CS 5472 - Advanced Topics in Computer Security

Topic 10: Secure Hardware and Quantum Cryptography (1)

Spring 2023 Semester
Instructor: Bo Chen
bchen@mtu.edu
https://cs.mtu.edu/~bchen
https://snp.cs.mtu.edu

Notes

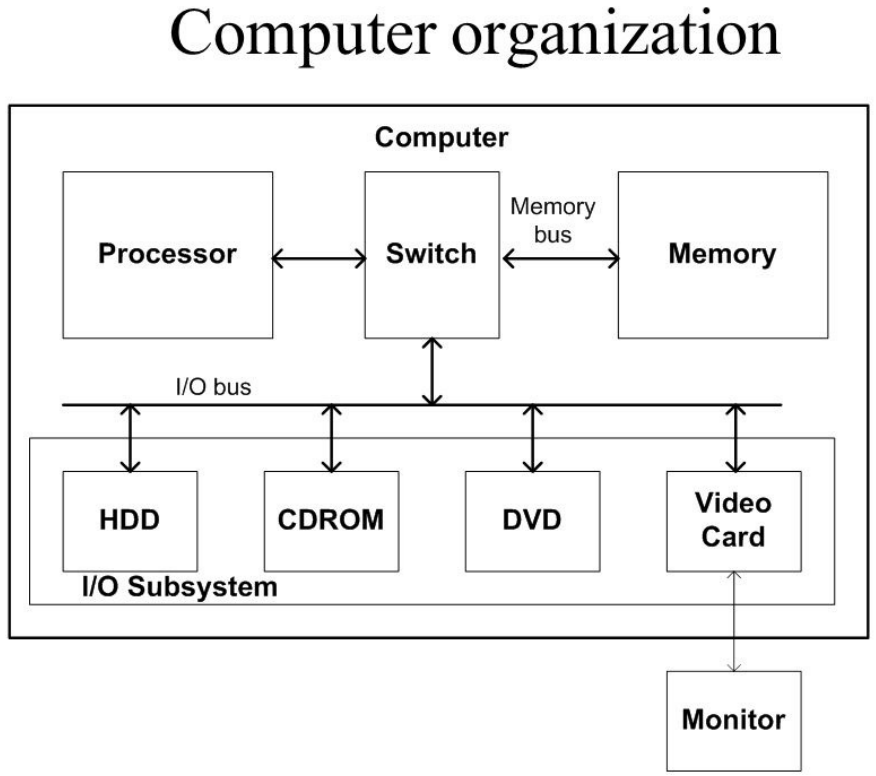
- Start to prepare your exam early which will be on next Thursday and close book
  - Will review everything on next Tuesday
- The grade for the second round of paper presentation has been posted

The Focus of Today

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

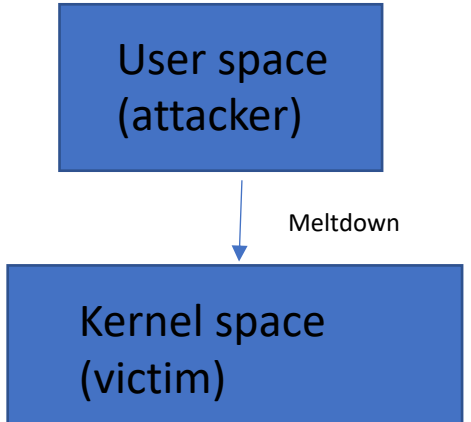
Typical Computer Hardware

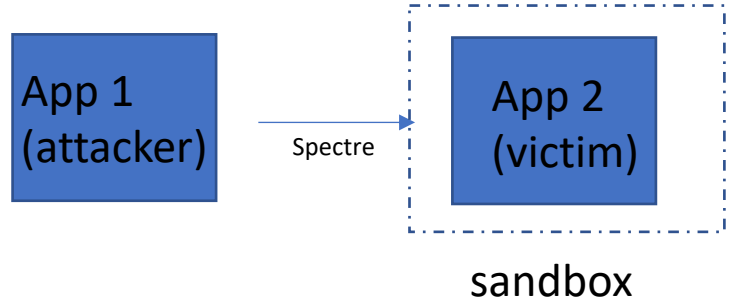
- Processor
  - An electronic circuit which performs operations on some external data sources (e.g., CPU, GPU)
- Memory
  - Volatile memory (e.g., DRAM, SRAM)
- Peripheral
  - A peripheral device is an ancillary device used to put information into and get information out of the computer



