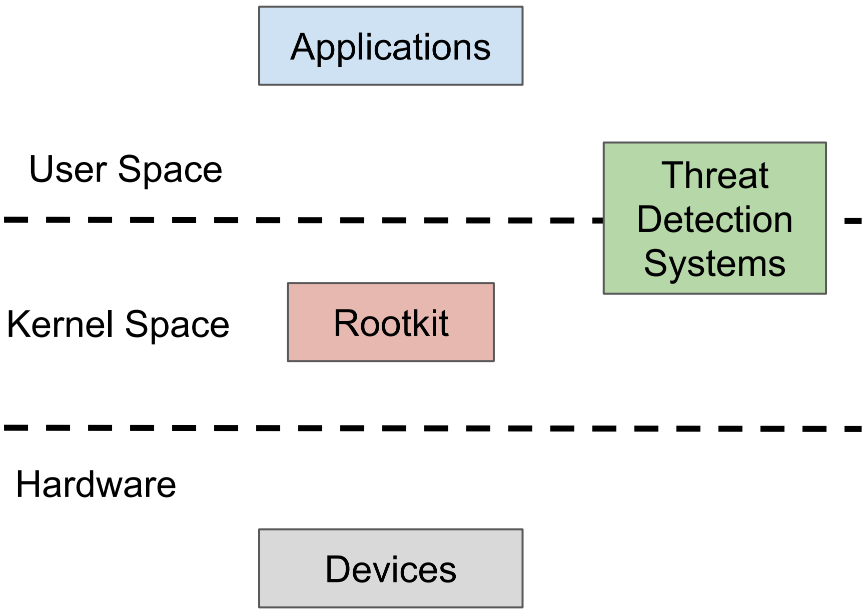
An Enclave Assisted Snapshot-based Kernel Integrity Monitor

Dimitris Deyannis, Dimitris Karnikis, Giorgos Vasiliadis, Sotiris Ioannidis
{deyannis, dkarnikis, gvasil, sotiris}@ics.forth.gr

FORTH
INSTITUTE OF COMPUTER SCIENCE

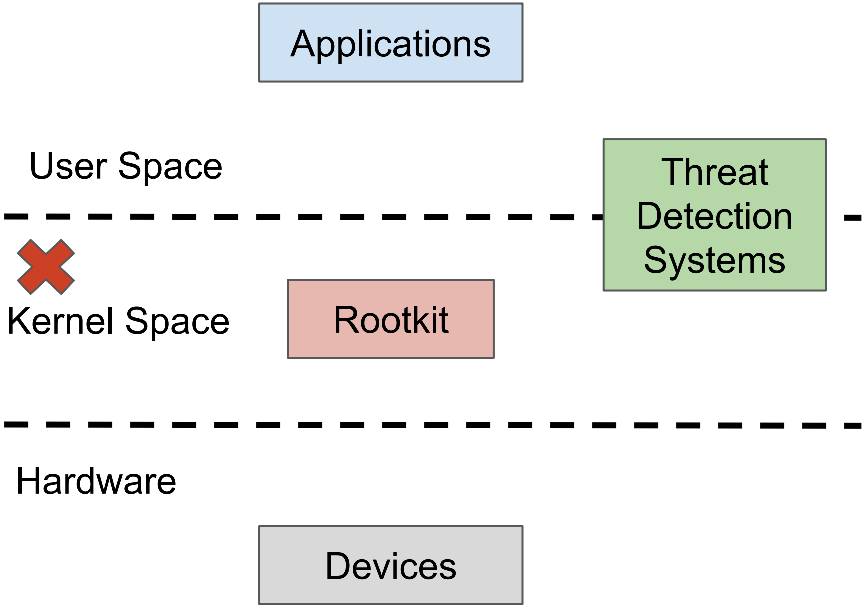
Kernel-level Rootkits

- Provide the most flexibility to attackers
- Compromise the entire OS
- Affect process execution
- Extract security and privacy critical data
- Access to HW devices (NIC, SSDs, etc.)
- Disable threat detection systems



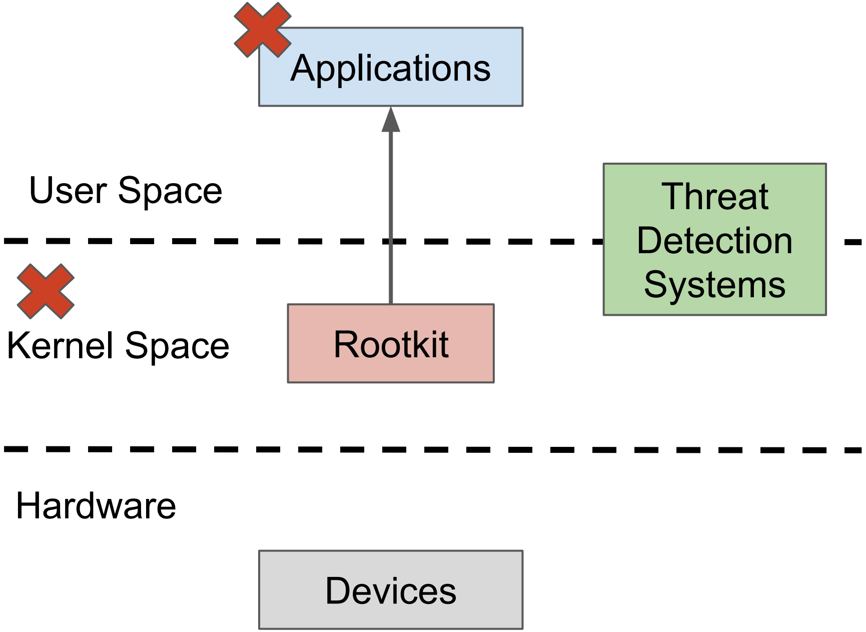
Kernel-level Rootkits

- Provide the most flexibility to attackers
- Compromise the entire OS
- Affect process execution
- Extract security and privacy critical data
- Access to HW devices (NIC, SSDs, etc.)
- Disable threat detection systems



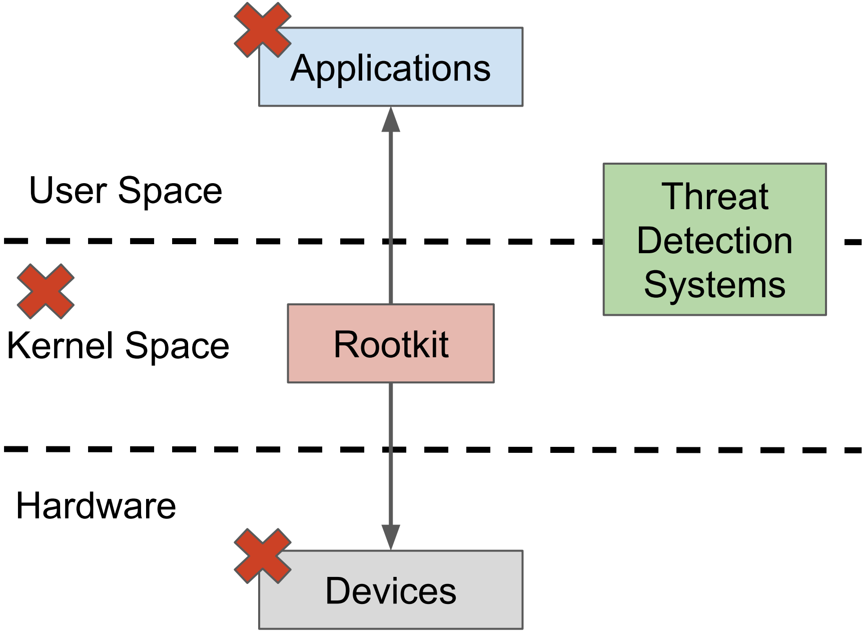
Kernel-level Rootkits

- Provide the most flexibility to attackers
- Compromise the entire OS
- Affect process execution
- Extract security and privacy critical data
- Access to HW devices (NIC, SSDs, etc.)
- Disable threat detection systems



