CAP-TEE

Capability Architectures in Trusted Execution

UNIVERSITY OF BIRMINGHAM

CHERI & Trusted Execution Environments

Jennifer Jackson – University of Birmingham
In collaboration with KU Leuven

Our project is funded by the Digital Security by Design (DSbD) Programme delivered by UKRI to support the DSbD ecosystem

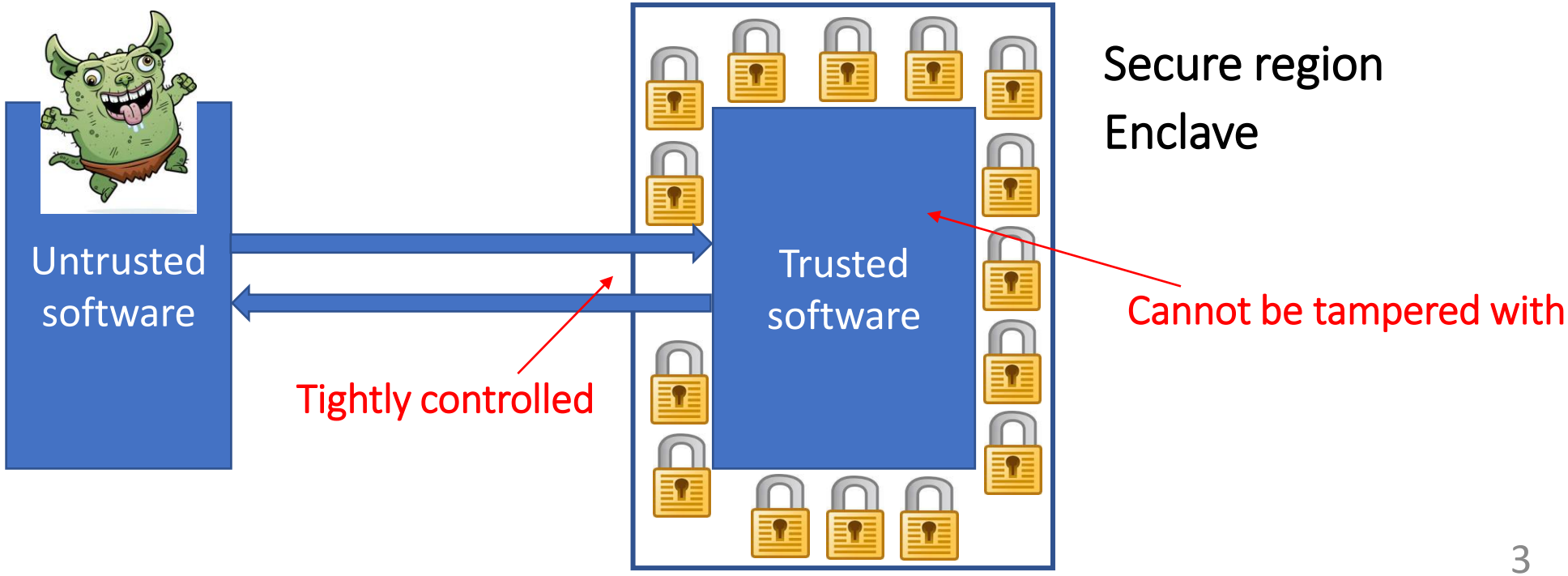
Jennifer Jackson, David Oswald, Mark Ryan, Mihai Ordean, Richard Thomas, Flavio Garcia

Introduction

- Trusted execution and capabilities
- CHERI-based prototype TEE.
- Object capabilities and domain switching
- Demo

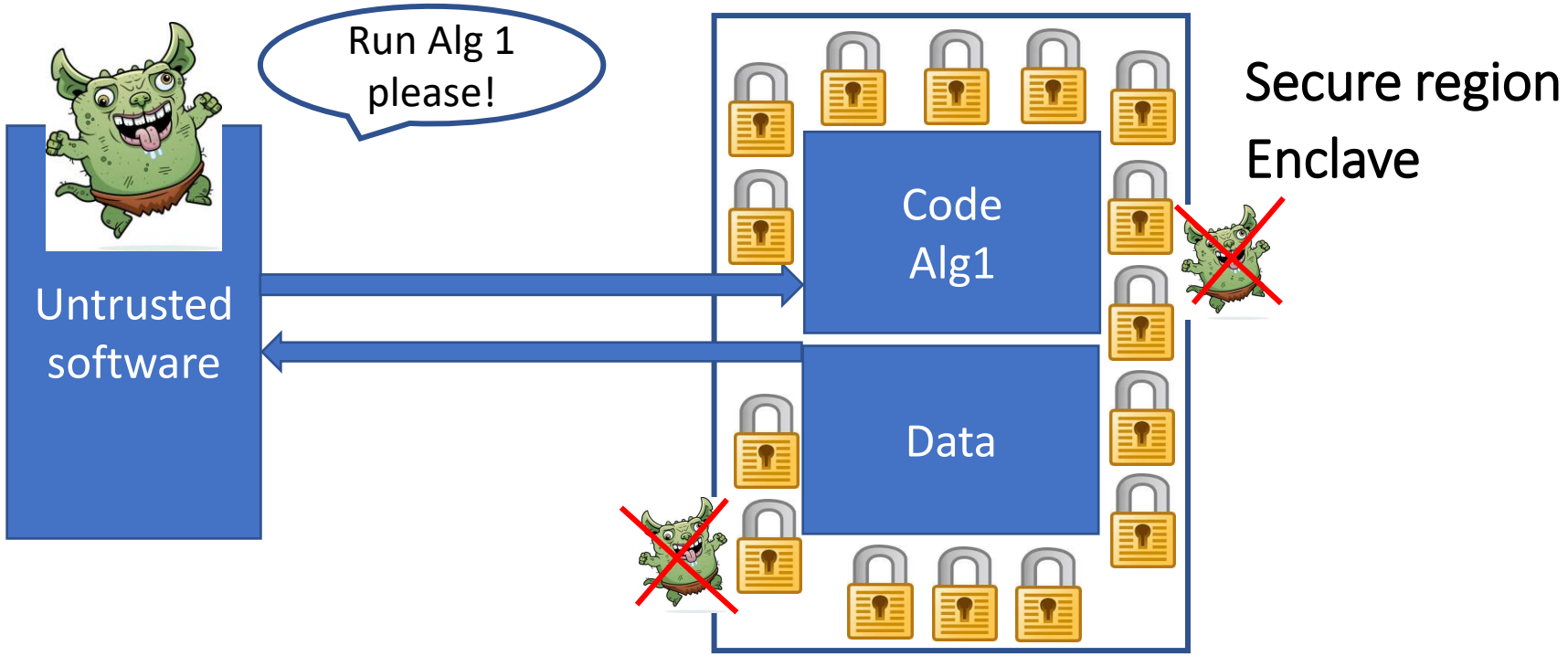
TEE - Trusted Execution Environment and Capabilities

- **Trusted Execution Environments (TEEs)**
  - shield sensitive data and computation inside a secure region/enclave, away from the rest of the untrusted operating system and services.



TEE - Trusted Execution Environment and Capabilities

- **Trusted Execution Environments (TEEs)**
  - shield sensitive data and computation inside a secure region/enclave, away from the rest of the untrusted operating system and services.



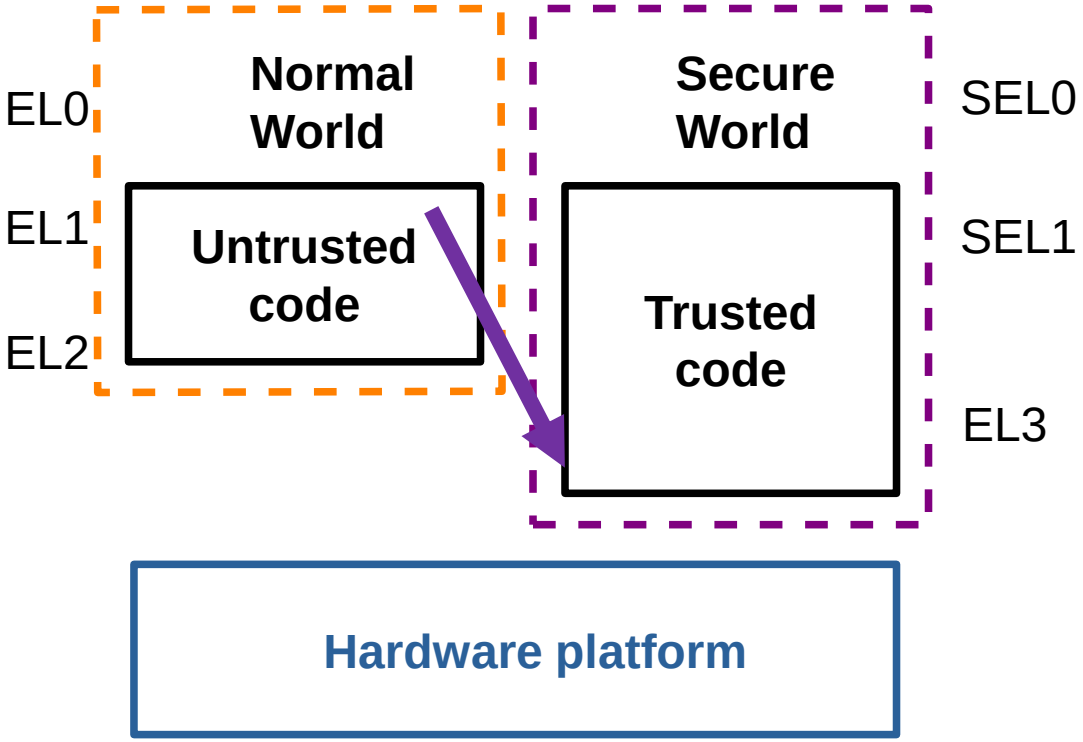
TEE - Trusted Execution Environment and Capabilities