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





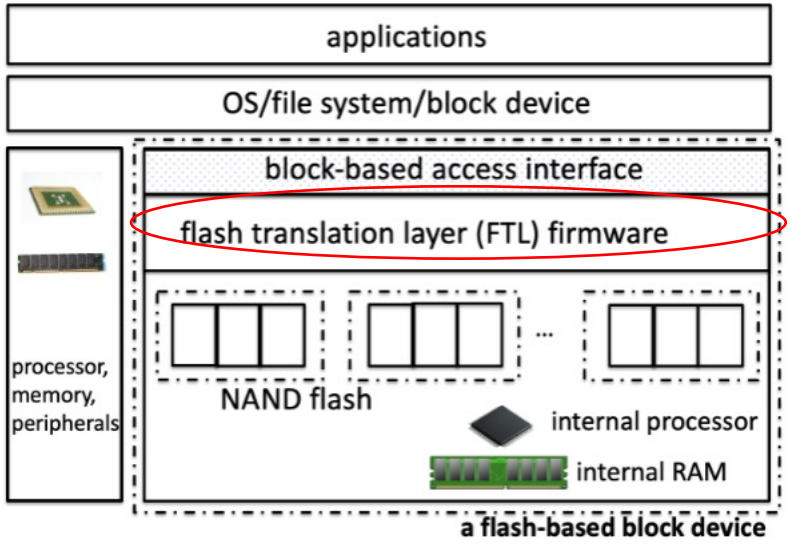
How Can I Ensure The Security of My Computer/Computing Device?

- No software (OS/system software/applications) can be trusted
  - They are all vulnerable
- What is the root of trust?
- 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

FTL may not be a good way, as it is part of the I/O device, and staying far away from the host computing device; also, it is typically run by low-end hardware

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)

