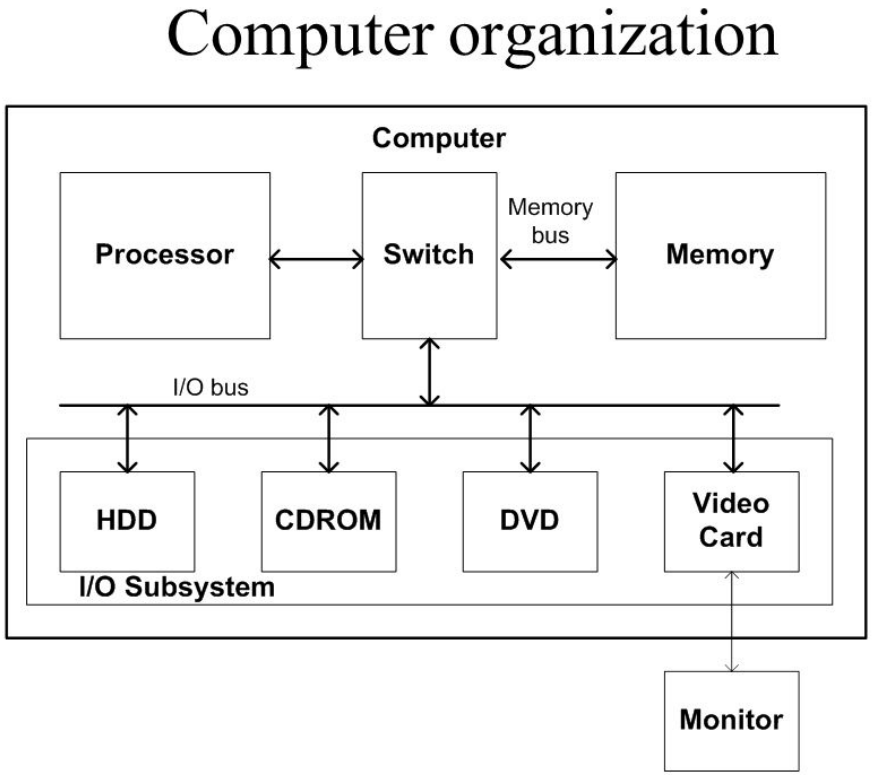
The Focus of Today

- Hardware security
  - The compromise of OS
  - Provide security at the hardware / firmware level (trusted hardware / firmware)

Typical Computer Hardware

- Processor
  - An electronic circuit which performs operations

  on some external data sources (e.g., CPU, GPU)
- Memory
  - Volatile memory (e.g., DRAM, SRAM)

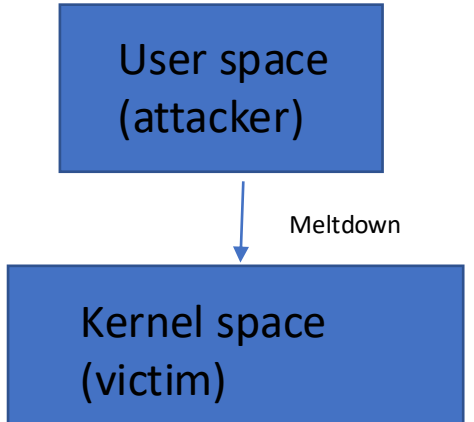


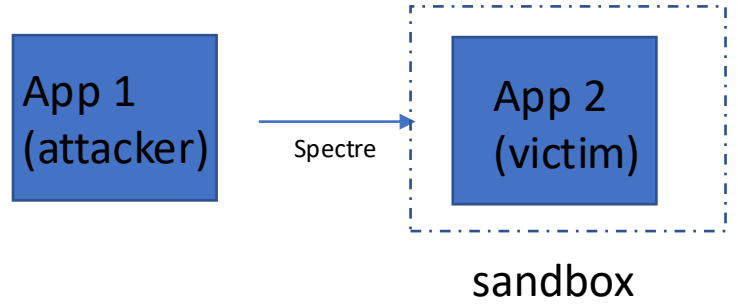
- Peripheral
  - A peripheral device is an ancillary device

  used to put information into and get information out of the computer

Do You Trust Your Own Computer?

