Hardware Security

Asst. Prof. Mihai Bucicoiu

SYSTEMS LABORATORY
Computer Science & Engineering Department

This lecture

- Is **not** about:
  - Hardware Trojan
  - Side-channel attacks on hardware
  - Physically Unclonable Function
  - Other: e.g., Cold boot attack

- Is about:
  - Root-of-trust
  - Hardware- assisted computer security: TPM, ArmTrustZone, IntelSGX

Trustworthy Computing

- Goal: Protect data from misuse
- Approach: Turn a portion of a platform into a trustworthy environment
- TCB is not sufficient

Security Properties [1]

- Isolated Execution
  - Inside a Trusted Execution Environment (TEE)
- Secure Storage
  - Integrity, confidentiality
- Attestation (remote and local)
  - Data given only to the trusted machine
- Secure Provisioning
  - Channel for sending data
- Trusted Path
  - Communication channel for peripherals (Secure I/O)

Trusted Platform Module (TPM)

Why?

- “For years Bill Gates has dreamed of finding a way to make the Chinese pay for software, TC looks like being the answer to his prayer.” by Ross Anderson

TPM history [2]

- The Trusted Computing Platform Alliance (TCPA) The Trusted Computing Platform Alliance (TCPA)
  - Established by the 5 founders in 1999: Intel, AMD, IBM, HP and MSFT
  - TPM v1
- The Trusted Computing Group (TCG)
  - Established in March 2003 as continuation of TCPA
  - TPM v2

TPM Capabilities [3]

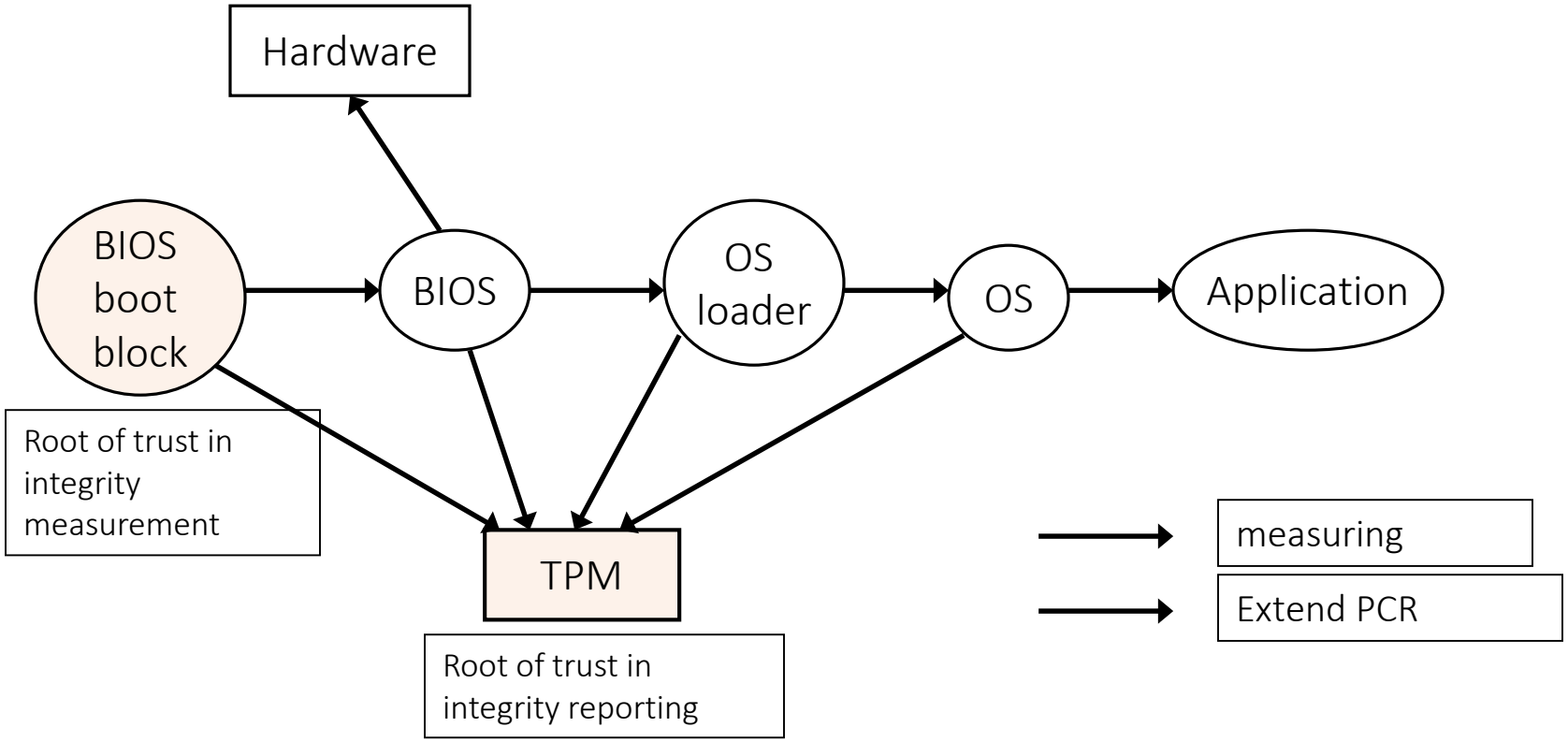
- Provides three root of trusts:
  - Root of trust for measurement (RTM) a trusted implementation of a hash algorithm
  - Root of trust for storage (RTS) a trusted implementation for one or more secret keys —the storage root key (SRK)
  - Root of trust for reporting (RTR) a trusted implementation for a secret key representing a unique platform identity, the endorsement key, (EK).
    - Signed by the platform vendor.