Arm Trustzone

Intel SGX Application

TEE - Trusted Execution Environment and Capabilities

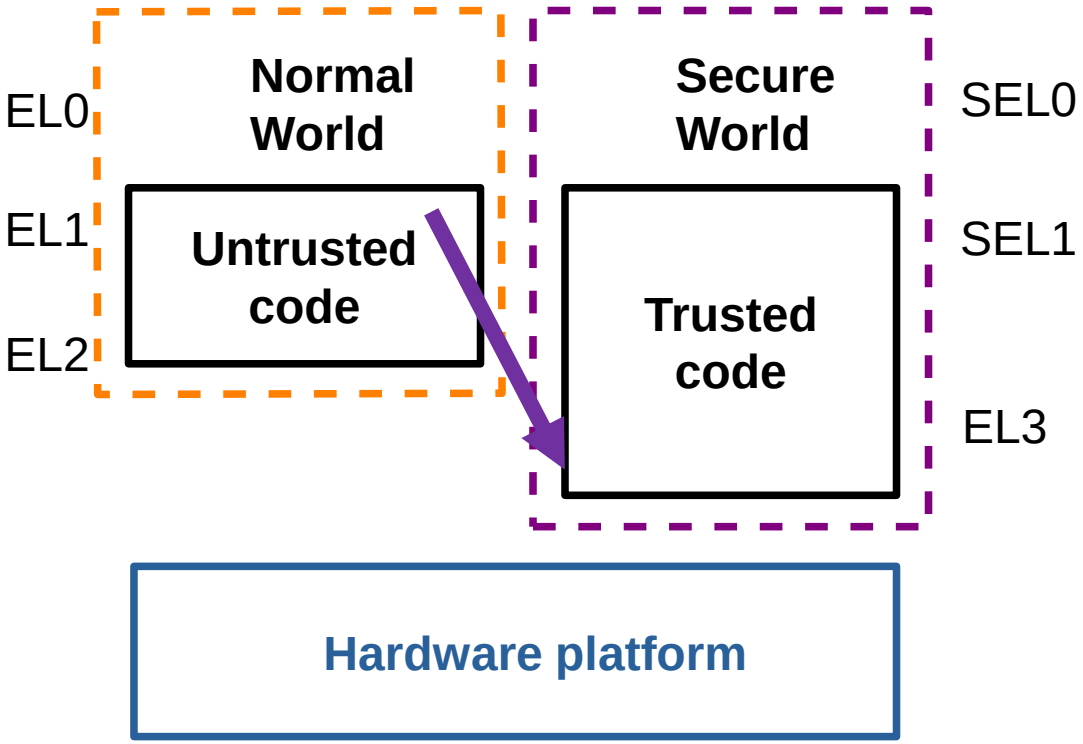
Arm Trustzone



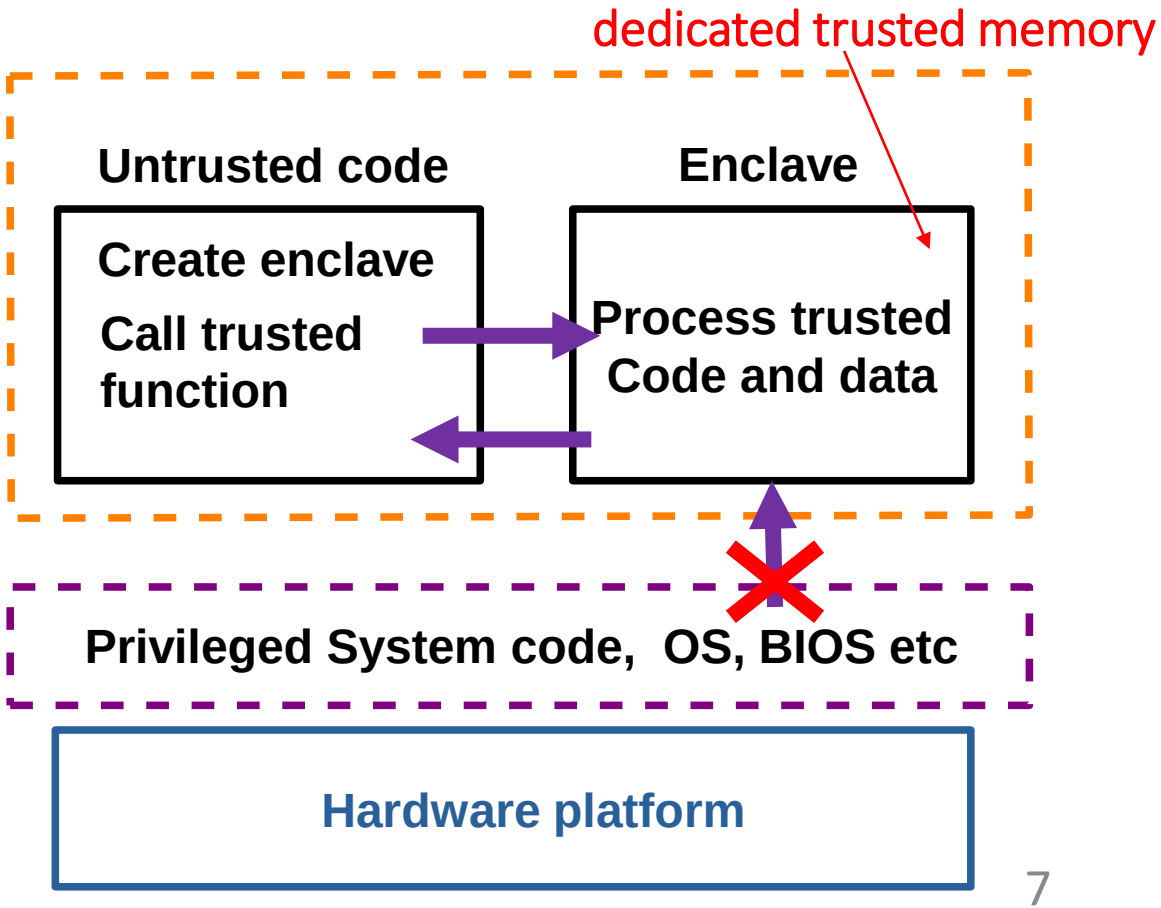
Intel SGX Application

TEE - Trusted Execution Environment and Capabilities

Arm Trustzone

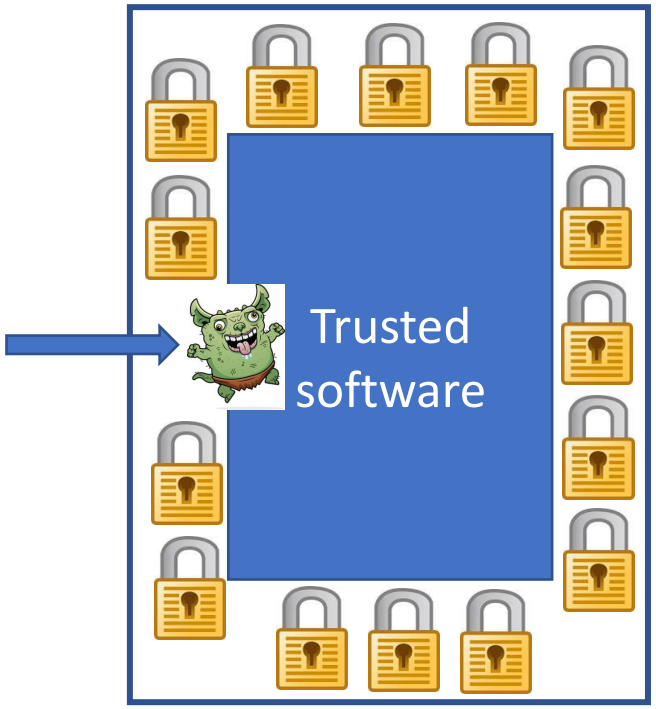


Intel SGX Application



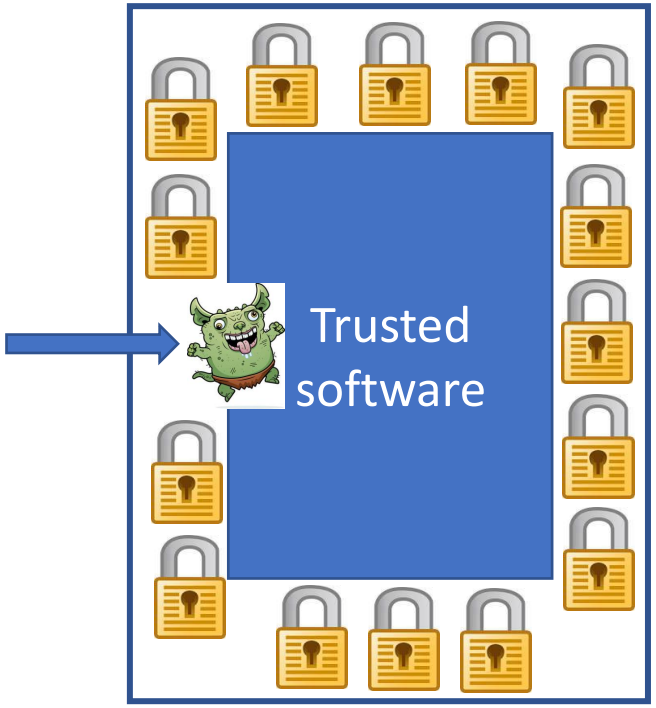
TEE - Trusted Execution Environment and Capabilities

- **TEEs, vulnerable**
  - to a multitude of hardware and software-based attacks.



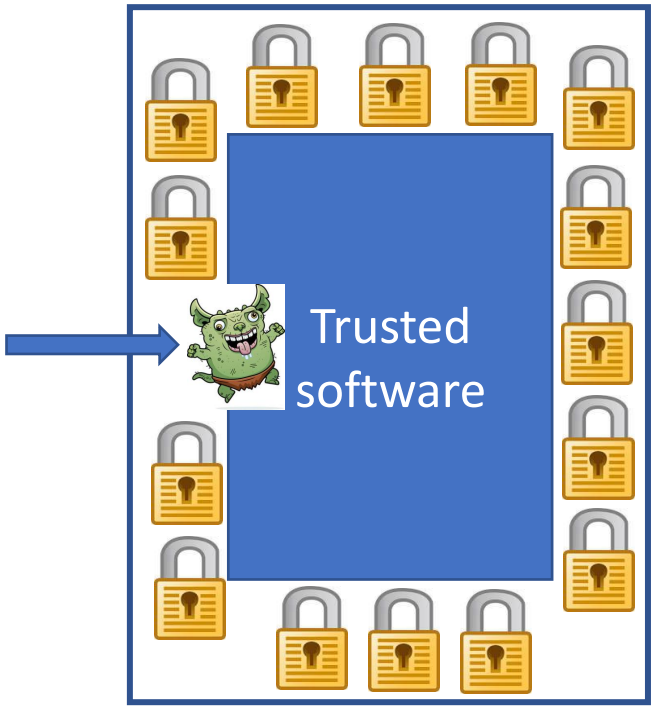
TEE - Trusted Execution Environment and Capabilities

- **TEEs, vulnerable**
  - to a multitude of hardware and software-based attacks.
- **Using Capability architectures**
  - **CHERI** may **mitigate** against a variety of **memory vulnerability** problems.
  - **CHERI** supports the creation of **isolated regions of memory**.