- Clearly no
- The malware may compromise the OS/ applications and steal/ modify critical information in both the memory and the external storage
  - Both the OS and the applications are vulnerable
  - The malware can compromise the applications
  - The rootkit can compromise the OS (the rootkit can obtain the root privilege)
- The malware can even take advantage of vulnerabilities in the computer processors to steal critical information
  - Meltdown
  - Spectre





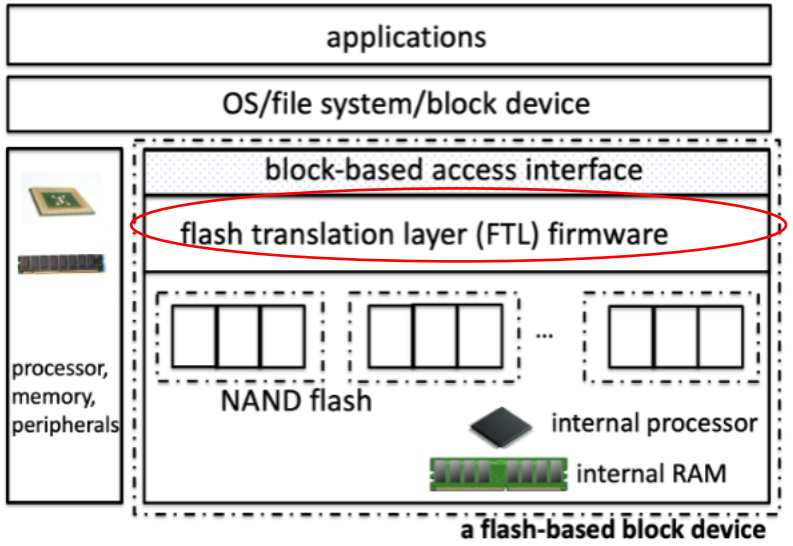
How Can I Ensure The Security of My Computer / Computing Device?

- No software (OS/system software/applications) can be trusted
  - They are all vulnerable
- What is the root of trust?
  - Blockchain?
- The only option is to explore the security features in the hardware components equipped with the computing device
  - A flash storage device has an isolated flash translation layer (FTL)
    - SSD, USB, UFS cards, SD/ mini SD/ Micro SD cards, eMMC cards
  - The processor equipped with the device may incorporated some sort of trusted computing features