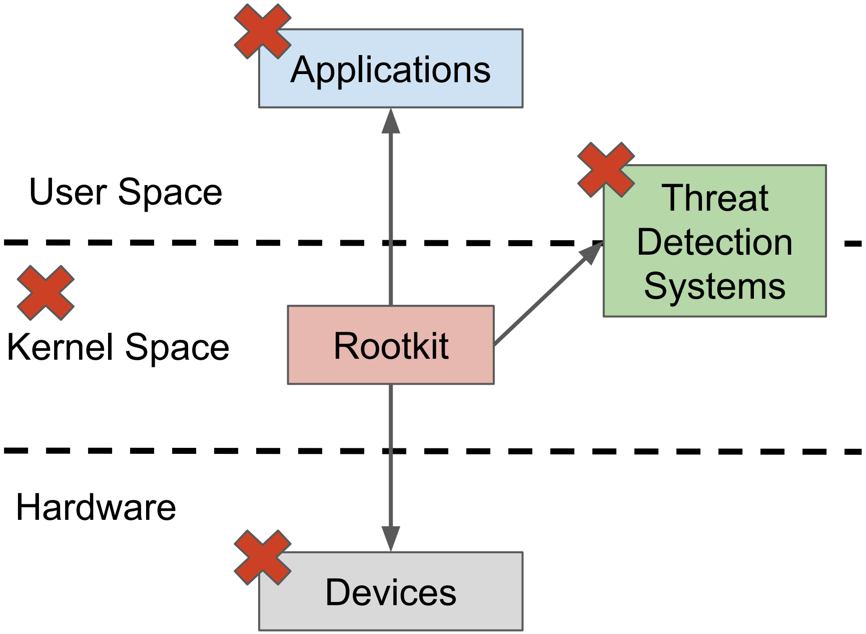
Kernel-level Rootkits

- Provide the most flexibility to attackers
- Compromise the entire OS
- Affect process execution
- Extract security and privacy critical data
- Access to HW devices (NIC, SSDs, etc.)
- Disable threat detection systems



Kernel-level Rootkits

- Provide the most flexibility to attackers
- Compromise the entire OS
- Affect process execution
- Extract security and privacy critical data
- Access to HW devices (NIC, SSDs, etc.)
- Disable threat detection systems



Kernel Integrity Monitors

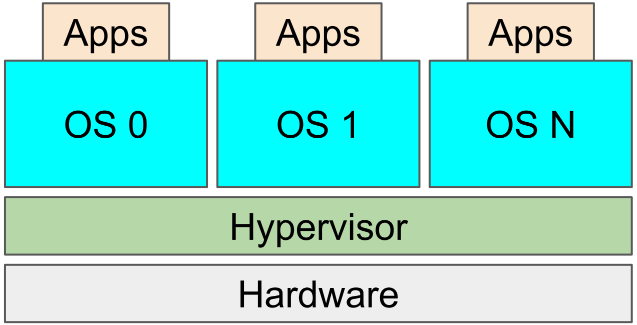
- Constantly monitor the integrity of the operating system kernel
- Reside in a secure space outside of the kernel

- Common operating modes
  - Snapshots
  - Event triggers
  - Snooping

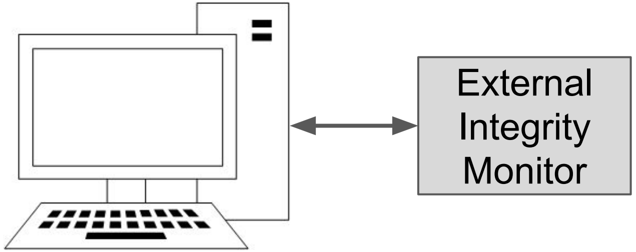
- Major approaches
  - Hypervisor-assisted
  - Hardware-assisted

Kernel Integrity Monitors

- Hypervisor-assisted

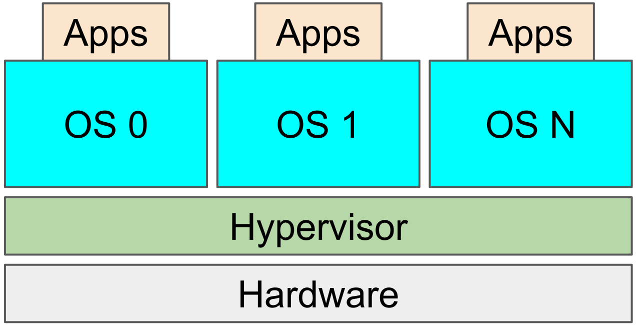


- Hardware-assisted

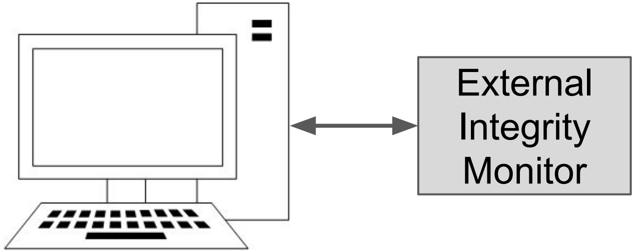


Kernel Integrity Monitors

- Hypervisor-assisted
  - ✗ **Rely on hypervisor presence**
  - ✗ **Increased code base**

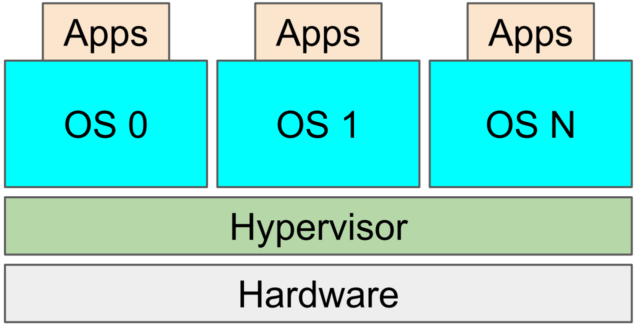


- Hardware-assisted

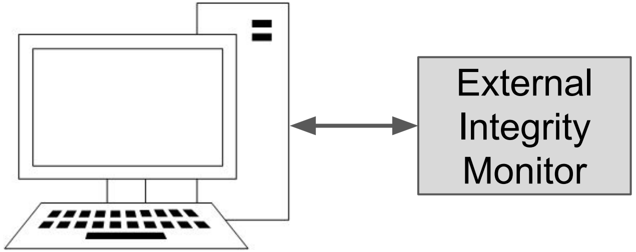


Kernel Integrity Monitors

- Hypervisor-assisted
  - ✗ **Rely on hypervisor presence**
  - ✗ **Increased code base**



- Hardware-assisted
  - ✗ **External hardware (FPGA, GPU, etc.)**
  - ✗ **Non-commodity system setup**



SGX-Mon

- Utilizes Intel SGX enclaves
  - ☑ **Remains hidden and protected from attackers**
  - ☑ **Resides in the user space**

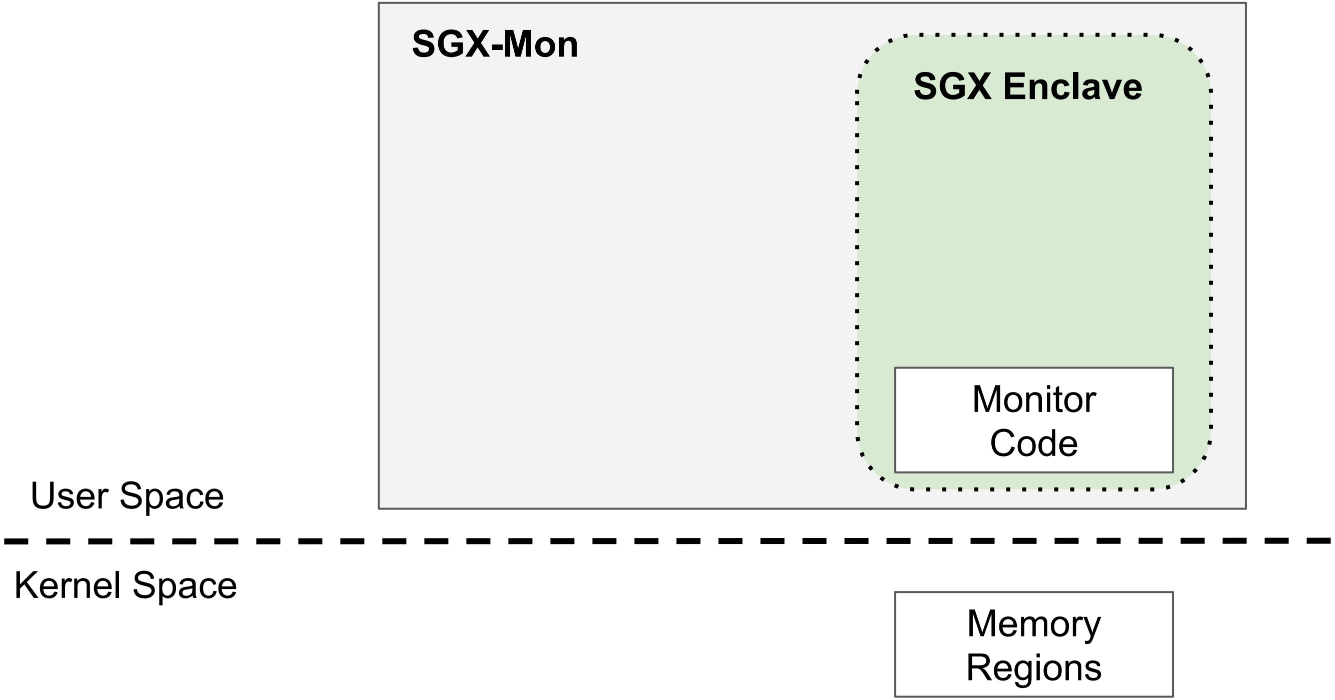
- No hypervisor or external hardware
  - ☑ **Small TCB**
  - ☑ **Commodity system setup**
  - ☑ **Utilizes a custom driver on bootstrap**