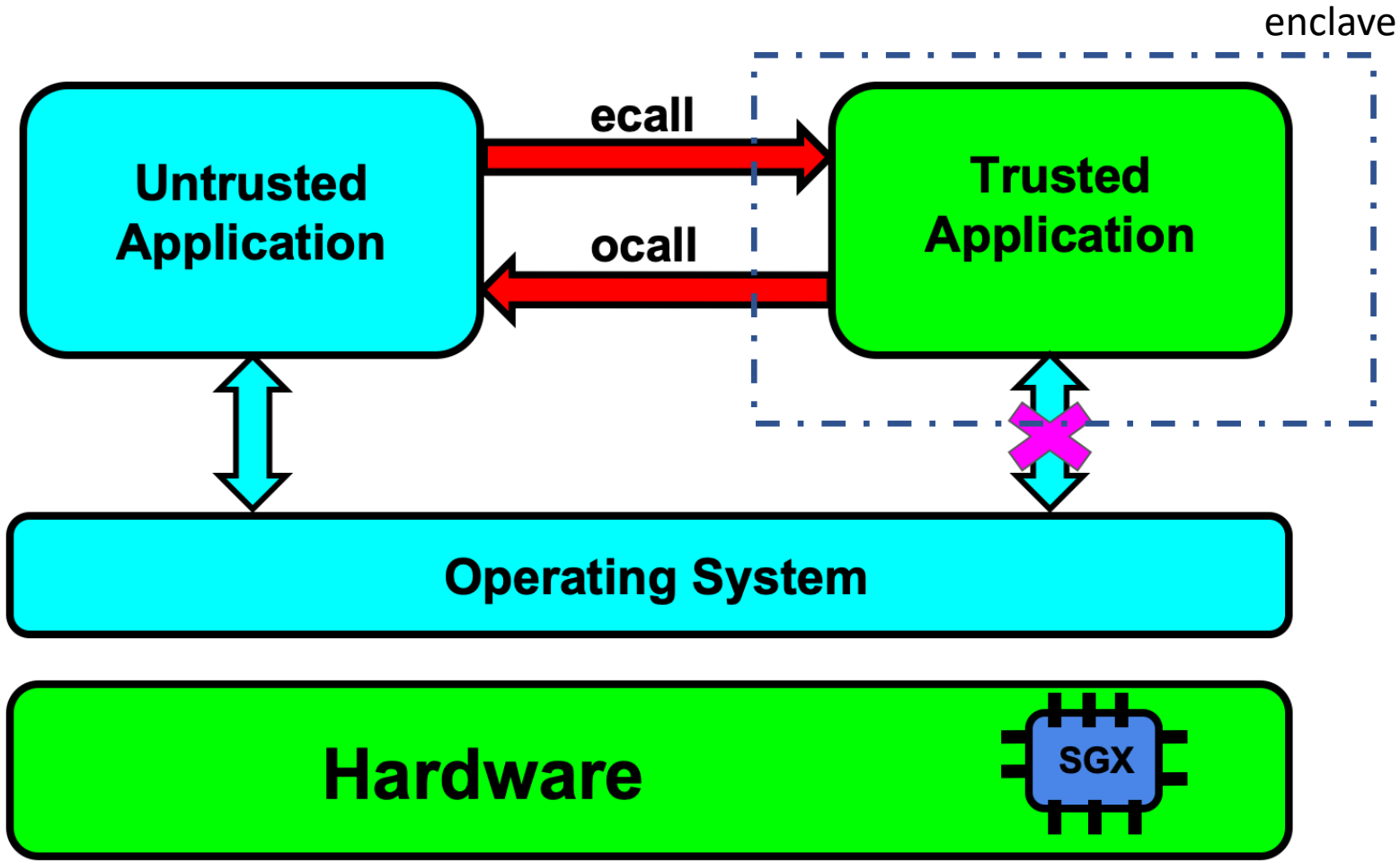
- Intel
  - Trusted Execution Technology
  - Software Guard Extensions (SGX)
  - "Silent Lake" (available on Atom processors)
- AMD
  - Secure Encrypted Virtualization (SEV)
  - Secure Memory Encryption (SME)
  - Transparent SME (TSME)
- ARM (mostly for embedded systems and mobile devices)
  - TrustZone
- IBM
  - IBM Secure Service Container
  - IBM Secure Execution
- Etc.

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



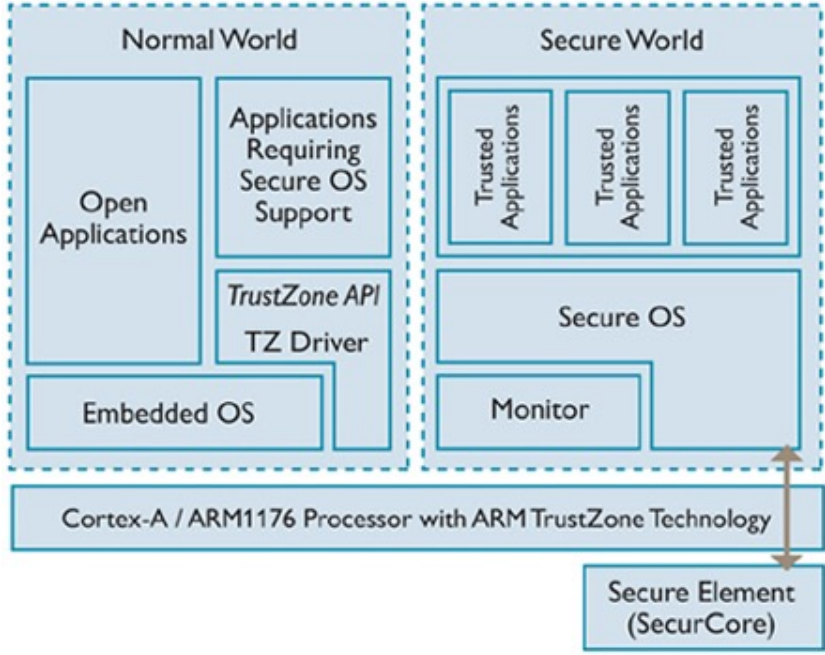
A secure encrypted memory with both confidentiality and integrity guarantee