TEE - Trusted Execution Environment and Capabilities

- **TEEs, vulnerable**
  - to a multitude of hardware and software-based attacks.
- **Capability architectures**
  - **CHERI** may **mitigate** against a variety of **memory vulnerability** problems.
  - **CHERI** supports the creation of **isolated regions of memory**.
- **Explore CHERI for TEEs**
  - Improve security



Explore CHERI for TEEs

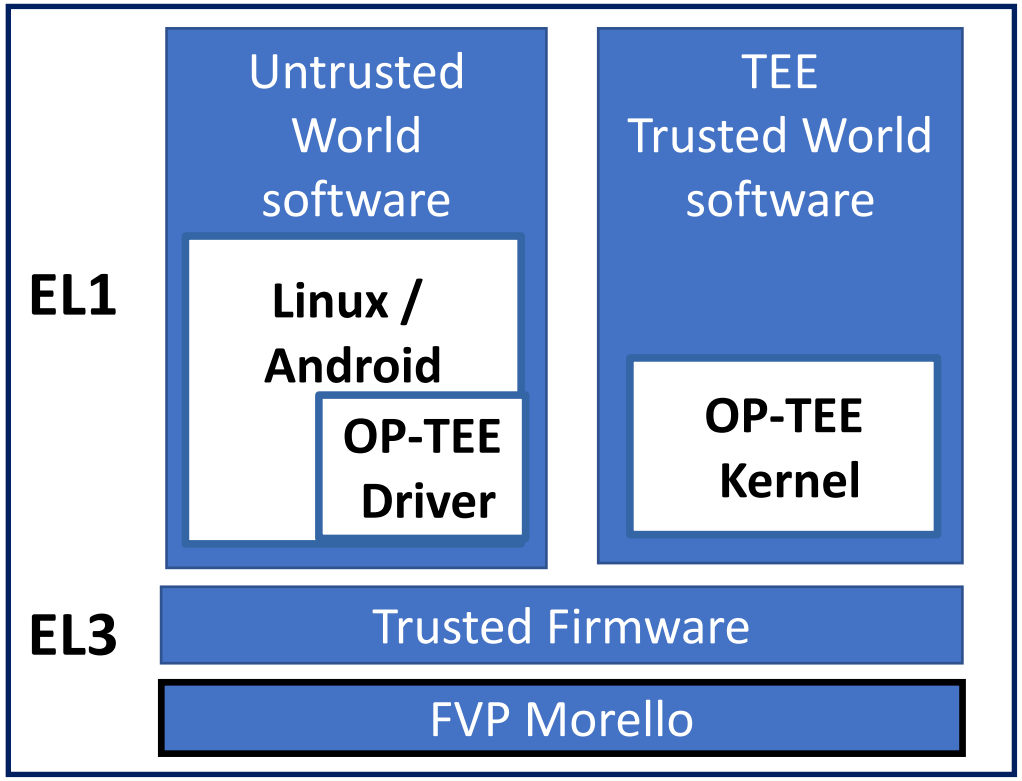
1. CHERI - OPTEE

2. CHERI prototype TEE

Explore CHERI for TEEs

1. CHERI - OPTEE

- Port **existing TEE** runtime such as **OP-TEE,** to a capability enabled TEE.

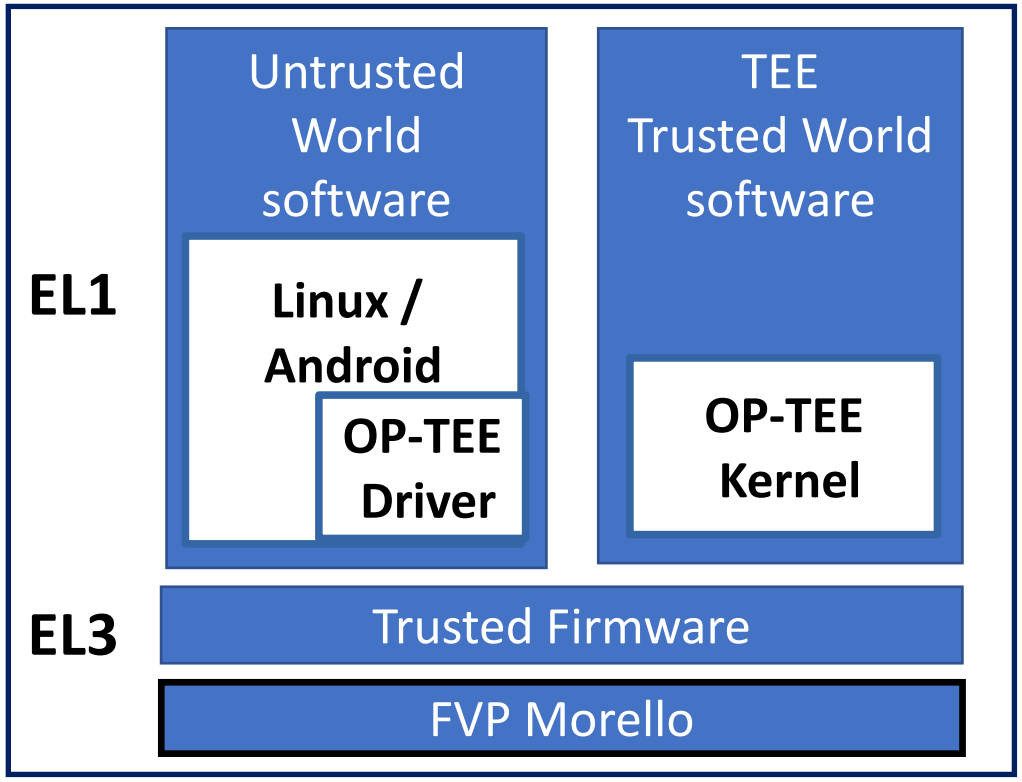


2. CHERI prototype TEE

Explore CHERI for TEEs

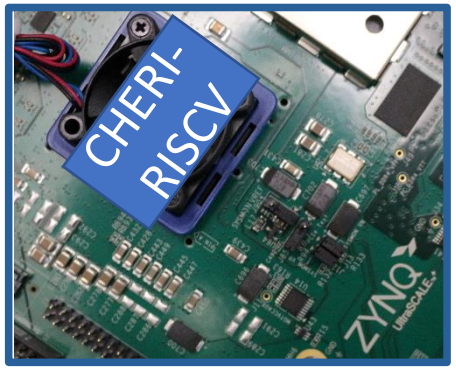
1. CHERI - OPTEE

- Port **existing TEE** runtime such as **OP-TEE,** to a capability enabled TEE.



2. CHERI prototype TEE

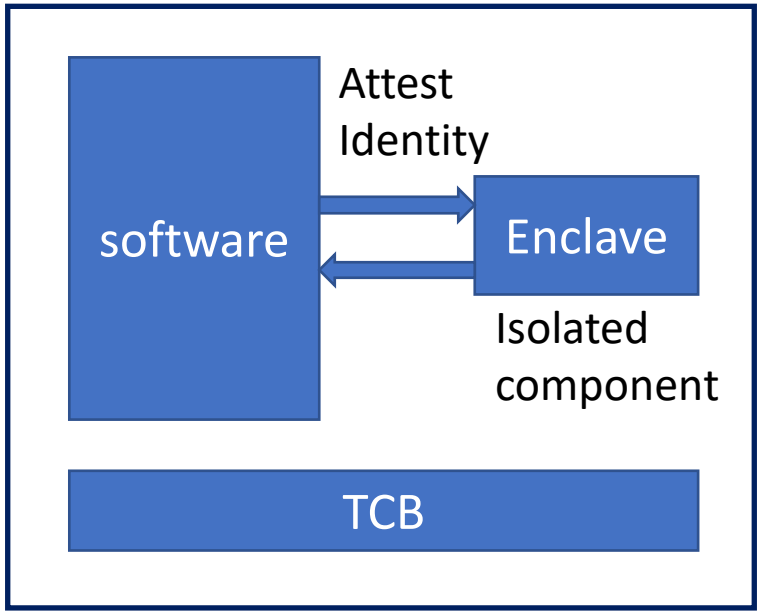
- **In collaboration with KU Leuven**
- **prototype CHERI-TEE on RISC-V**
- **prototype CHERI-TEE on Morello & integration with Trustzone**



Morello Platform Model

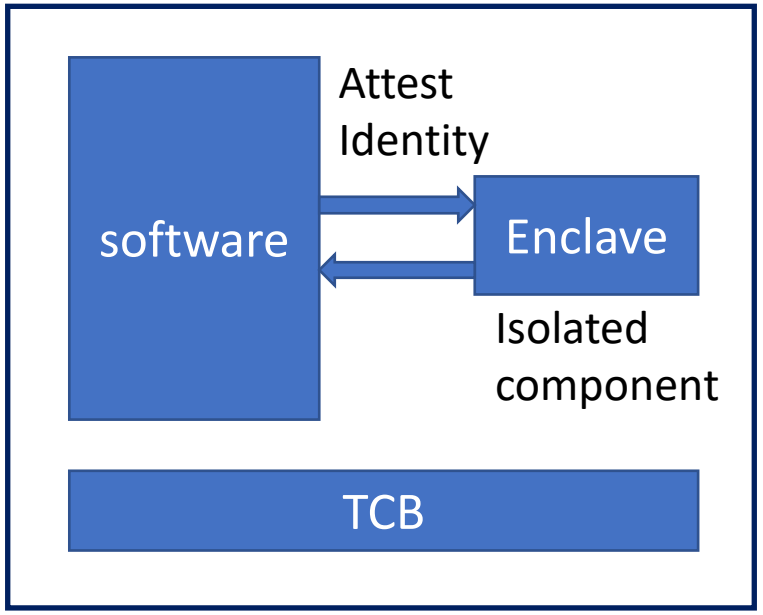
Download the open access Fixed Virtual Platform (FVP) on developer.