- Snapshot based
  - ☑ **Relies on simple hash operations**
  - ☑ **Easily extendable**

Intel SGX

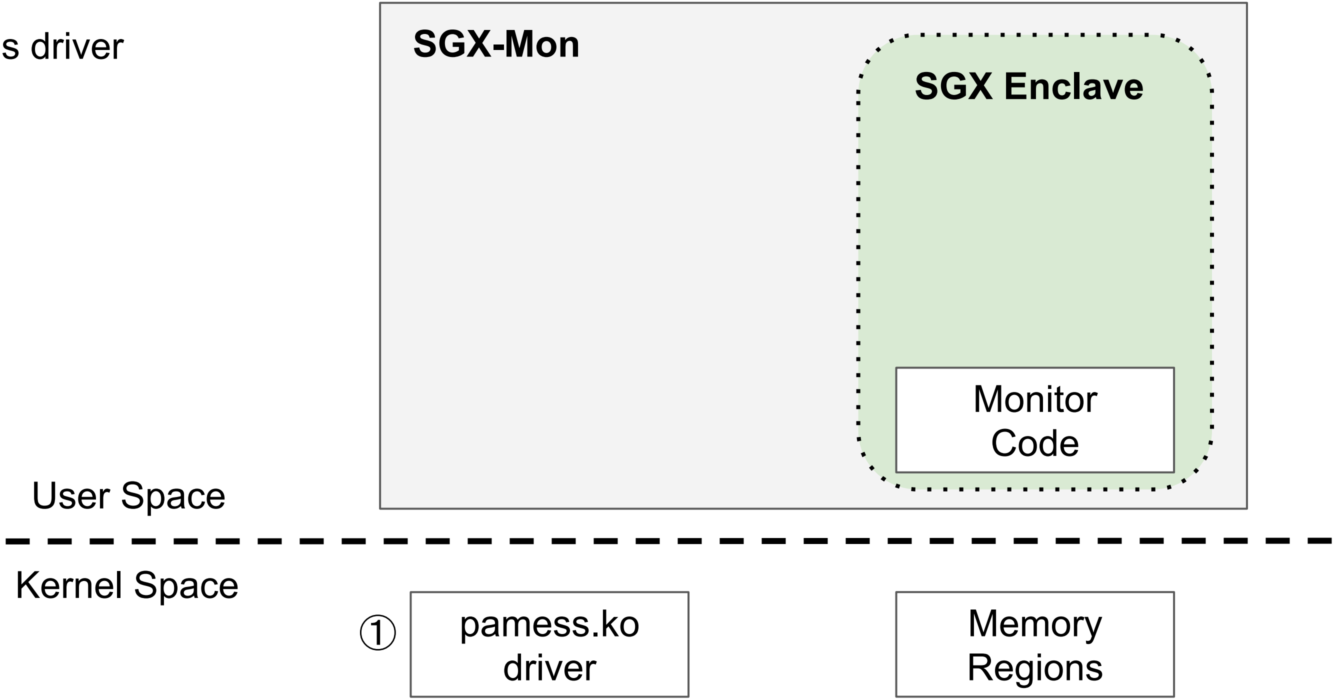
- Found in recent Intel processors
- Provides protected memory regions called enclaves
- Operates as a reverse sandbox in the user space
- The OS kernel has no access in the enclave
- CPU-enforced security