Attestation ensures trusted app really runs in SGX

ARM TrustZone

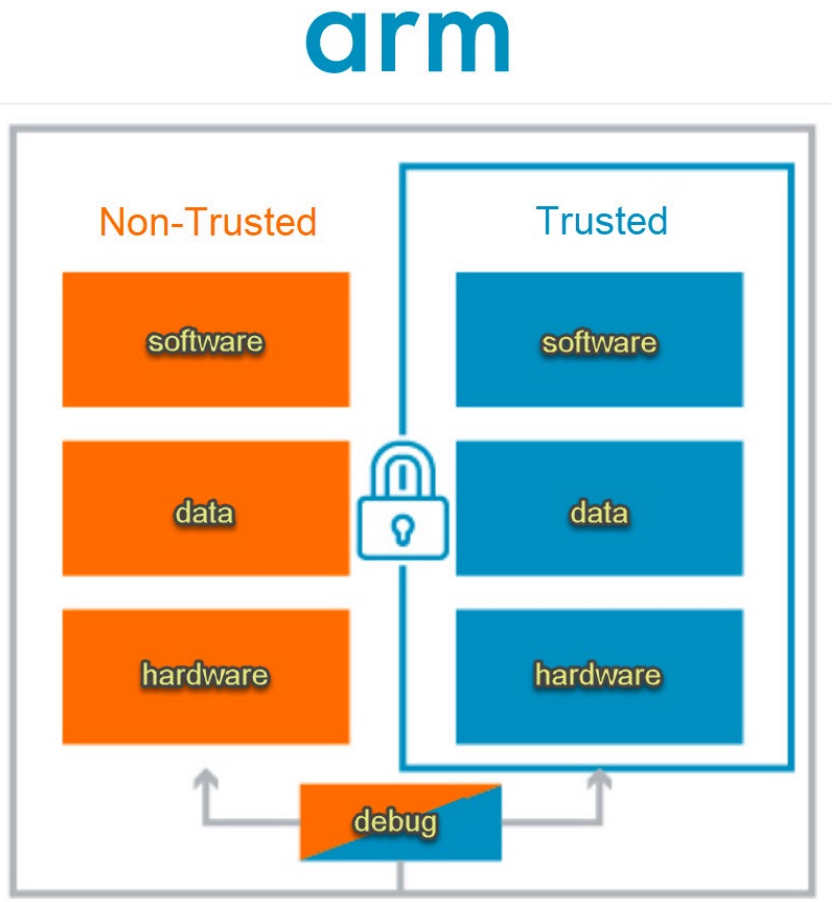
- Integrated into most of Arm Cortex-A processors; also in the latest Cortex-M23 and Cortex-M33 processors
  - **Mobile devices**
- Creating two execution environments which run simultaneously on a single processor:
  - A secure execution environment (**secure world**): can be used to run sensitive applications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

TrustZone®
System Security by ARM



ARM TrustZone (cont.)

- Each world operates independently when using the same processor
- The processor can only run at one world at a certain time (the processor is time slicing, with actual parallel computation)
  - A special **Non-Secure (NS) bit** determines in which mode the processor is currently working
  - A **privileged instruction Secure Monitor Call (SMC)** switches the processor between the normal world and the secure world
- Memory/ peripherals are aware of the corresponding world of the core and, applications running in the normal world cannot have access to the memory space of the secure world



How To Protect The Database If The Database Server is Untrusted

- Any database system typically has two components:
  - Database: storing all the data, including sensitive data
  - Database server: manage the database
- The database can be protected by performing encryption
- But database server may be compromised
  - The database server is hosted in the untrusted public cloud
  - The administrator is malicious
  - The OS is compromised by the malware
- The database server still needs to decrypt the database upon perform query and, if the database server is compromised, the database will be also compromised
- How can we provide the confidentiality, integrity, freshness of the data even if the database server is compromised?
  - SGX

Paper Presentation

- EnclaveDB: A Secure Database using SGX