TPM Capabilities

- ‘Platform Configuration Registers’ (PCR)
  - Can be read
  - Can only be extended, not writable
- Migratable vs non-migratable keys
  - EK and SRK never leave TPM

Trusted/Secure Boot

- After boot, PCRs contain hash chain of booted software



Secure Storage

- Step 1: TPM_TakeOwnership(OwnerPassword, …)
  - The SRK is created and can be deleted

- Binding/Unbind vs Sealing/Unsealing
  - Sealing is an extension to binding.
  - Contrary to binding, only non-migratable storage keys can be used to seal data.
  - Consequently, the encrypted data is always bound to a specific platform.

Attestation (remote and local)

- Why is remote attestation different from local attestation?
  - Answer: Because one's computation capabilities (i.e., local one has do to the cryptographic part on paper)

Attestation (remote and local)

- Step 1: Create Attestation Identity Key (AIK)
- Step 2: Sign PCR values (after boot)
- Step 3: Validate signed PCRs
  - How to do that for local attestation?

- Problems?
  - It only validates the loaded code, not the running one
  - Private attestation (cannot tell what machine it came from)
    - Privacy CA

Secure Provisioning

- Can be done using sealing
- Similar to local attestation

Trusted Path

- No real support from TPM
- Using Dynamic Root of Trust

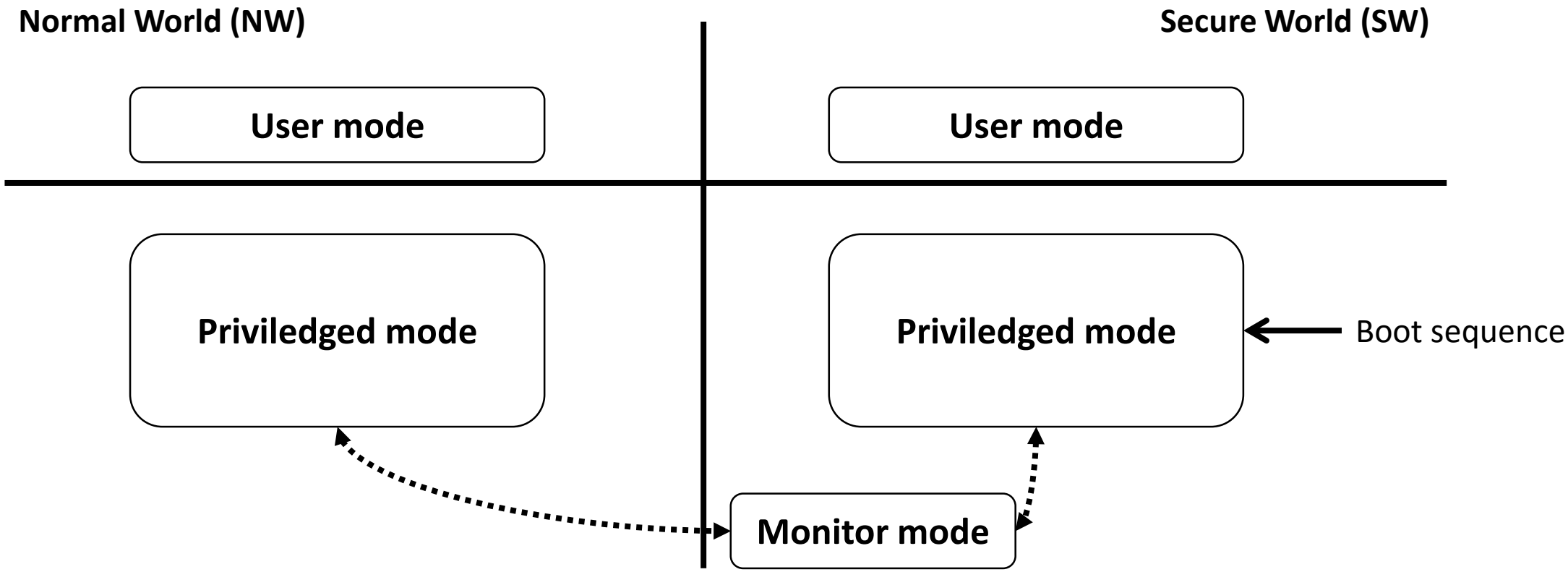
TPM Controversy

- Could be used quite coercively
  - E.g., web pages only readable by browser X
  - Documents only usable with word processor Y

- Vendor lock-in

ARM TrustZone

TrustZone Capabilities



- The entry to monitor execute the Secure Monitor Call (SMC)

Isolated Execution

- By design
- Two virtual Memory Management Units (one for each state)
  - The secure world can access the normal world data
- Can also implement secure boot