Secure Bootstrap Phase



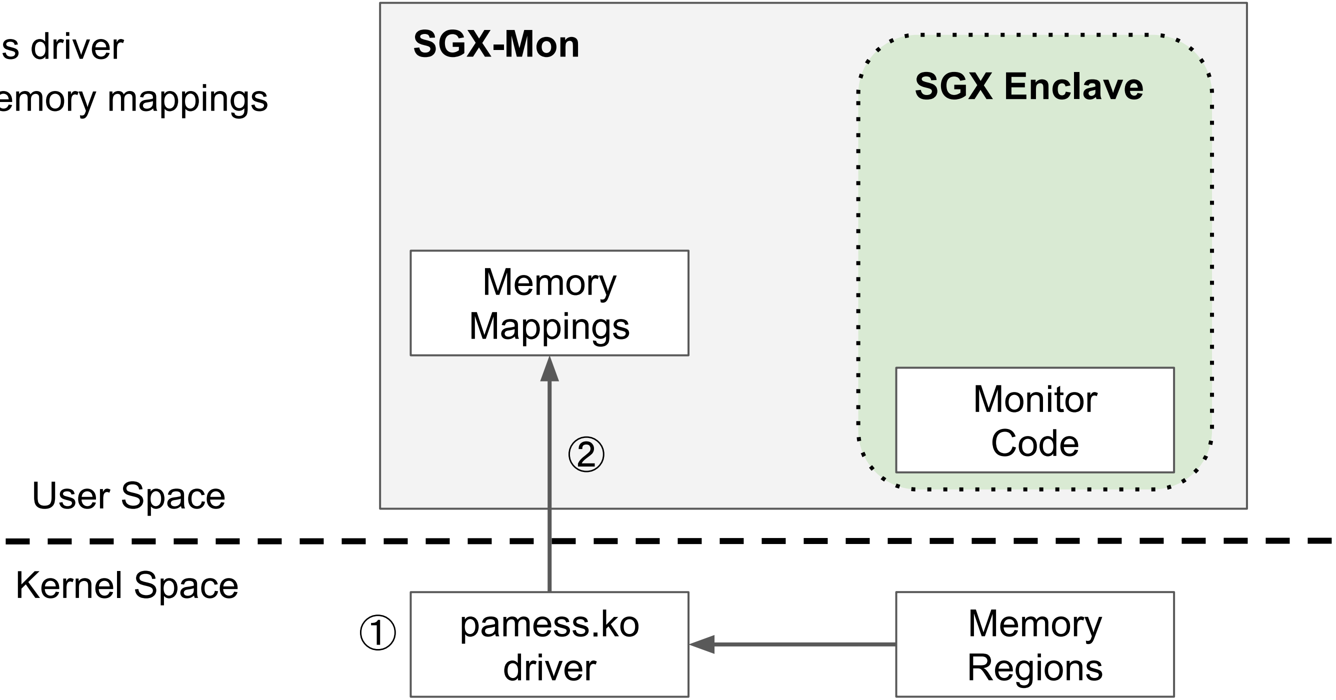
Secure Bootstrap Phase

1. Load pamess driver



Secure Bootstrap Phase

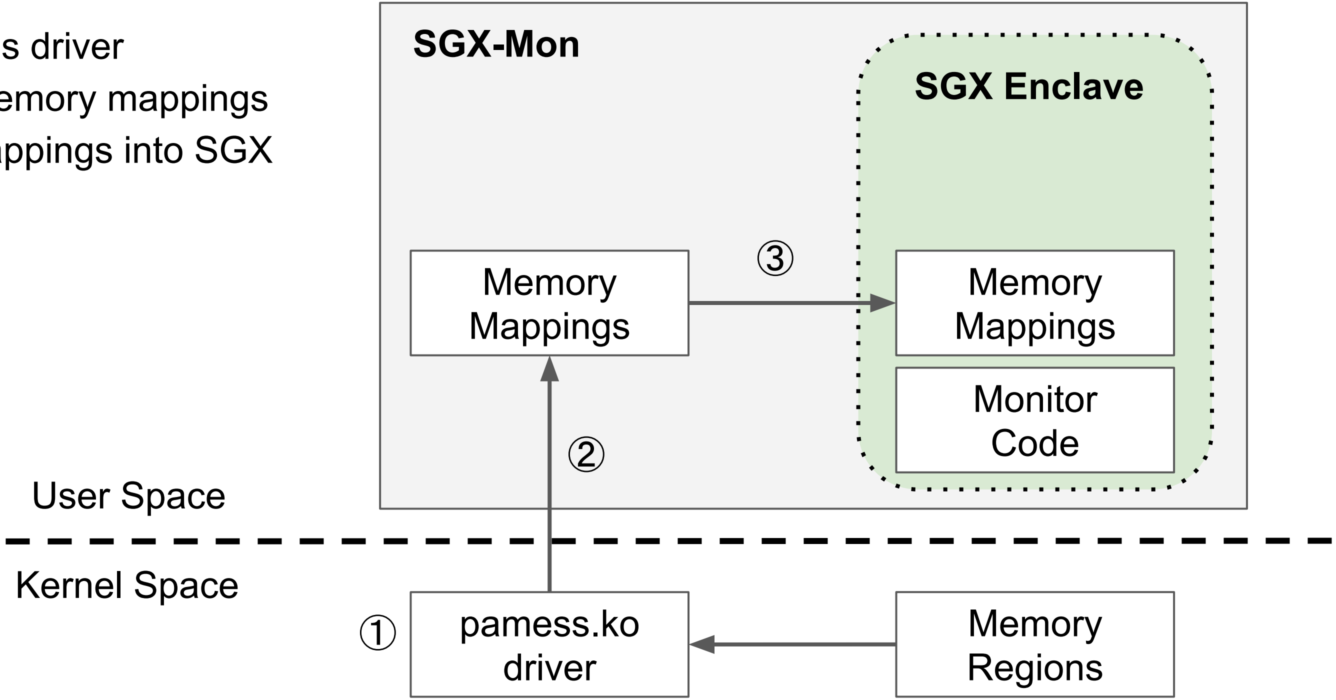
1. Load pamess driver
2. Generate memory mappings



INSTITUTE OF COMPUTER SCIENCE

Secure Bootstrap Phase

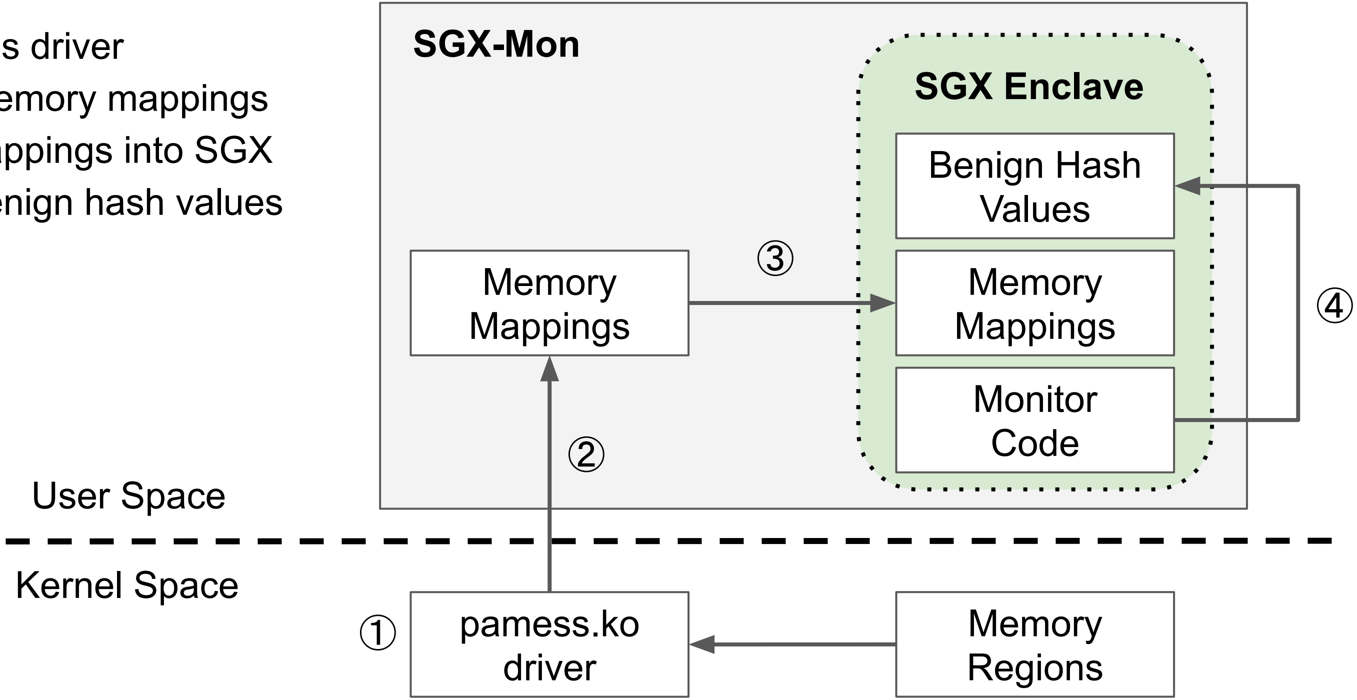
1. Load pamess driver
2. Generate memory mappings
3. Pass the mappings into SGX