CHERI-based Prototype TEE



- Isolated regions of memory
- Created during run-time
- Small trusted computing Base TCB

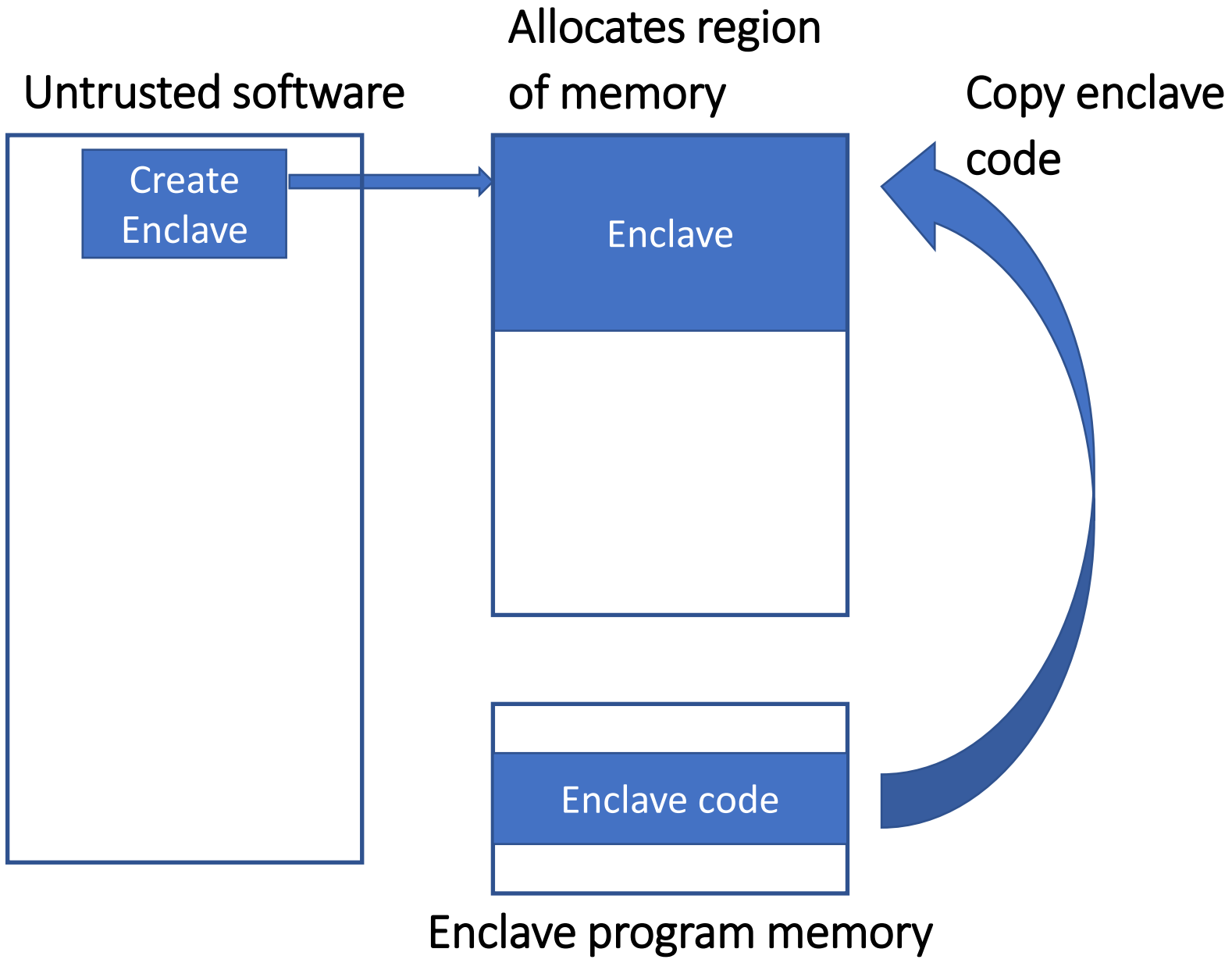
CHERI-based Prototype TEE

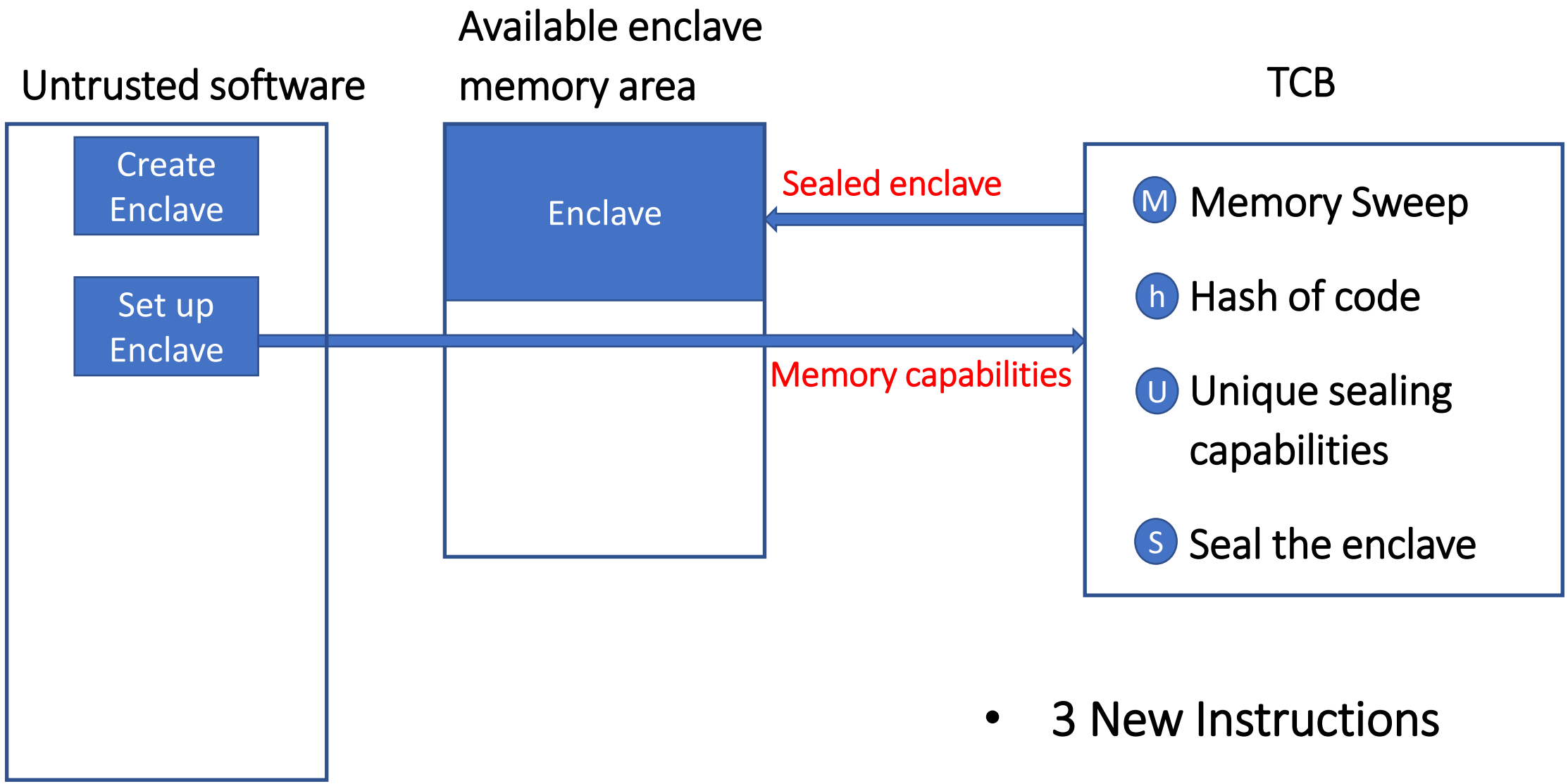


- Isolated regions of memory
- Created during run-time
- Small trusted computing Base TCB

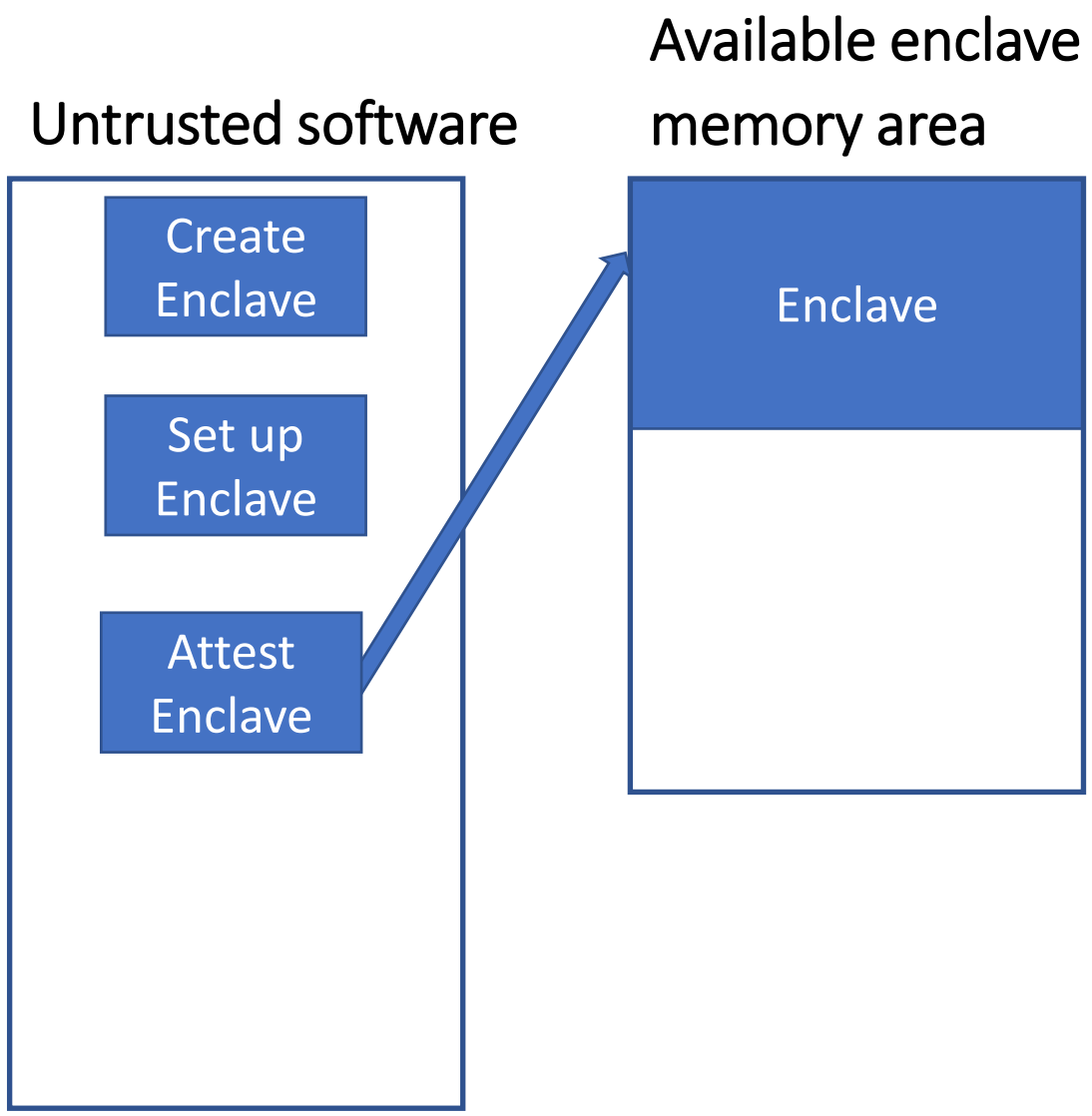
- **Existing CHERI mechanisms**
  - **Sealed capabilities pairs**
- **Two new mechanisms**
  - **To establish trust in an enclave**
    - **exclusive ownership** of a block of **memory** (memory sweep)
    - **Obtaining sealing capabilities** derived from an enclave's identity (**symbolic private key** to encrypt or sign other capabilities)
- **First on a capability-based platform**