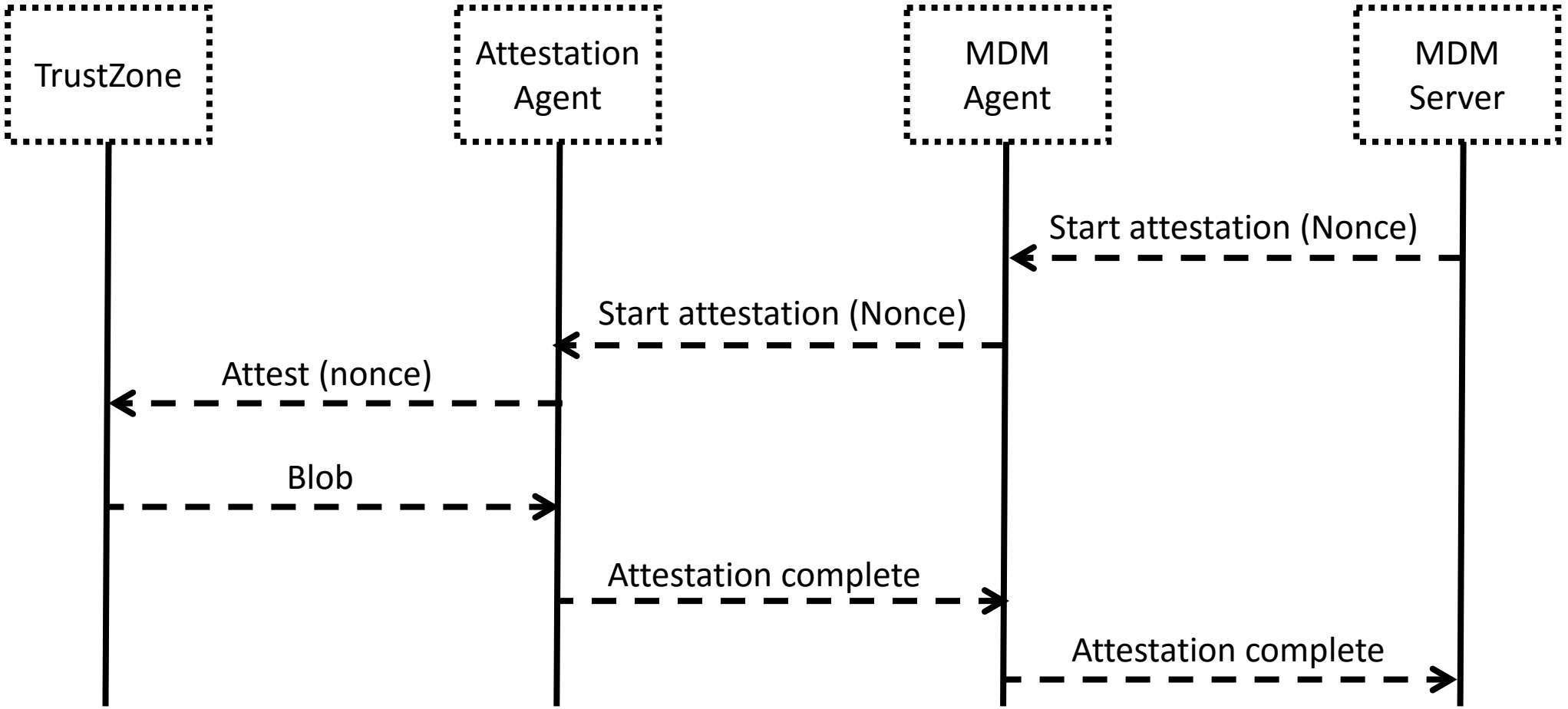
Attestation – Case Study KNOX

- Samsung's TrustZone-based Integrity Measurement Architecture (TIMA)
- TIMA Periodic Kernel Measurement (PKM)
- TIMA Real-time Kernel Protection (RKP)
  - intercepts critical kernel events, which are then inspected in TrustZone

Attestation – Case Study KNOX

- Attestation Blobs are signed by TIMA
- Unique device public/private key pair (starting with the Note 3)
- Certificate for device key is signed with Samsung root key
- TIMA generates an attestation public/private key pair, and signs a certificate for the attestation key using the device private key
- Attestation private key is used to sign data inside attestation blob