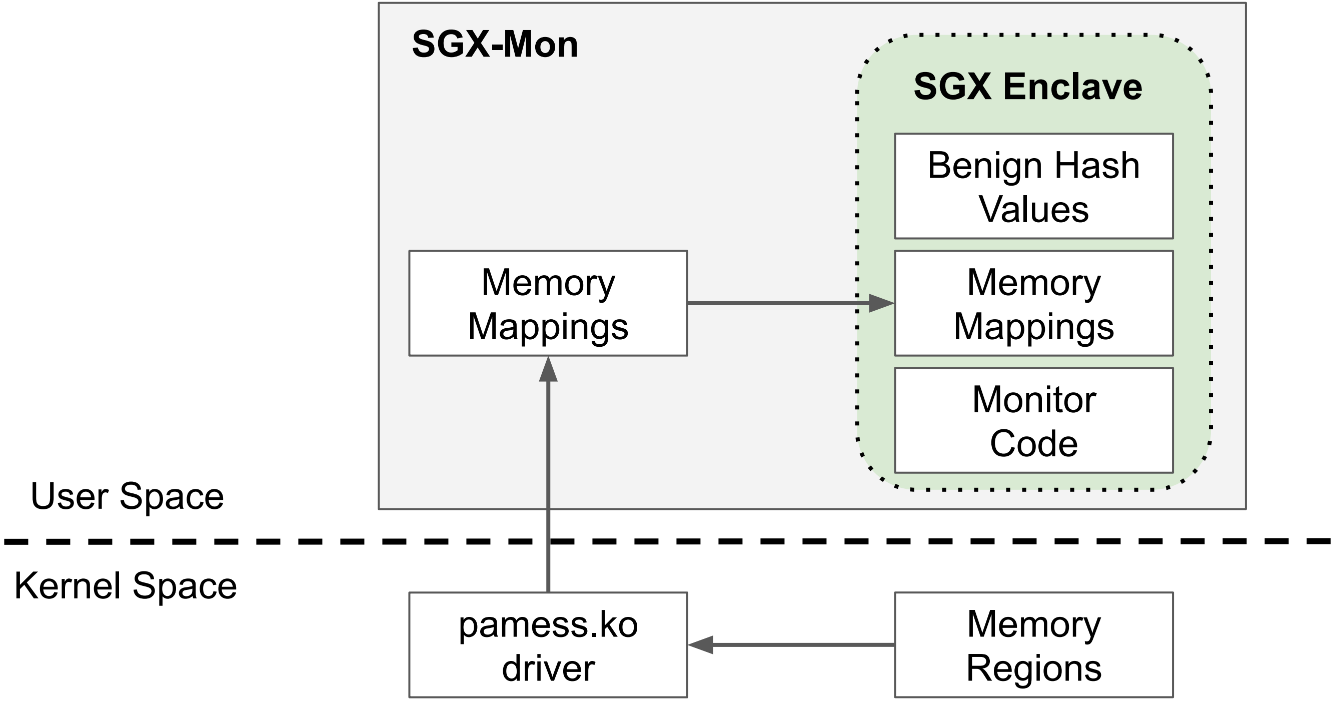
INSTITUTE OF COMPUTER SCIENCE

Secure Bootstrap Phase

1. Load pamess driver
2. Generate memory mappings
3. Pass the mappings into SGX
4. Generate benign hash values

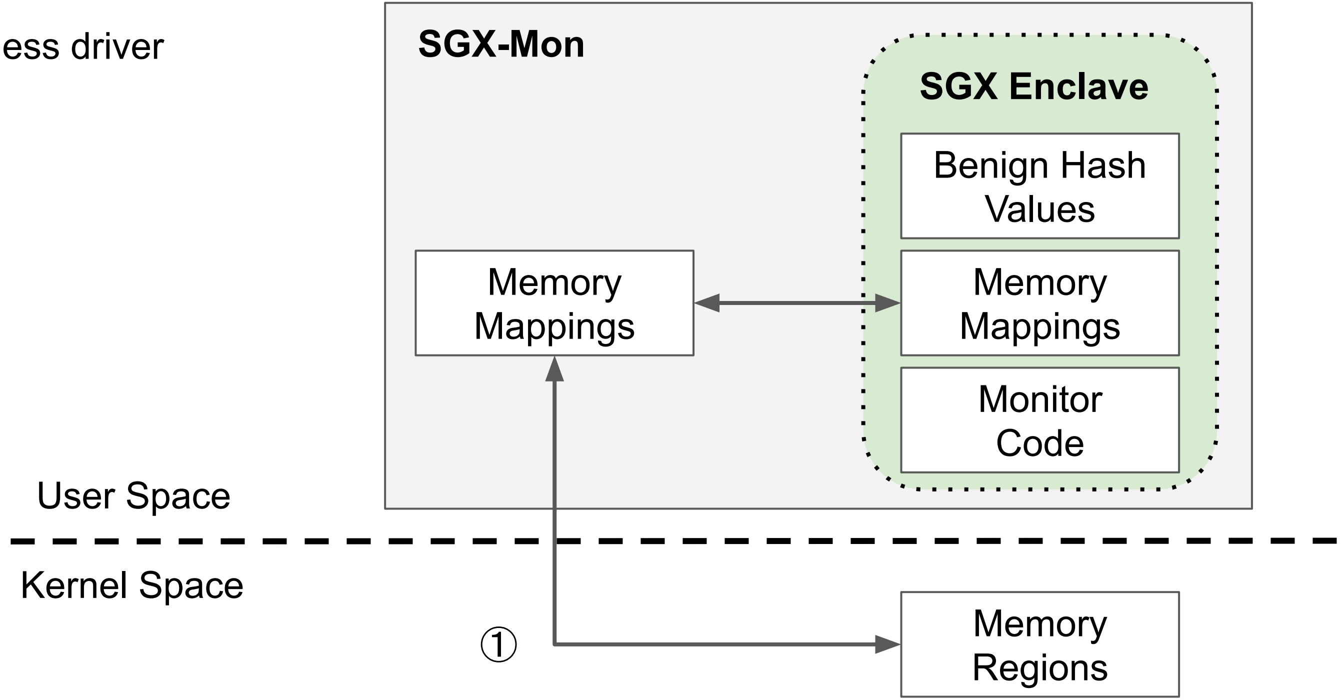


Monitoring Phase



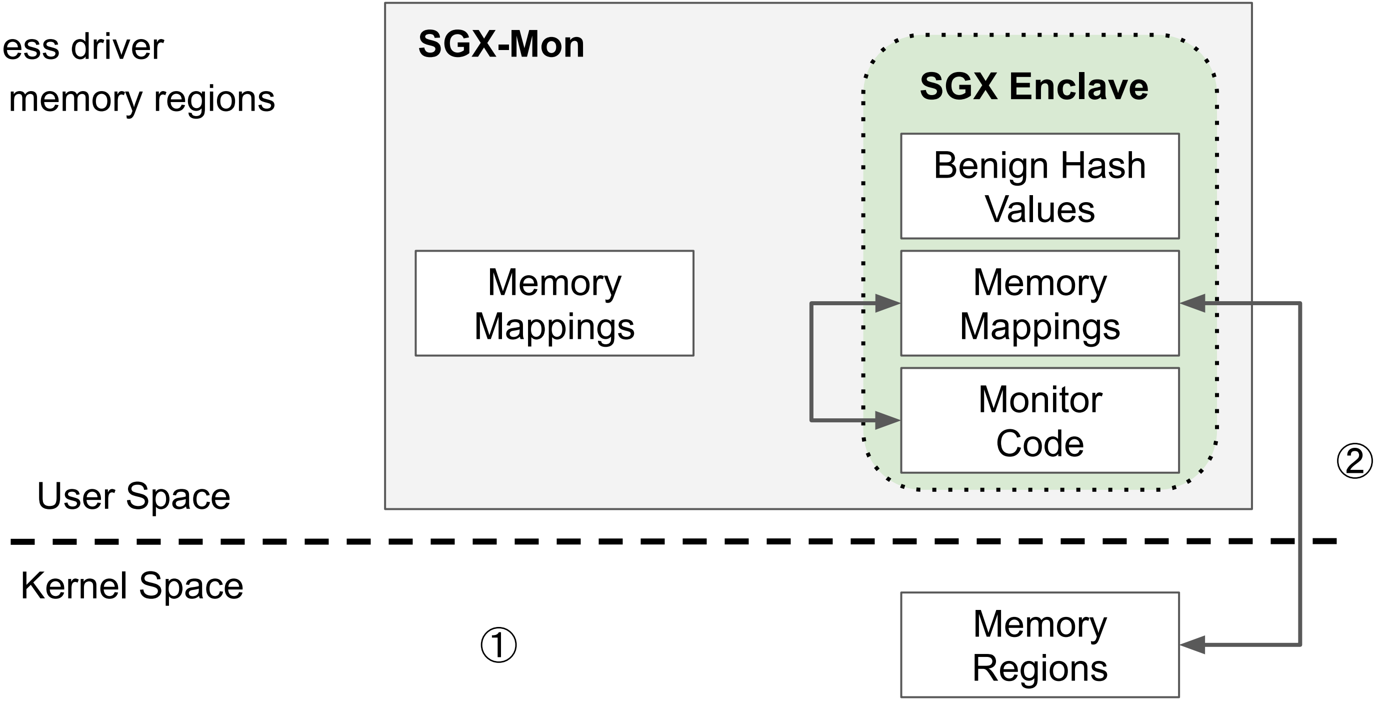
Monitoring Phase

1. Unload pamess driver



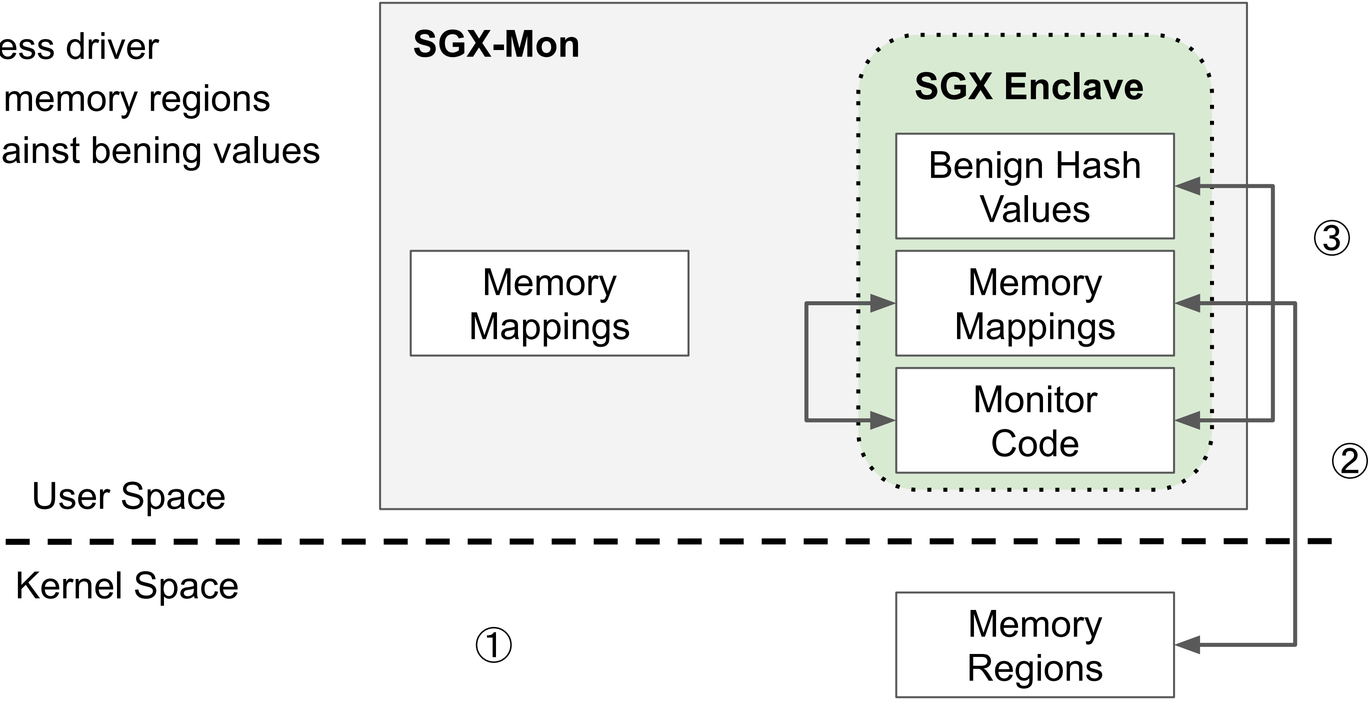
Monitoring Phase

1. Unload pamess driver
2. Scan kernel memory regions



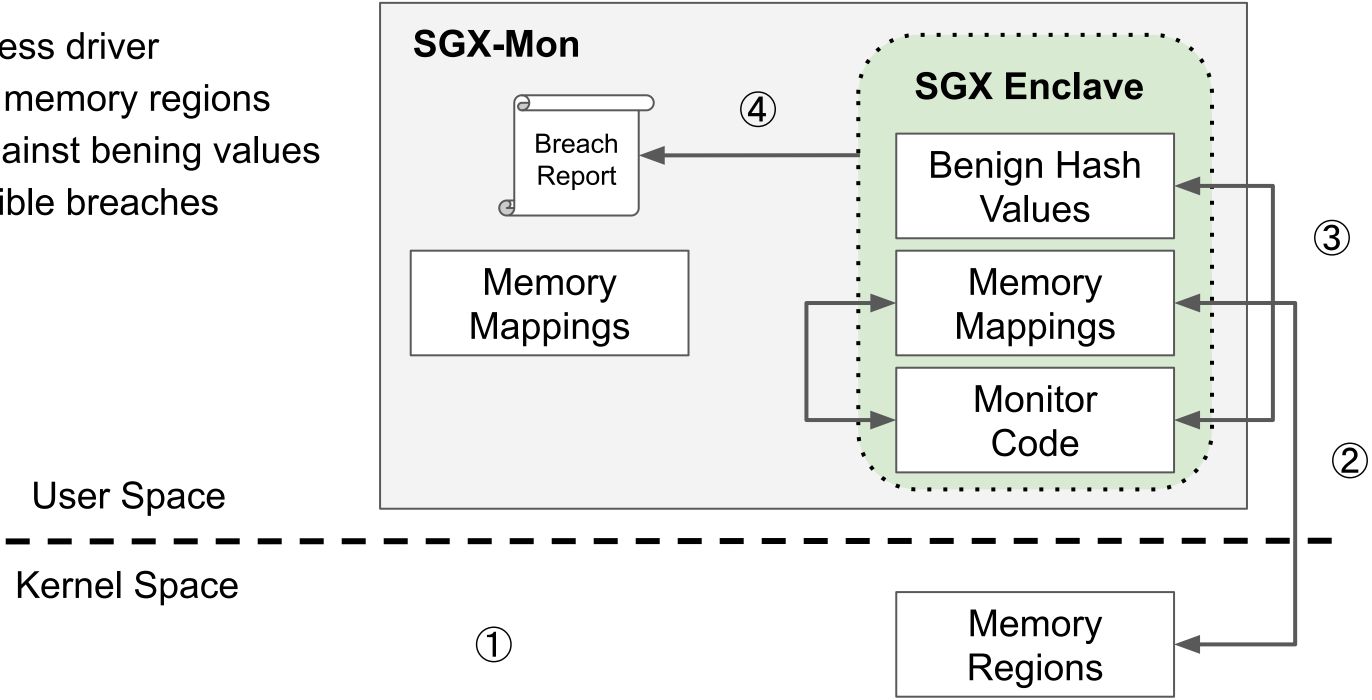
Monitoring Phase

1. Unload pamess driver