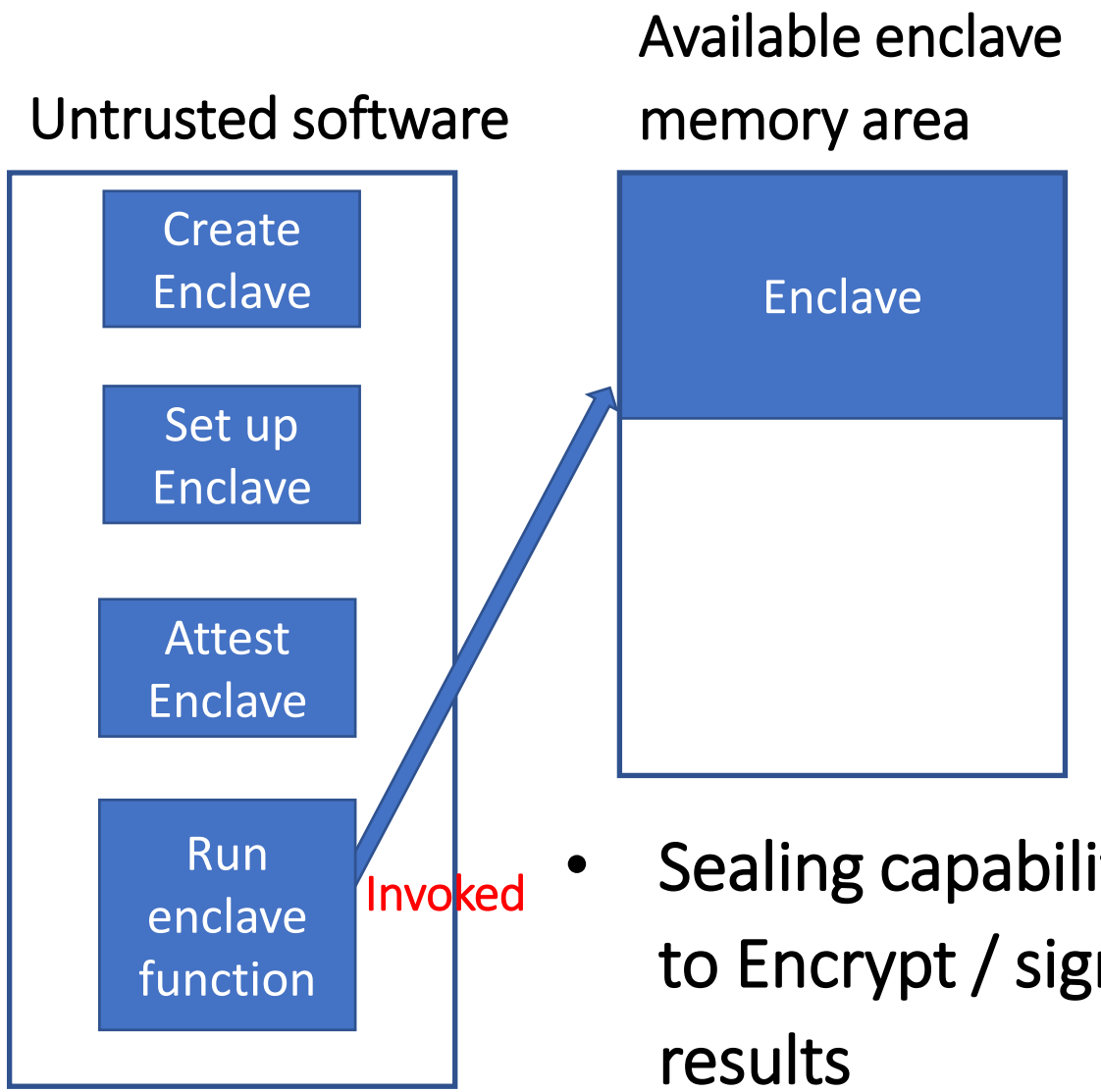
Thomas Van Strydonck, June 2022, PhD Thesis
Formal Reasoning about Hardware Capability Architectures
Chapter 4: CHERI-TrEE: Flexible enclaves on capability machines
https://lirias.kuleuven.be/retrieve/667137


Allocates region of memory
Untrusted software
Copy enclave code
Create Enclave
Enclave
Enclave code
Enclave program memory



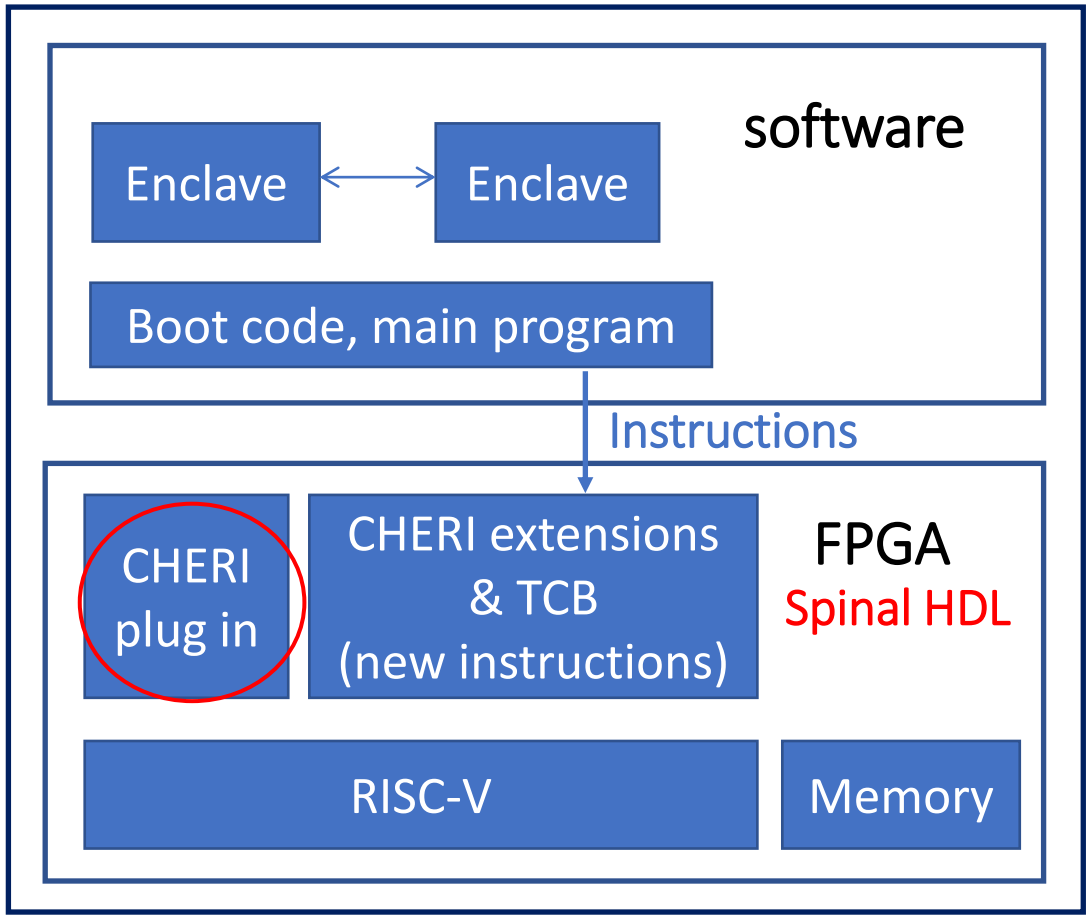
- 3 New Instructions


Untrusted software
Available enclave memory area
Create Enclave
Set up Enclave
Attest Enclave
Enclave