Attestation – Case Study KNOX



SYSTEMS LABORATORY

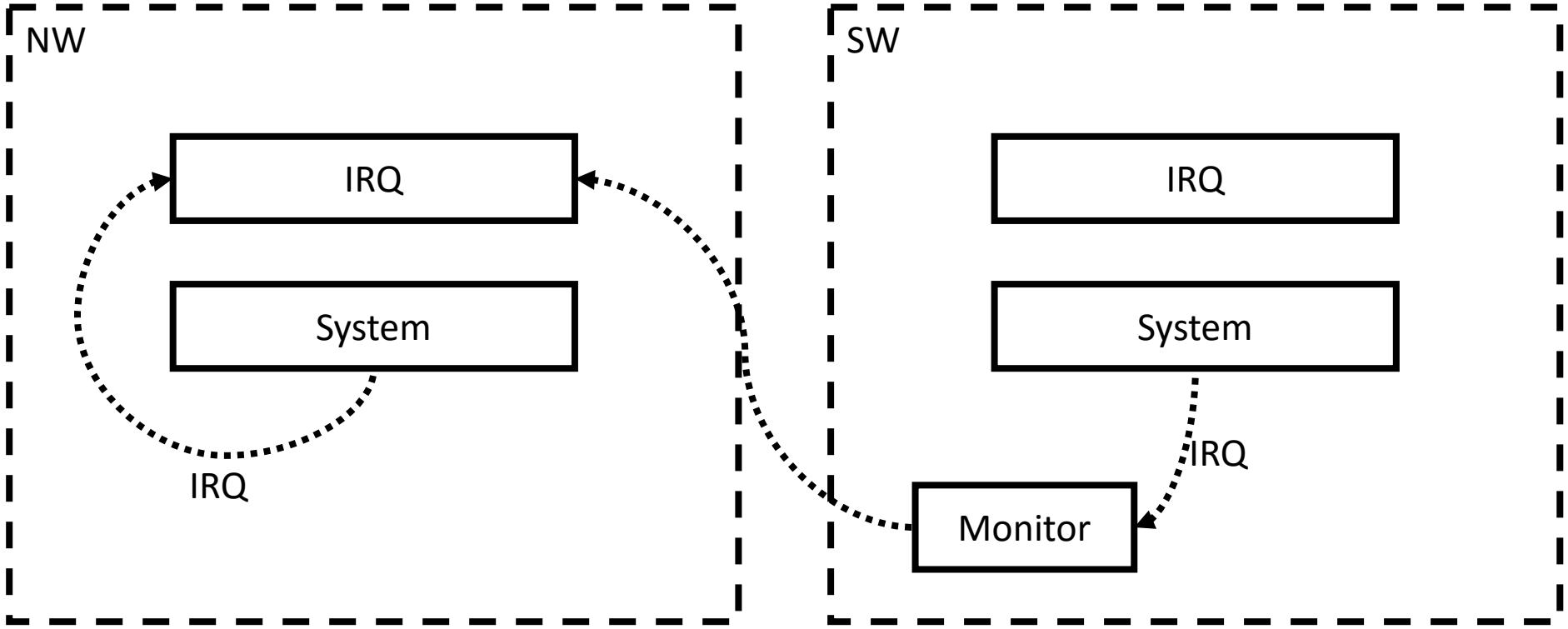
Computer Science & Engineering Department

Other capabilities

- Secure Storage and Provisioning can be implemented using TIMA

Trusted Path

- The ability to trap IRQ and FIQ directly to the monitor



TrustZone Discussion

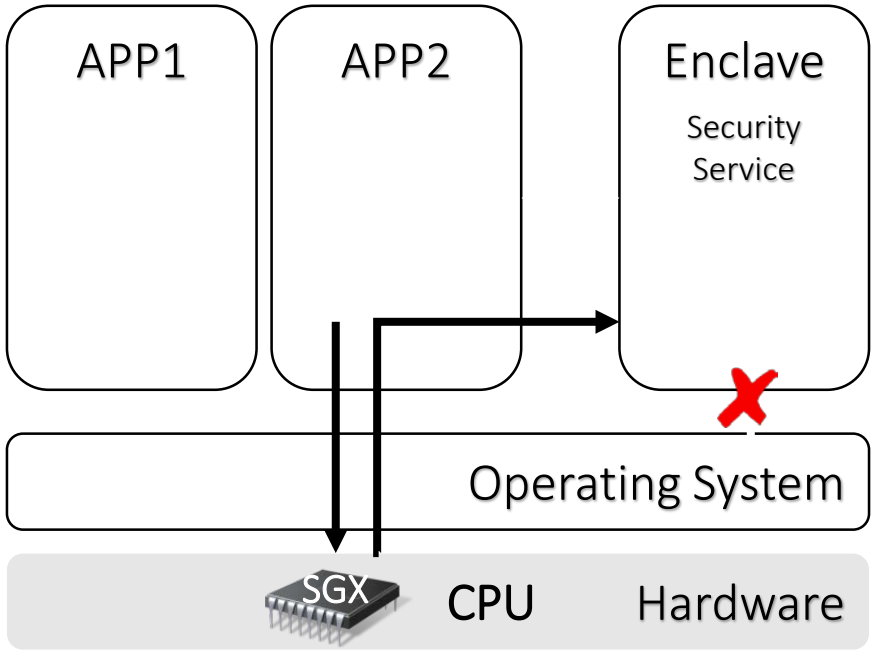
- Vulnerabilities in the TEEOS (CVE-2015-4421)
- Closed system for third application development
- Only one compartment for TCB
- No Virtualization support