2. Scan kernel memory regions
3. Compare against bening values



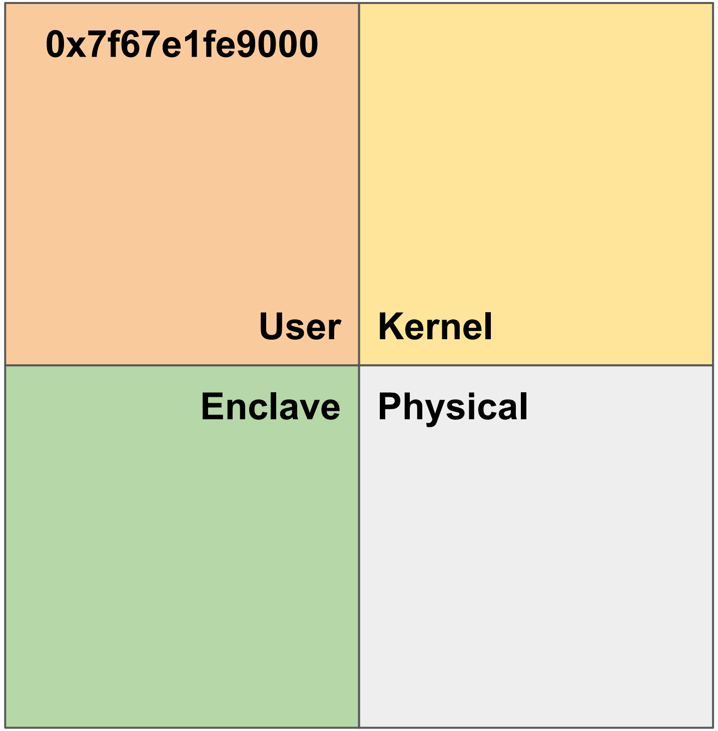
Monitoring Phase

1. Unload pamess driver
2. Scan kernel memory regions
3. Compare against bening values
4. Report possible breaches



FORTH
INSTITUTE OF COMPUTER SCIENCE

Mapping OS Kernel Memory



0x7f67e1fe9000

User

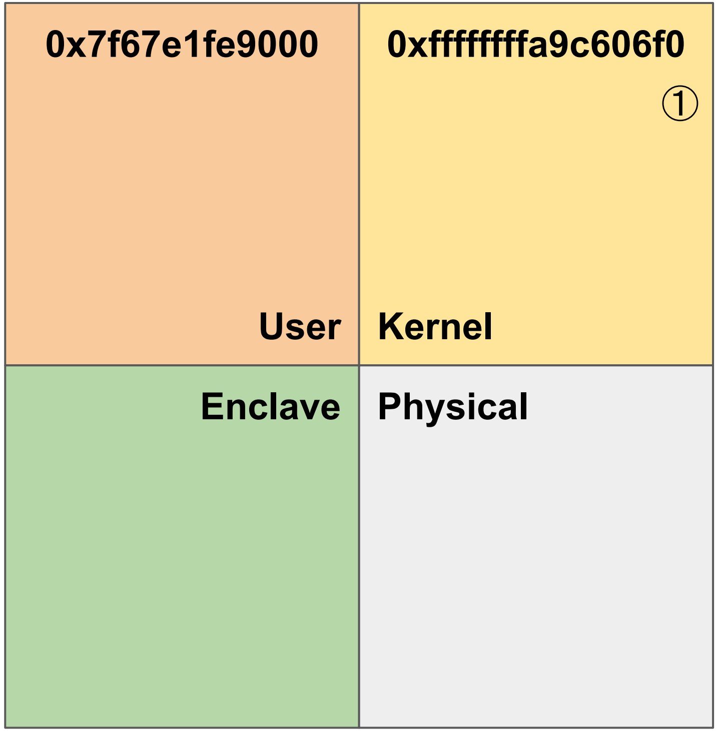
Kernel

Enclave

Physical

Mapping OS Kernel Memory

1. Find the desired kernel virtual address



0x7f67e1fe9000

User

0xffffffffa9c606f0

①

Kernel

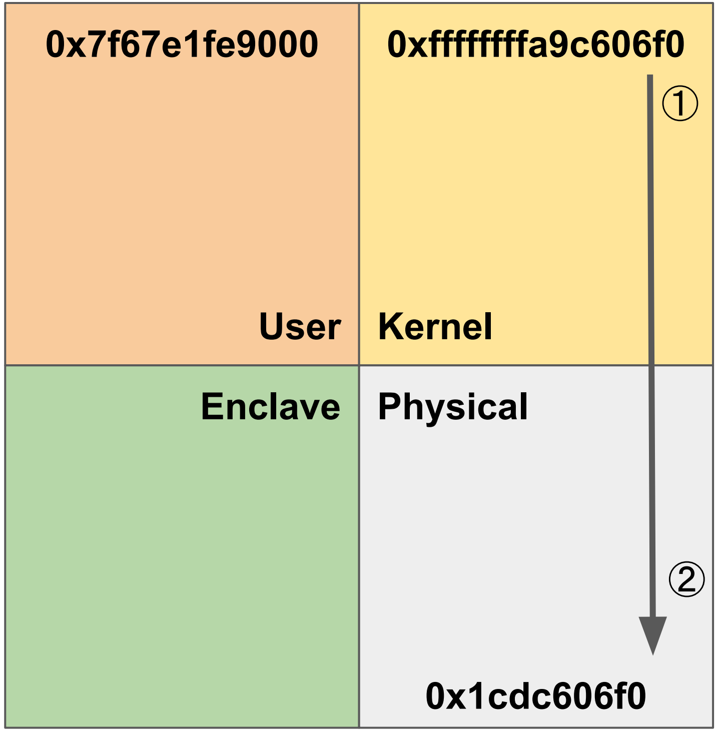
Enclave

Physical