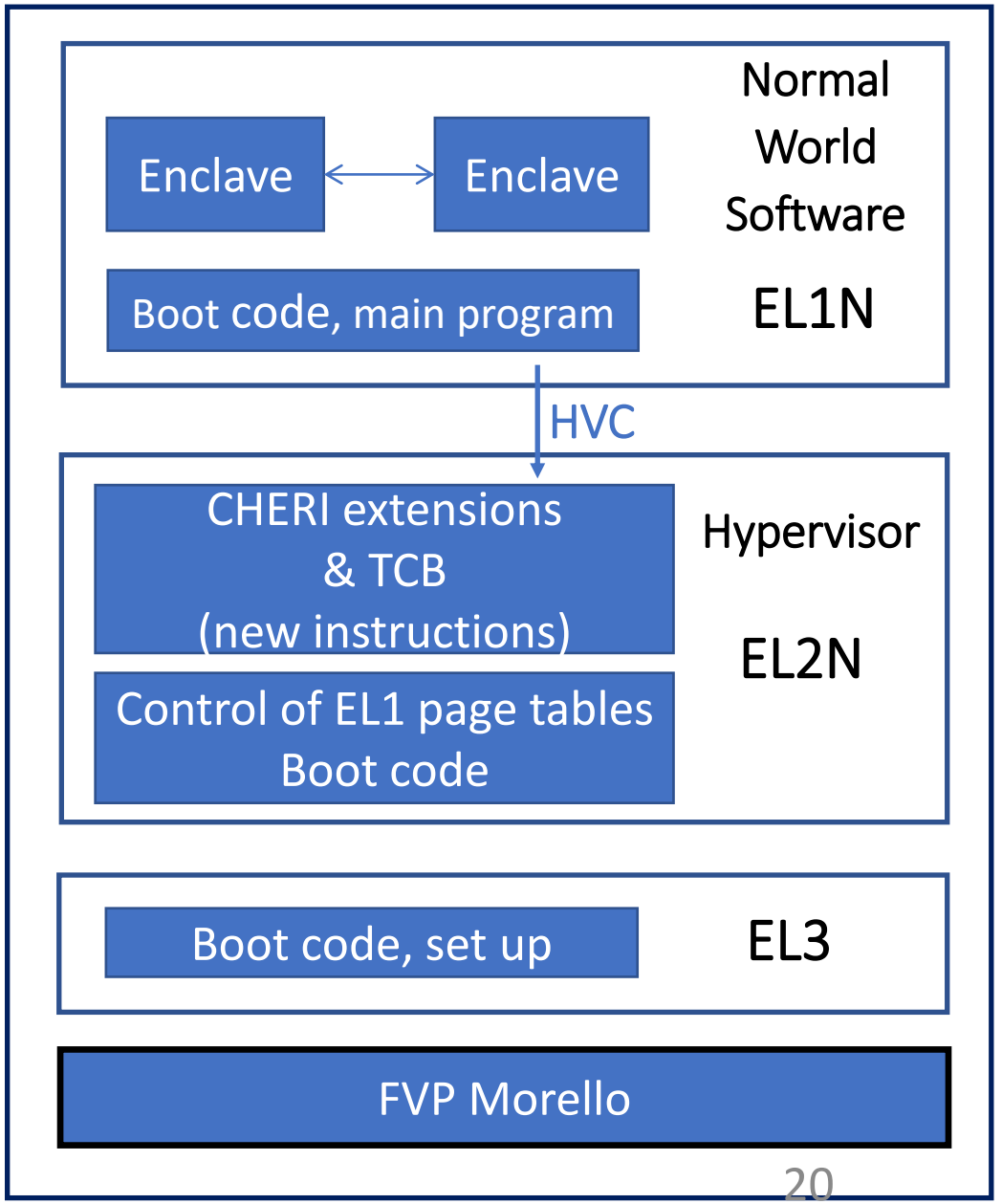


- Sealing capabilities to Encrypt / sign results

RISC-V Prototype



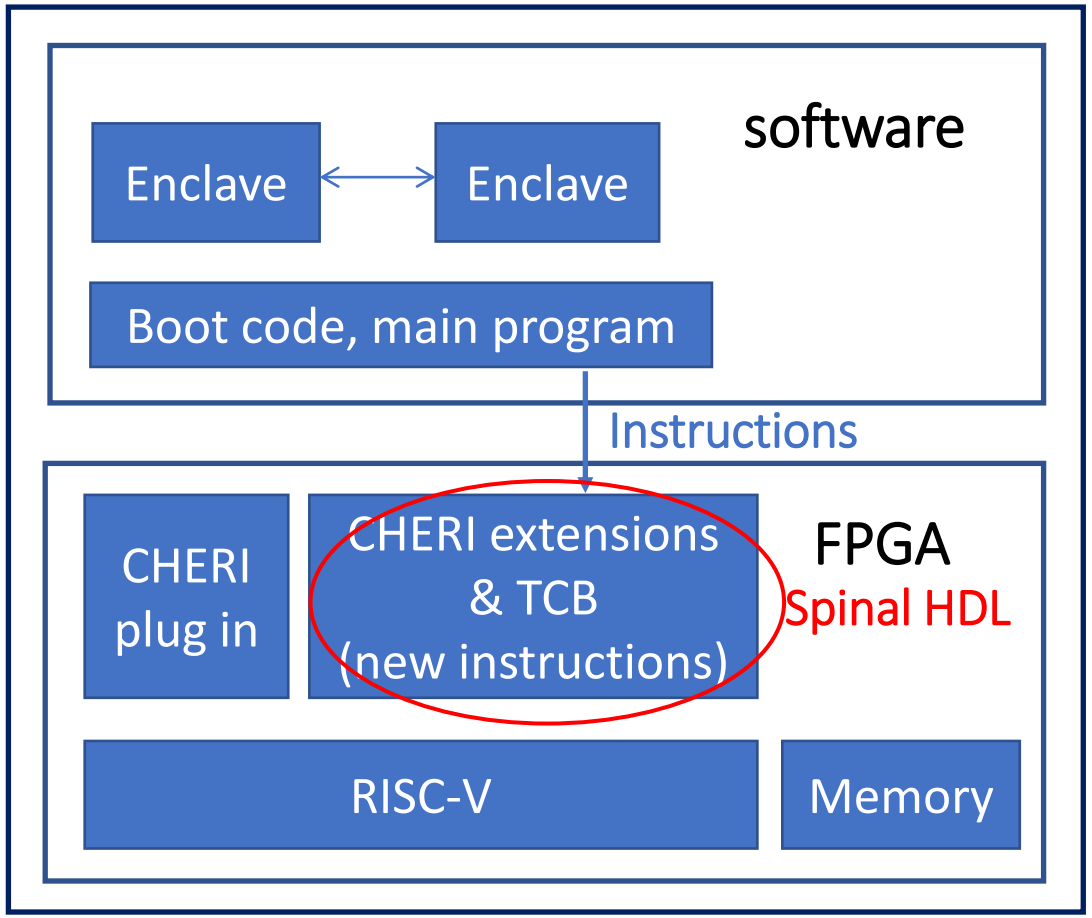
Morello Prototype



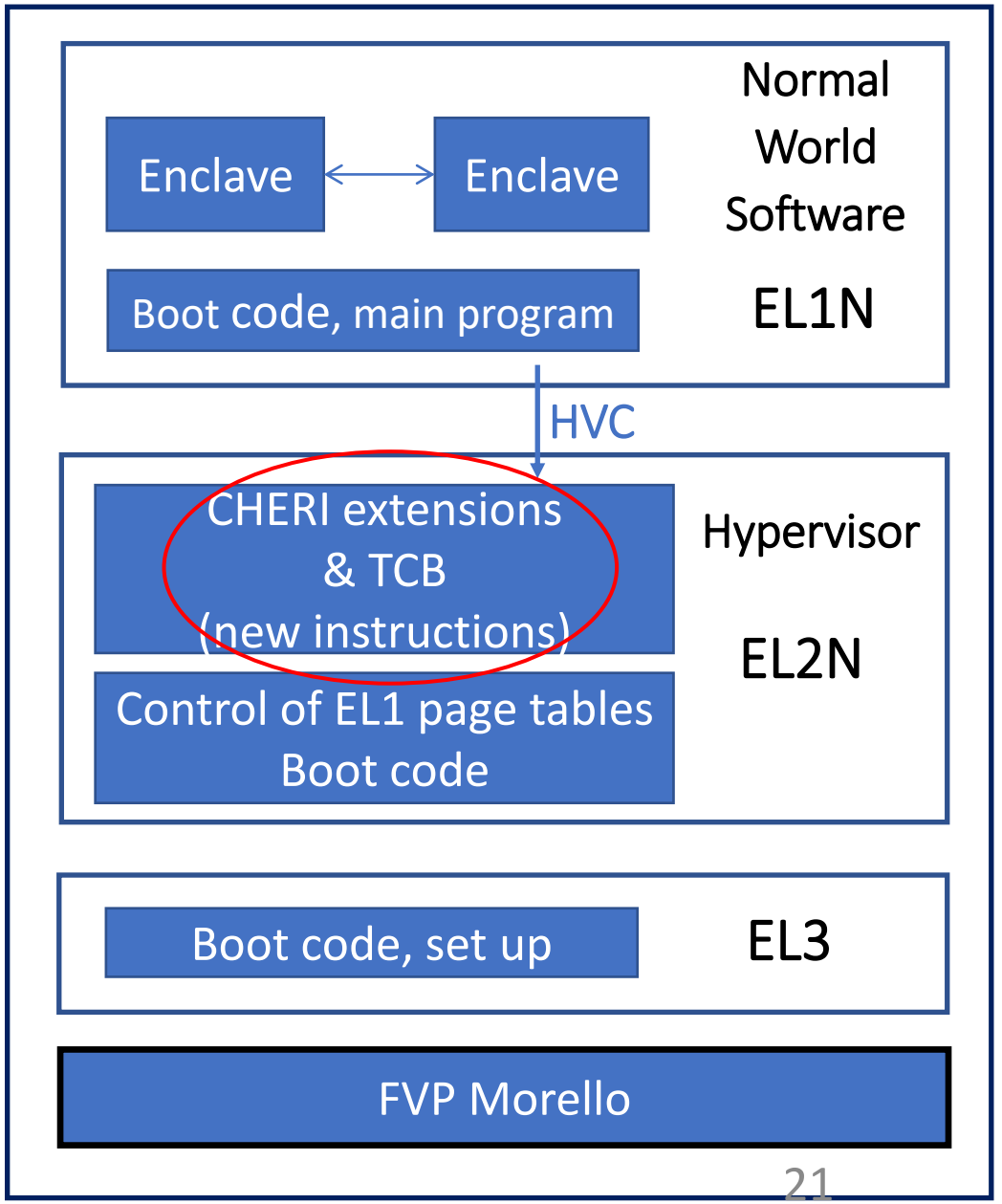
User space enclaves

- In both RISC-V and Morello
- Additional CHERI instructions needed to initialise the enclaves