Utilizing The FTL to Enhance Security

- The flash translation layer (FTL) is isolated from

to the OS by the storage hardware, and the OS cannot touch it



- We can integrate some of the security functionality

in the FTL, which cannot be compromised by the

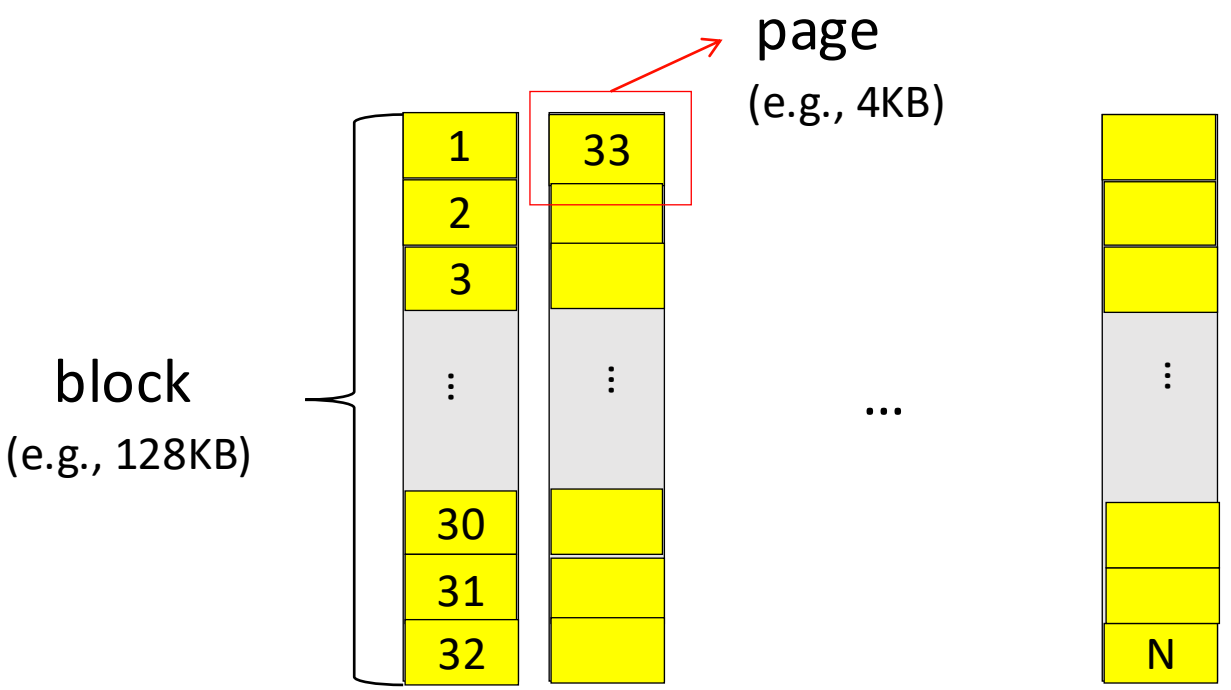
OS-level malware

  - Malware detection
  - Data protection and recovery
  - Access control

NAND Flash Memory

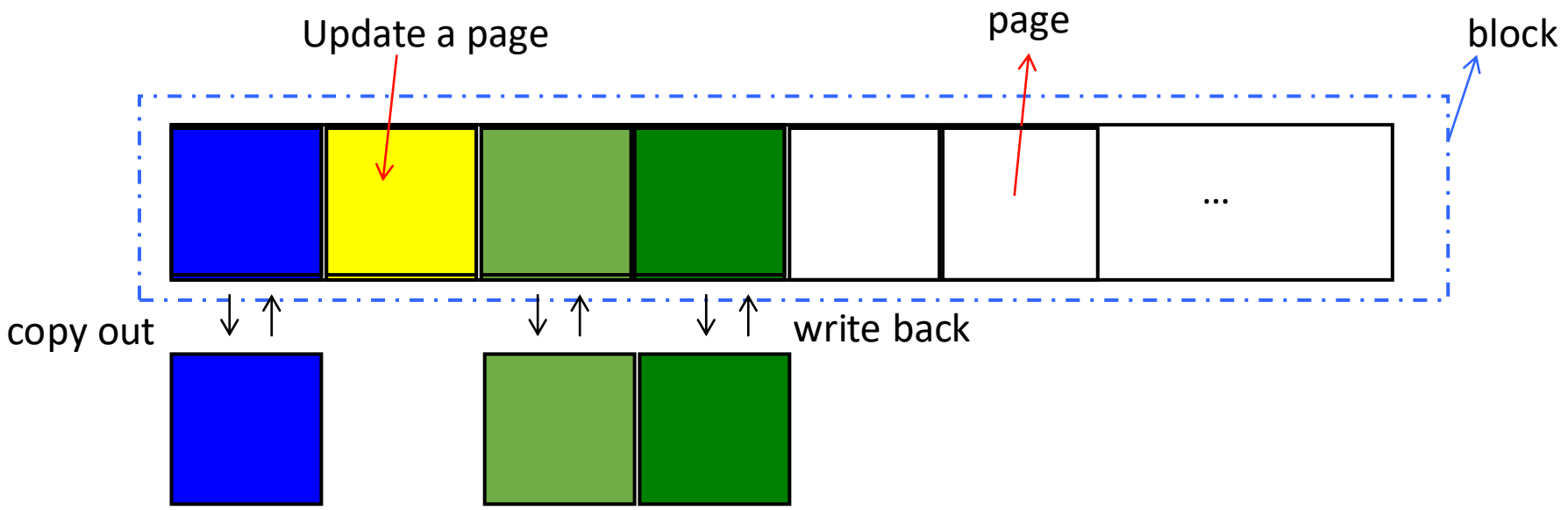
- NAND flash memory as mass storage
  - SSD (used widely in personal computers and servers)
  - Flash memory cards like SD cards, MMC card, UFS cards (used broadly in mobile devices/IoT devices)