Mapping OS Kernel Memory

1. Find the desired kernel virtual address

2. Identify its physical address

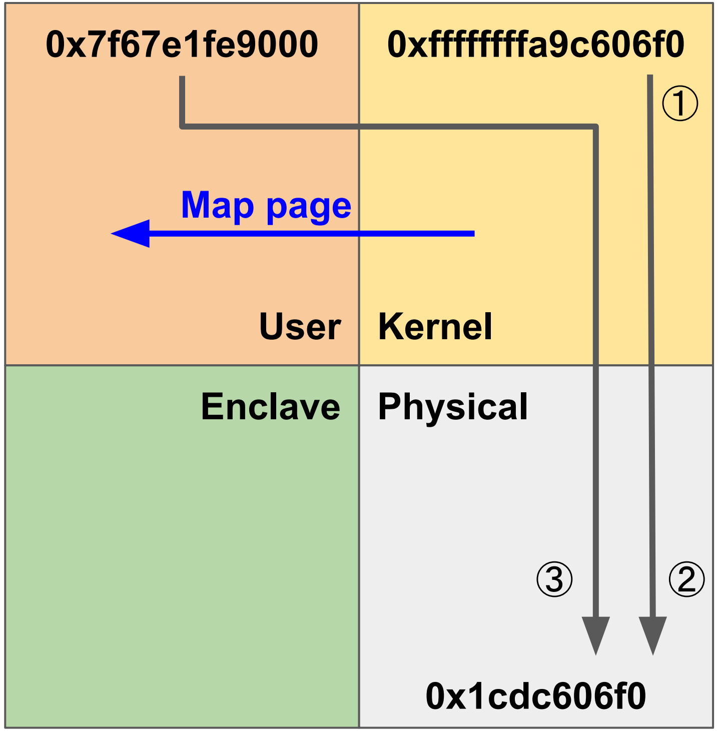


Mapping OS Kernel Memory

1. Find the desired kernel virtual address

2. Identify its physical address

3. Duplicate the mapping to user space using the pamess driver



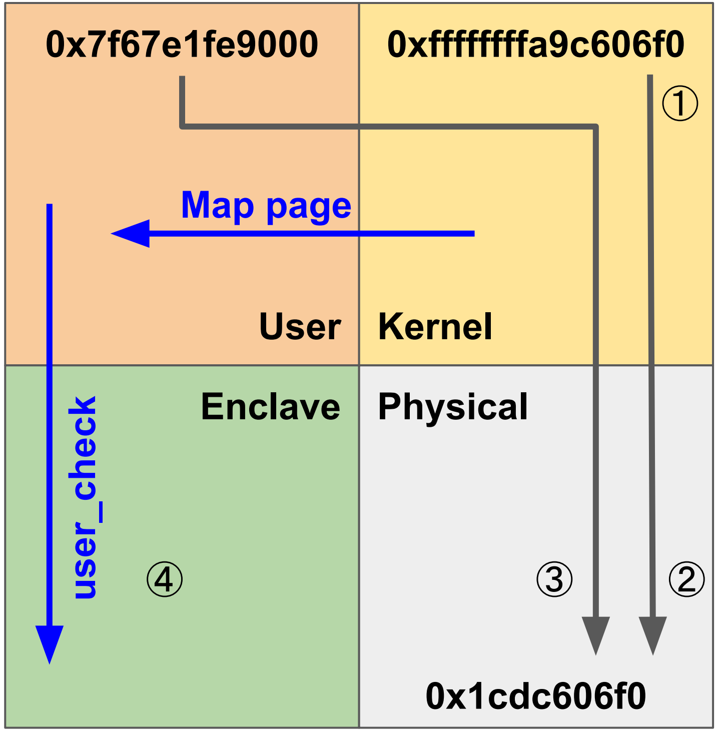
Mapping OS Kernel Memory

1. Find the desired kernel virtual address

2. Identify its physical address

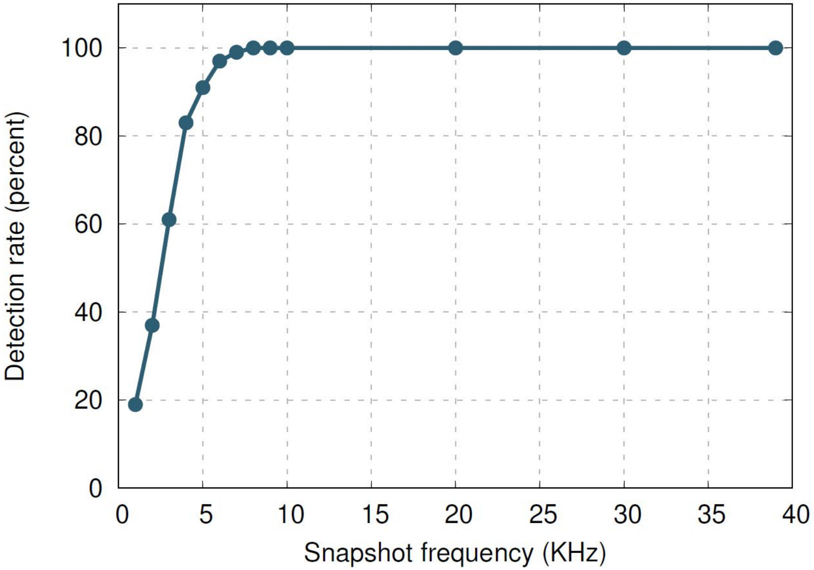
3. Duplicate the mapping to user space using the pamess driver