Intel Software Guard Extensions (SGX)

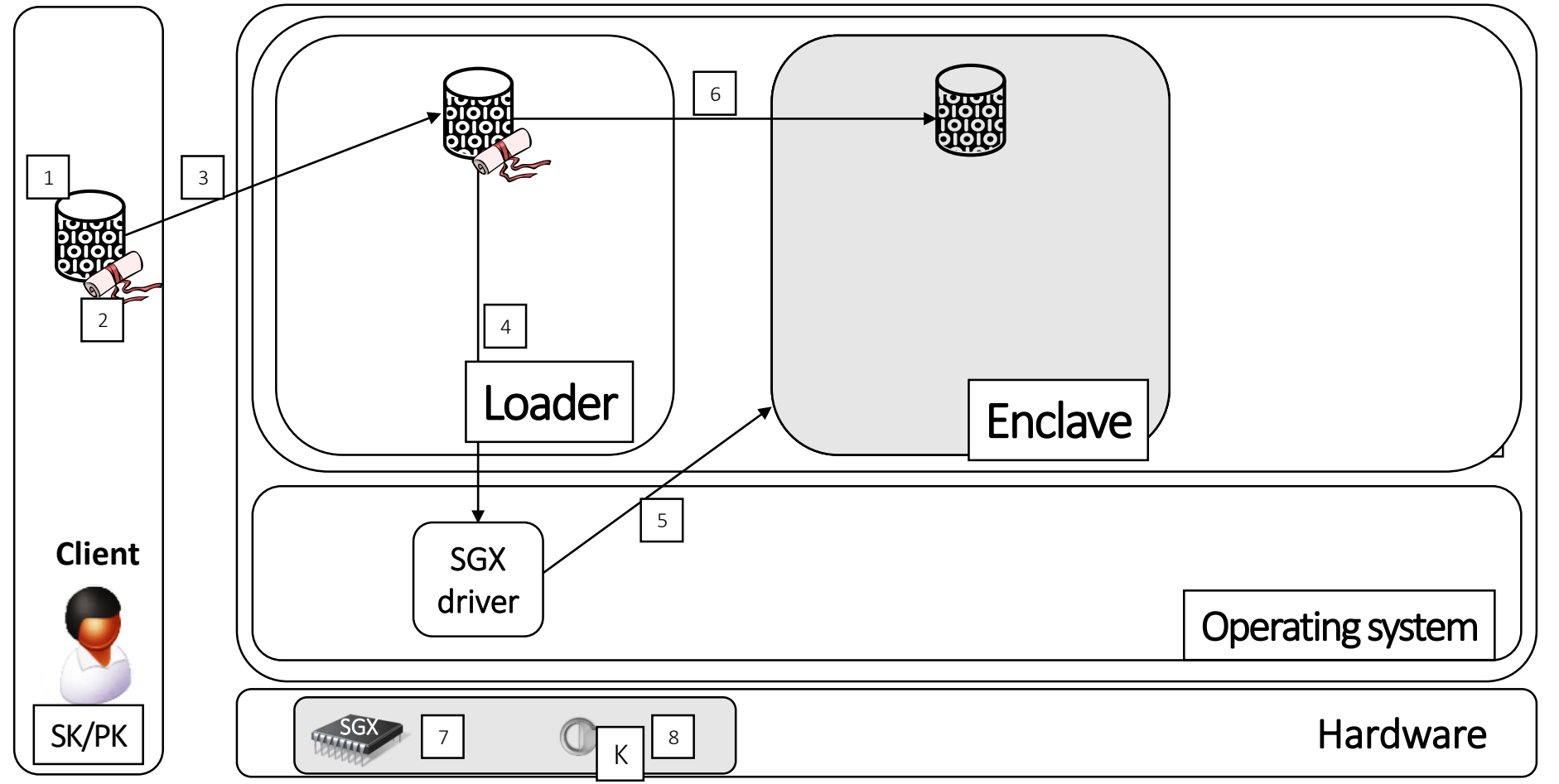
SGX Capabilities

- Security critical code isolated in enclave
- Only CPU is trusted
  - Transparent memory encryption
- Enclaves cannot harm the system
  - Only unprivileged code (CPU ring3)
  - Memory protection
- Designed for Multi-Core systems
  - Multi-threaded execution of enclaves
  - Parallel execution of enclaves and untrusted code