- NAND flash organization
  - Block
  - Page



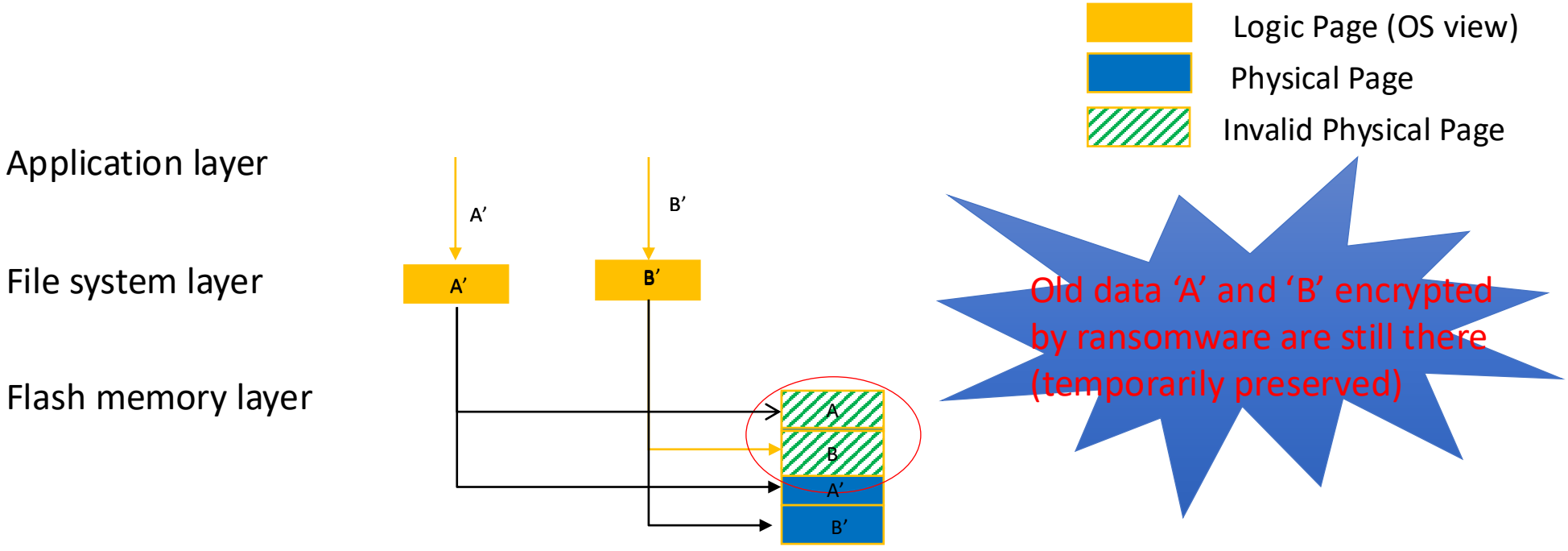
Special Characteristics of Flash Memory

- 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

Out of Place Update - Flash Memory



Utilizing Trusted Hardware to Enhance Security

- Trusted platform module (TPM): also known as ISO/IEC 11889, is an internatio standard for a secure cryptoprocessor, a dedicated microcontroller designed t secure hardware through integrated cryptographic keys
  - Need an independent co-processor
  - Disadvantages: need to purchase additional hardware, a lot of energy consumption

- Trusted execution environment (TEE): a secure area of a main processor
  - A TEE as an isolated execution environment provides security features such as isolated execution, integrity of applications executing with the TEE, along with confidentiality of their assets
  - It guarantees code and data loaded inside to be protected with respect to confidentiality and integrity
  - Advantage: **TEE is a part of the existing processor, and no need to purchase additional hardware**

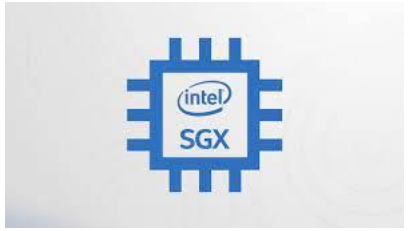
Hardware Support of TEE (Trusted Execution Environment)