RISC-V Prototype



Morello Prototype



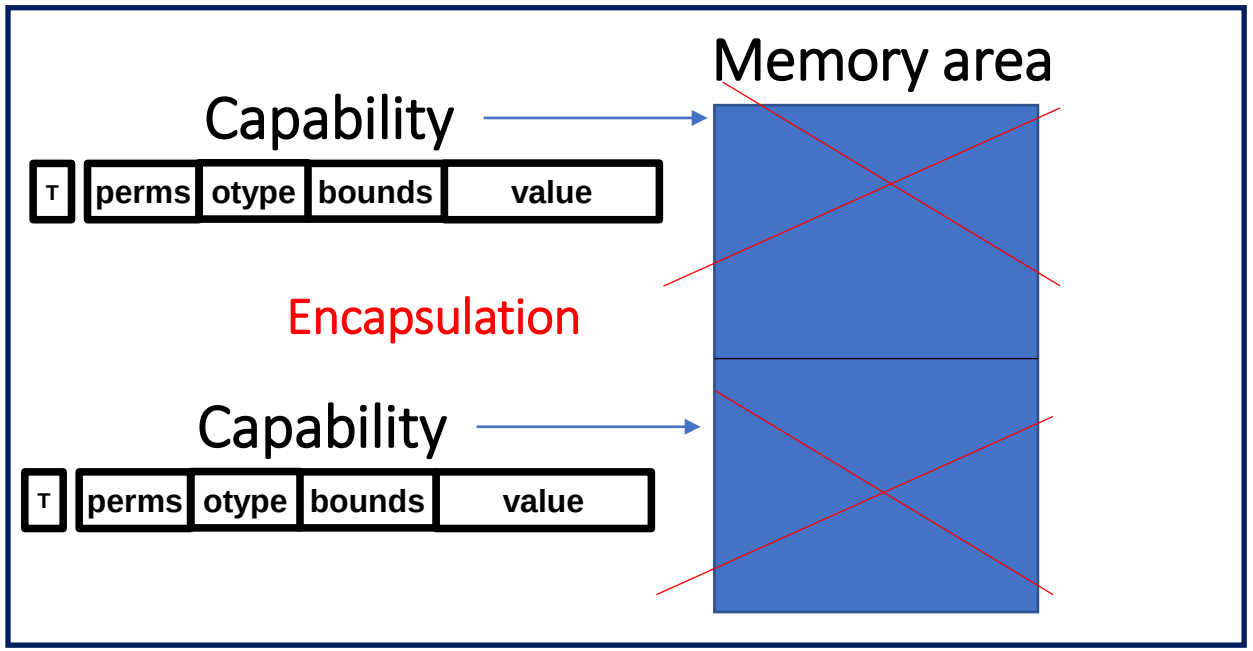
User space enclaves

- In both RISC-V and Morello
- Additional CHERI instructions needed to initialise the enclaves

Object Capabilities and domain switching

- **2015 CHERI**: A Hybrid Capability-System Architecture for Scalable **Software Compartmentalization,** Robert N.M. Watson; Jonathan Woodruff; Peter G. Neumann … 2015 IEEE Symposium on Security and Privacy

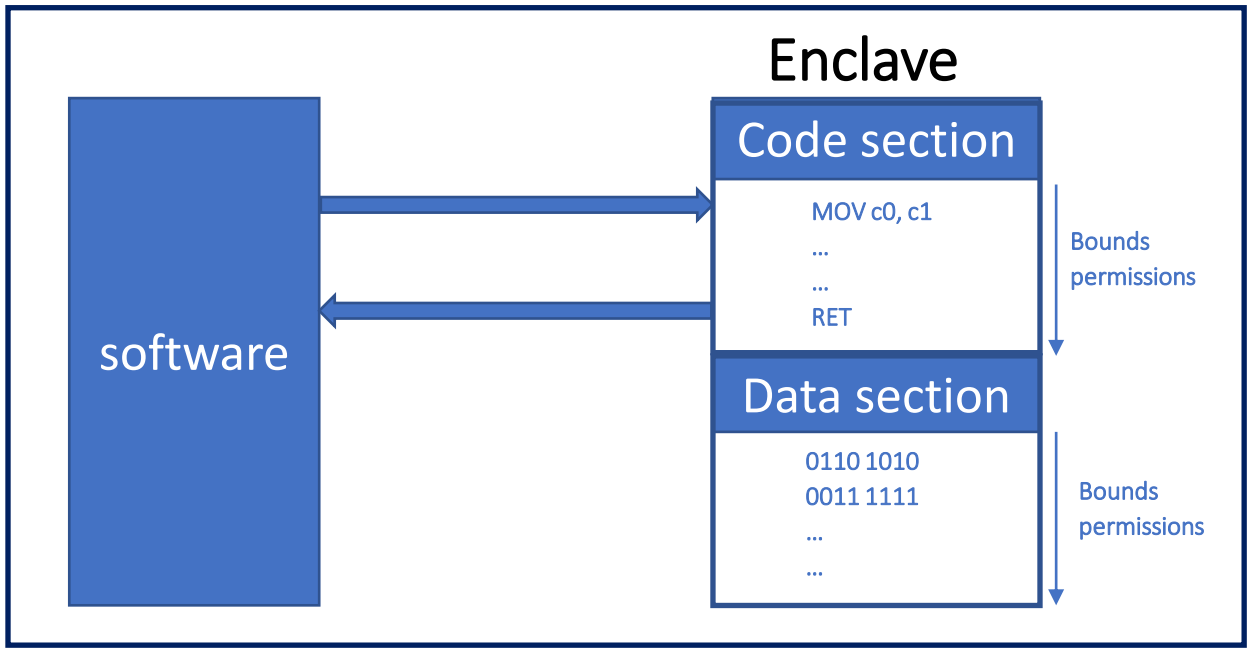
Object Capabilities and domain switching



- **2015 CHERI**: A Hybrid Capability-System Architecture for Scalable **Software Compartmentalization,** Robert N.M. Watson; Jonathan Woodruff; Peter G. Neumann … 2015 IEEE Symposium on Security and Privacy