4. Pass the user space virtual address into the SGX enclave



Optimal Snapshot Frequency

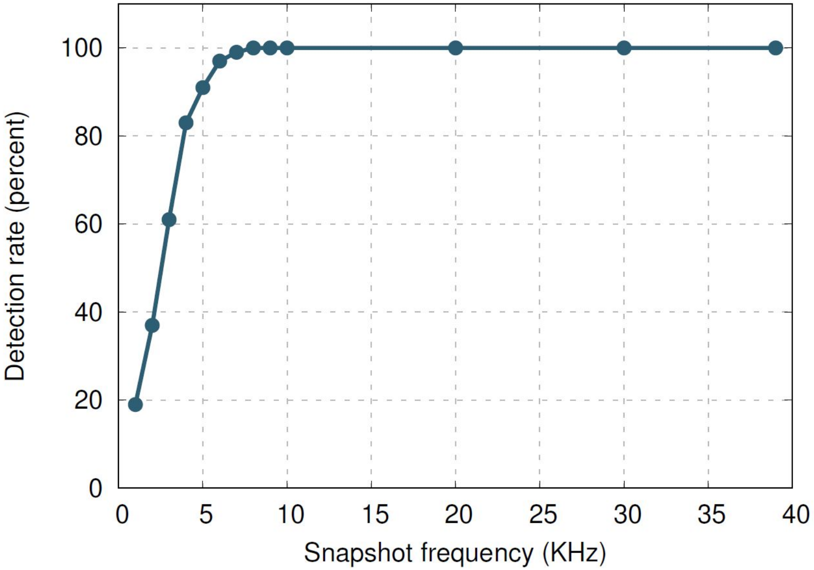
- Custom self-hiding Loadable Kernel Module
  - Enters the LKM list, altering the head’s value
  - Deletes its entry, restoring the original value
  - Emulates a transient attack



Optimal Snapshot Frequency

- Custom self-hiding Loadable Kernel Module
  - Enters the LKM list, altering the head's value
  - Deletes its entry, restoring the original value
  - Emulates a transient attack

- SGX-Mon scans the head of the LKM

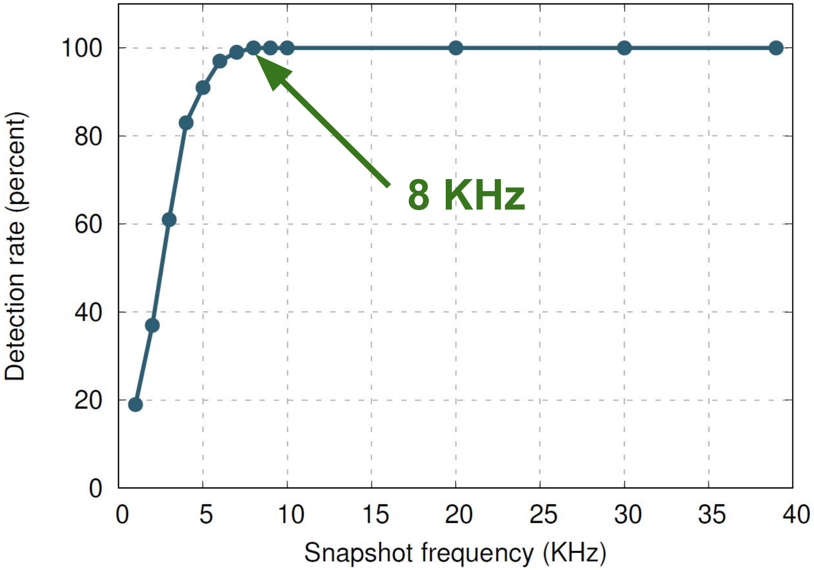


INSTITUTE OF COMPUTER SCIENCE

Optimal Snapshot Frequency

- Custom self-hiding Loadable Kernel Module
  - Enters the LKM list, altering the head's value
  - Deletes its entry, restoring the original value
  - Emulates a transient attack

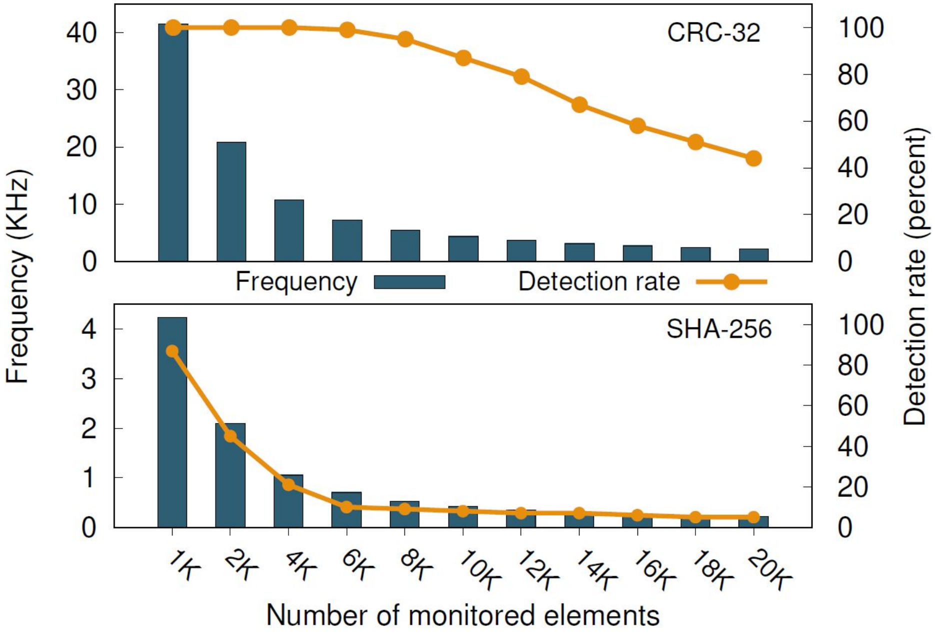
- SGX-Mon scans the head of the LKM



✓ **Snapshot frequencies greater than 8 KHz offer 100% detection rate**

Monitoring Accuracy

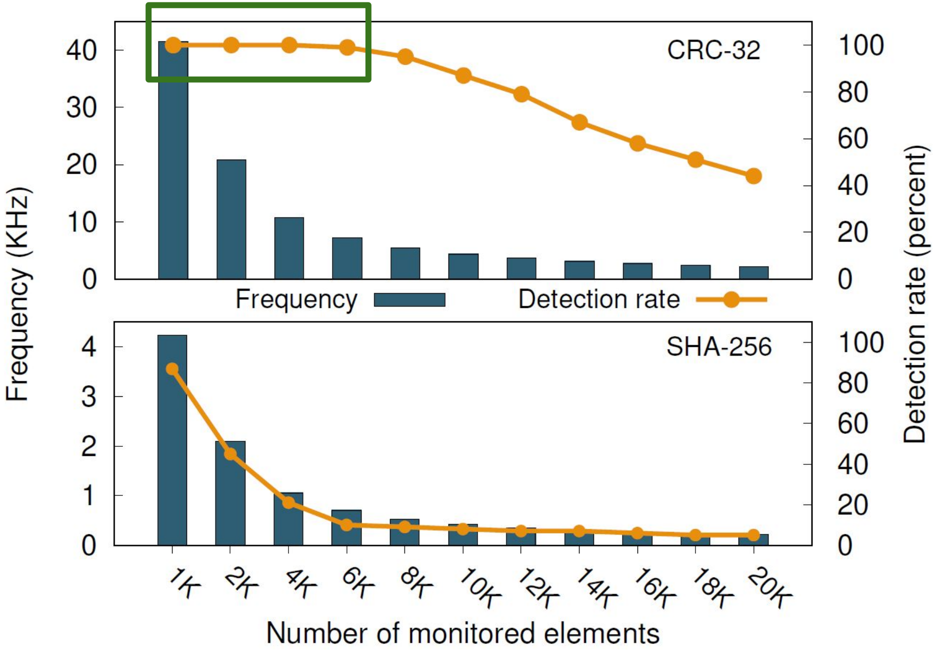
- 8-byte long kernel memory regions
- Obtained via /proc/kallsyms
- Snapshot using CRC-32 and SHA-256



INSTITUTE OF COMPUTER SCIENCE

Monitoring Accuracy

- 8-byte long kernel memory regions
- Obtained via /proc/kallsyms
- Snapshot using CRC-32 and SHA-256



✅ **100% detection rate with up to 6.000 kernel memory regions**

FORTH
INSTITUTE OF COMPUTER SCIENCE

Conclusion

- Snapshot based kernel integrity monitor
- Protected by Intel SGX enclaves
- Very small TCB
- Does not require a hypervisor or external hardware
- 100% accuracy while scanning up to 6000 kernel memory locations