- Intel
  - Software Guard Extensions (SGX)
  - Trust Domain Extensions (TDX)
- AMD
  - Secure Encrypted Virtualization (SEV)
- ARM (mostly for embedded systems and mobile devices)
  - TrustZone
  - Arm Confidential Compute (CCA)
- AWS Nitro System
- NVIDIA GPU
  - H100/H200 supports confidential computing

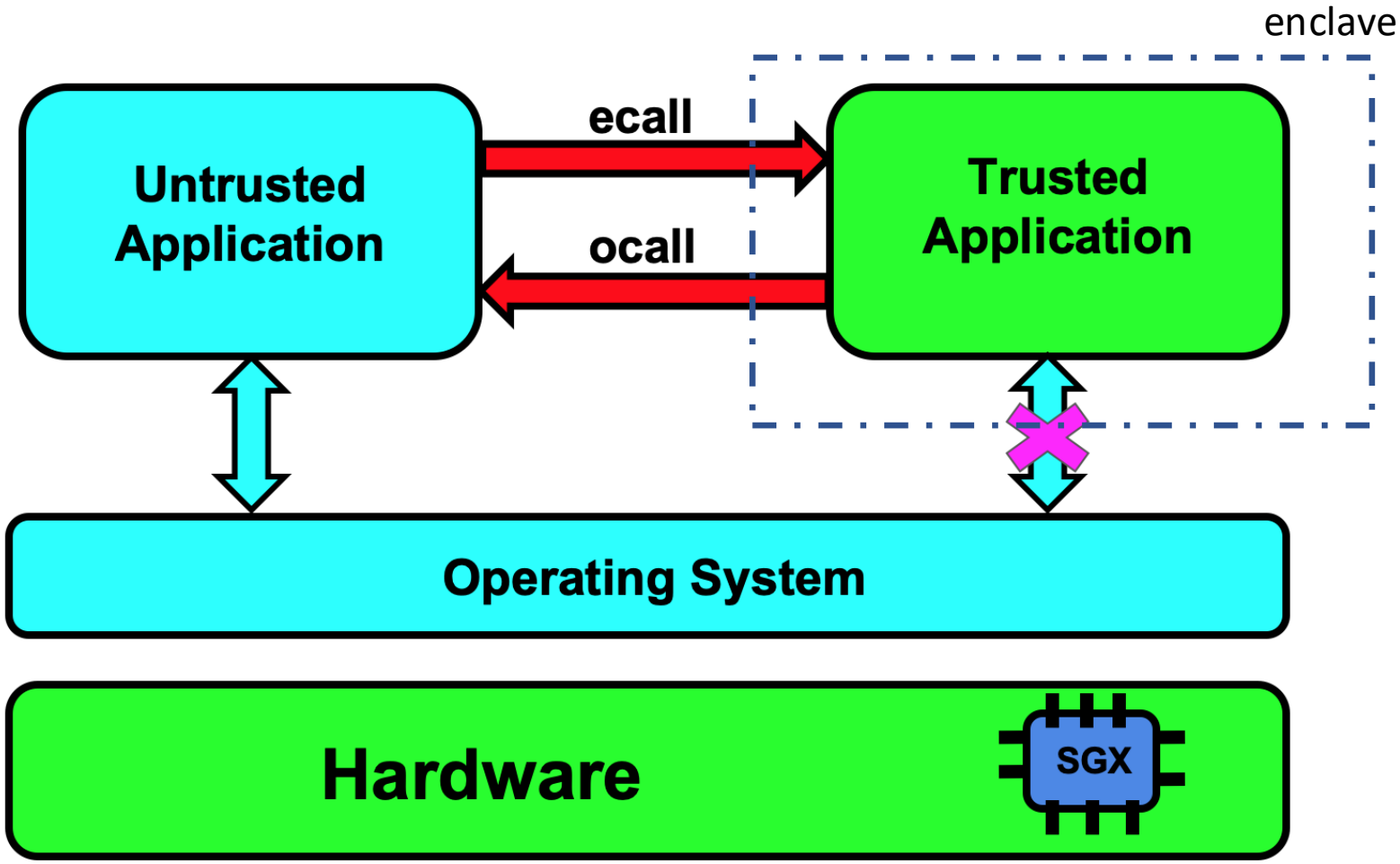
Intel SGX

- **Intel** Software Guard Extensions (SGX): integrated into Intel processors 7th generation (or later)
  - **Personal computers/Servers**
  - A set of security-related instruction codes that are built into some modern Intel CPUs
  - A pivot by Intel in 2021 resulted in the deprecation of SGX from the 11th and 12th generation Intel Core Processors, but development continues on Intel Xeon for cloud and enterprise use.

- Allow user-level as well as operating system code to define private regions of memory (enclaves)
  - The enclave is encrypted/ decrypted using keys only accessible to the processor (the keys are not able to be extracted by OS/ software)
  - Both the confidentiality and integrity of the contents in the enclave are protected and unable to be either read or saved by any process outside the enclave itself
  - The assumption is that Intel is trusted



SGX - Architecture



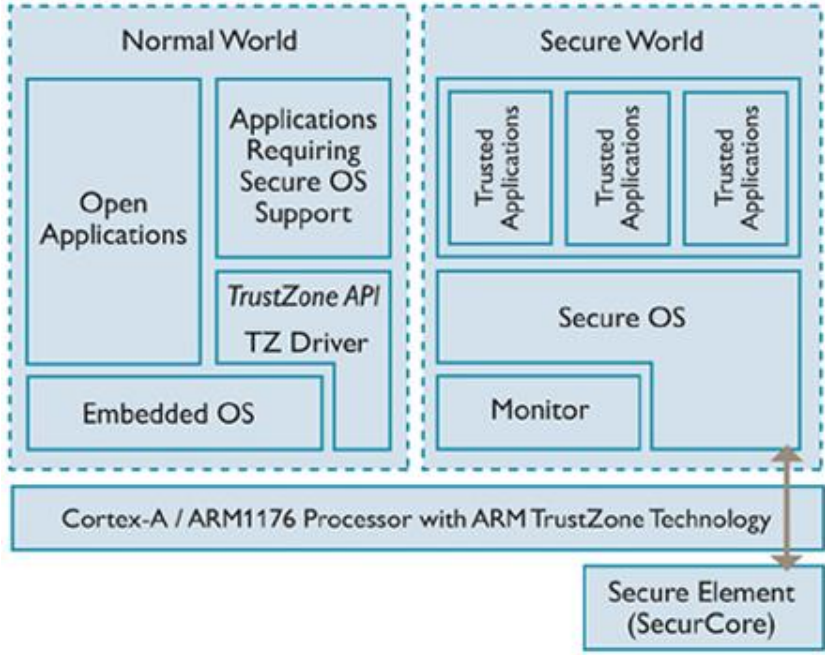
A secure encrypted memory with both confidentiality and integrity guarantee

Attestation ensures trusted app really runs in SGX

ARM TrustZone

- Integrated into most of Arm Cortex-A processors; also in the latest Cortex-M23 and Cortex-M33 processors
  - **Mobile devices**
- Creating two execution environments which run simultaneously on a single processor:
  - A secure execution environment (**secure world**): can be used to run sensitive applications
  - a non-secure execution environment (**normal world**): can be used to run non-sensitive applications

TrustZone®
System Security by ARM



Secure Decentralized Cloud Storage

- We have learned decentralized cloud storage in Topic 2
  - FileCoin relies on the blockchain to establish the root of trust
- Blockchain is not efficient and suffers from the scalability issues
- Can we instead use secure hardware and trusted firmware to establish the root of trust?
  - For data stored in each storage peer, we can rely on the TEE and FTL to verify the integrity of the data (self verification)
  - Once we have detected any corrupted data, we can rely on the TEE and FTL to repair the data without relying on other peers (self repair)

Paper Presentation

- Hardware-assisted Secure Decentralized Cloud Storage via Self-audit and Self-repair

- Josh Dafoe