  - Enclaves are interruptible

Isolated Execution



Trusted | Untrusted



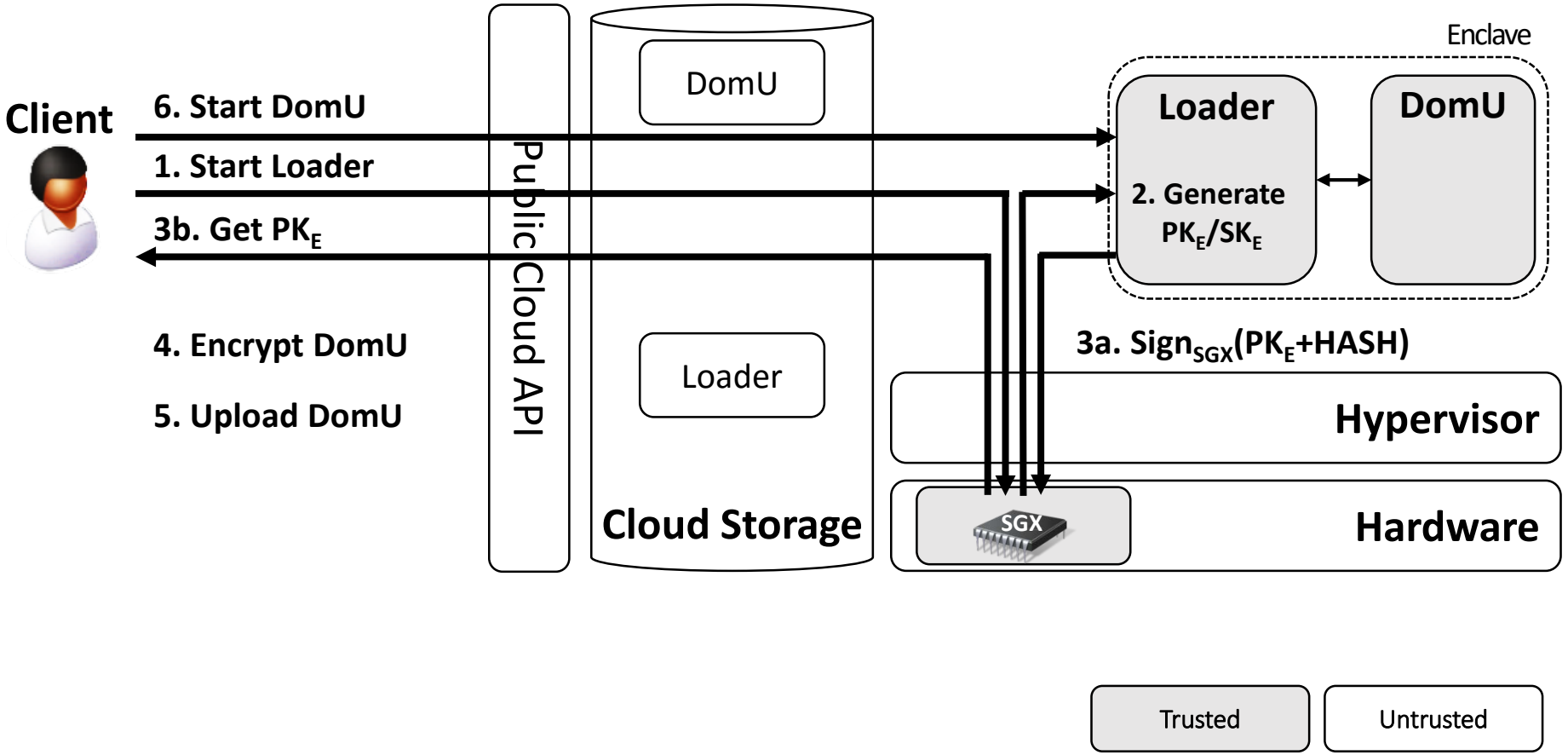
1. Create App
2. Create app certificate (includes HASH(App) and Client PK)
3. Upload App to Loader
4. Create enclave
5. Allocate enclave pages
6. Load & Measure App
7. Validate certificate and enclave integrity
8. Generate enclave K key
9. Protect enclave

Trusted | Untrusted

Attestation (remote and local)

- Yes, built-in with SGX
- An enclave can request a HW-signed REPORT
- In local attestation, one enclave can attest its TCB to another one

Secure Provisioning – Use Case VMM



Secure Storage

- Based on the Secure Provisioning of Key

Trusted Path

- Open research question

Open Challenges for SGX

- Malware in enclave
  - Check against blacklist before loading
  - White listed code can be exploited
    - Runtime attacks possible
  - Detect malicious behavior → block enclave
    - Enclave by itself cannot do much harm (memory protection)

Open Challenges for SGX

- VM Migration in the cloud
  - How can it be done transparent to the VM (the VMs OS)

- Side Channel attacks
  - Enclaves are interruptible
  - Caches are not flushed on switching between SGX and non-SGX mode
    - Data oblivious algorithms required [Kreuter et al., USENIX'13]

Comparation

	Isolated Execution	Secure Storage	Remote Attestation	Secure provisioning	Trusted Path
TPM	No	Yes (limited)	Yes	Yes	No
TrustZone	Yes	Yes	Yes	Yes	Yes
SGX	Yes	Yes	Yes	Yes	Probably

Hardware Security Modules (HSM)

HSM functionalities

- A piece of hardware and associated software/firmware that usually attaches to the inside of a PC or server and provides at least the minimum of cryptographic functions.

- Strong random number generation
- A secure time source
- Tamper-resistance

Security Keys [6]

- HSM are exposed to direct access attacks
- Already available in Chrome

References

1. http://repository.cmu.edu/cgi/viewcontent.cgi?article=1096&context=cylab
2. IBM.Press.A.Practical.Guide.to.Trusted.Computing.Jan.2008
3. https://www.cs.ox.ac.uk/files/1873/RR-08-11.PDF
4. http://asokan.org/asokan/Padova2014/tutorial-mobileplatsec.pdf
5. http://resources.infosecinstitute.com/uefi-and-tpm/
6. http://fc16.ifca.ai/preproceedings/25_Lang.pdf

References

7. http://www.cse.unsw.edu.au/~cs9242/15/exam/paper2.pdf
8. http://www.samsung.com/ro/business-images/insights/2015/An_Overview_of_the_Samsung_KNOX_Platform_V1.11-0-0.pdf