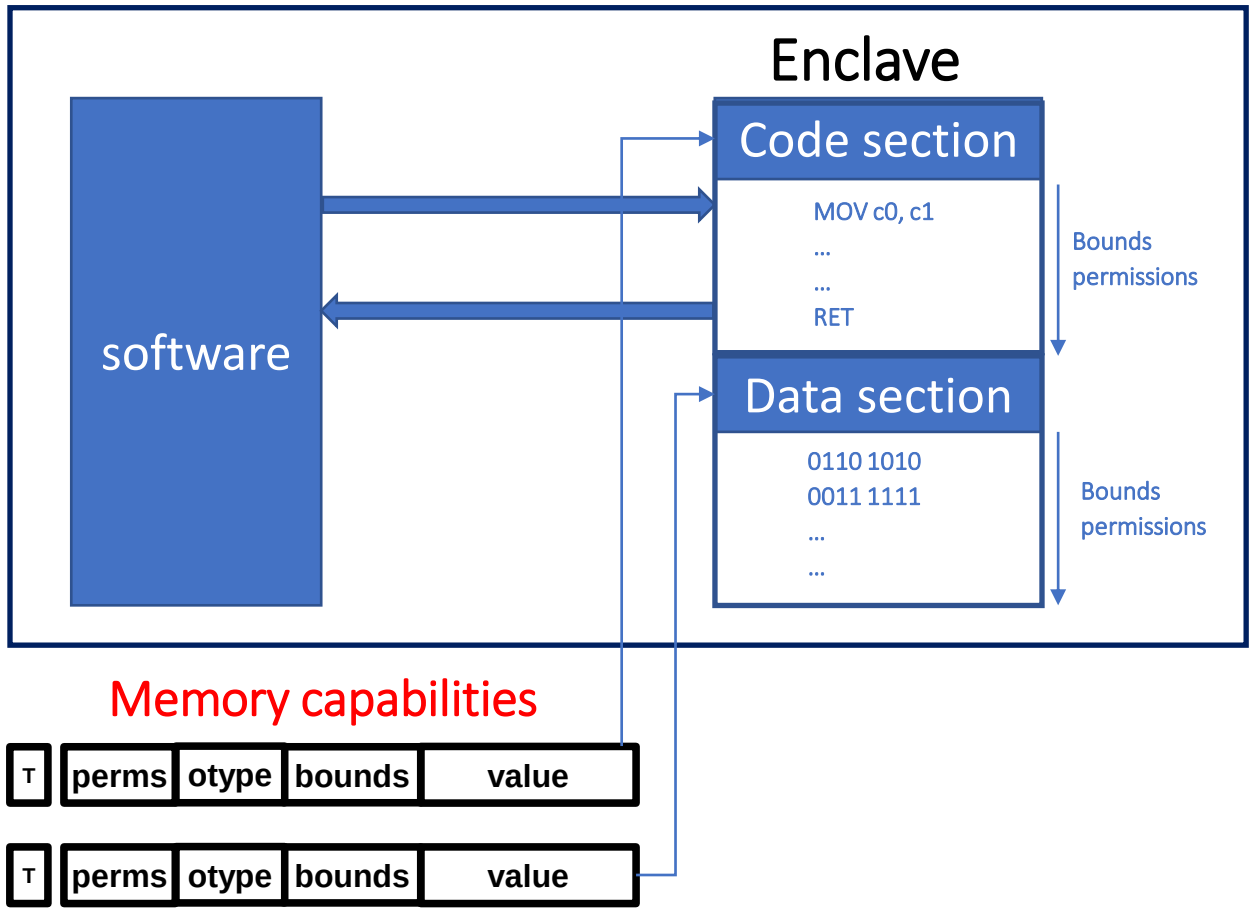
Untrusted access point

Object Capabilities and domain switching



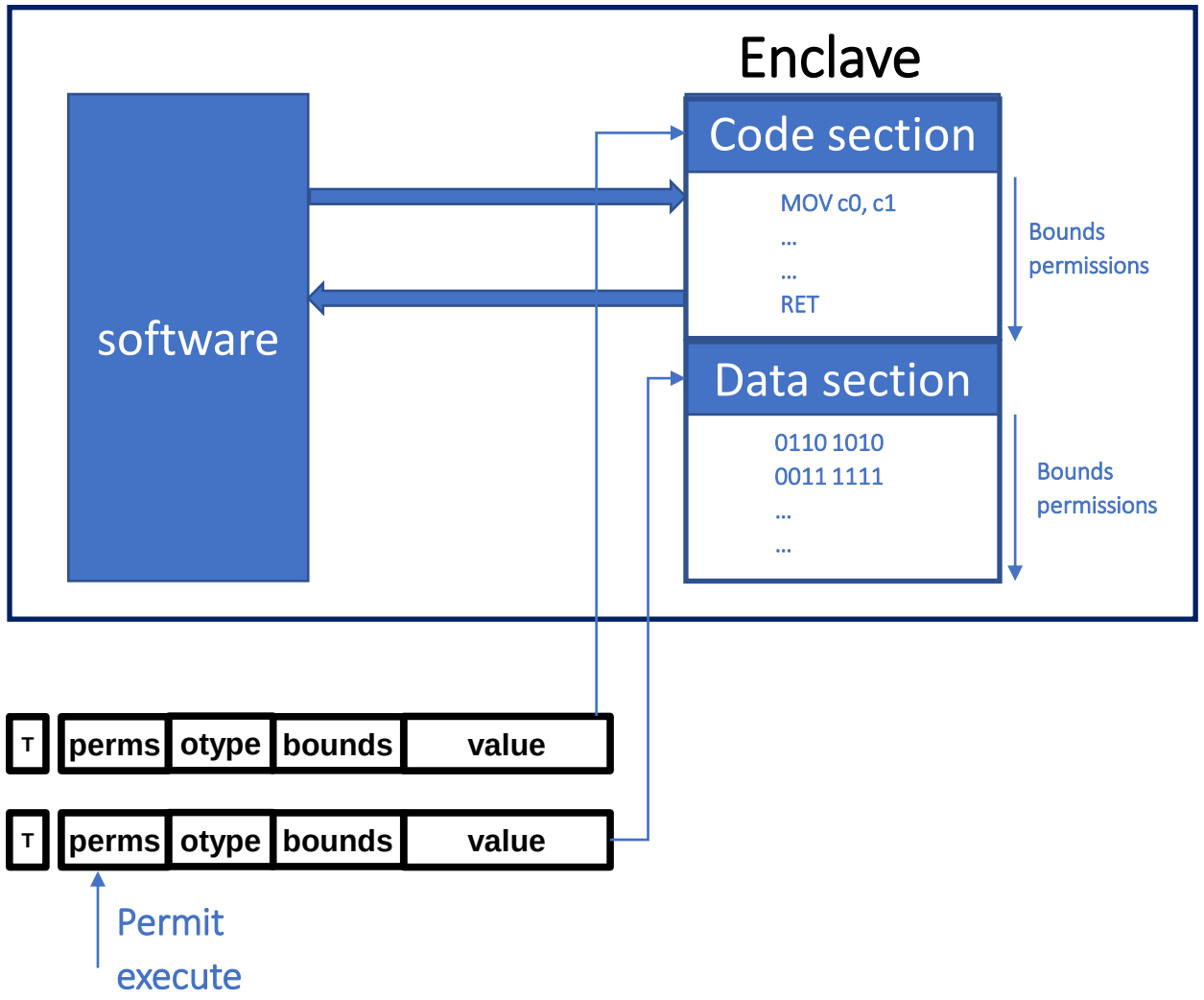
- Enclave consists of two parts, code section and data section

Object Capabilities and domain switching



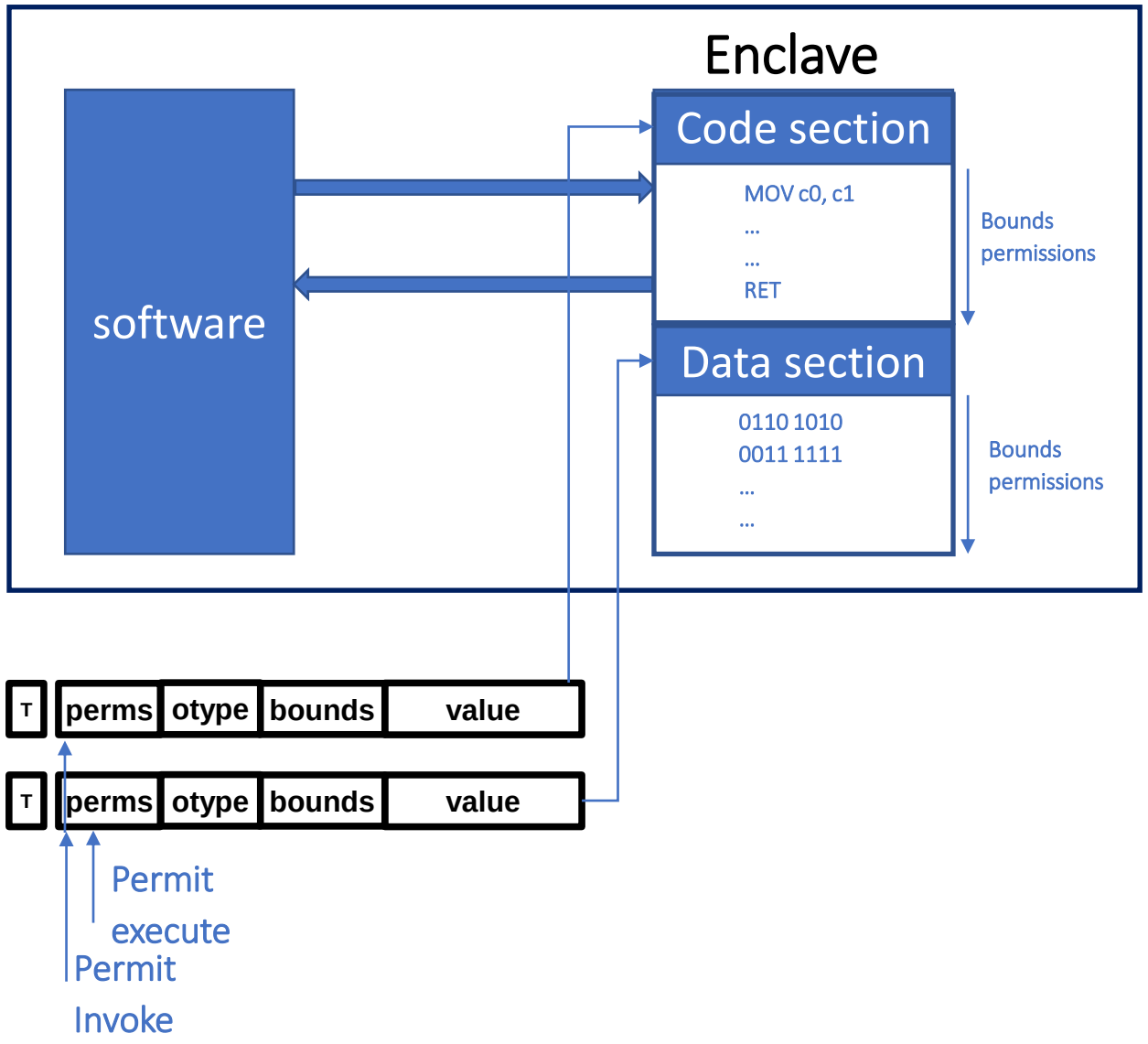
- Enclave consists of two parts, code section and data section
- Each section is represented by a capability with bounds and permissions

Object Capabilities and domain switching



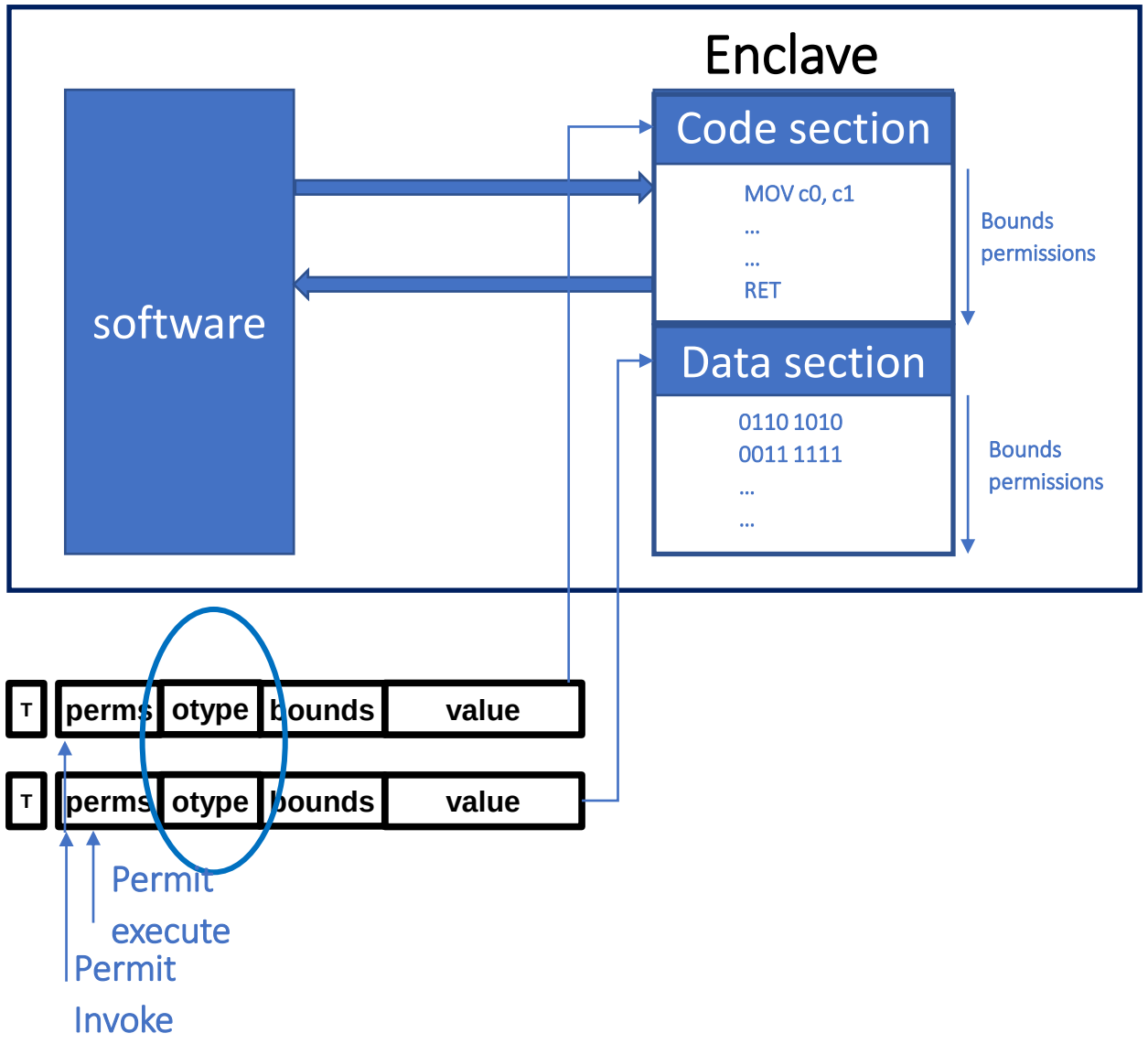
- Enclave consists of two parts, code section and data section
- Each section is represented by a capability with bounds and permissions
- Prevent execution in data region

Object Capabilities and domain switching



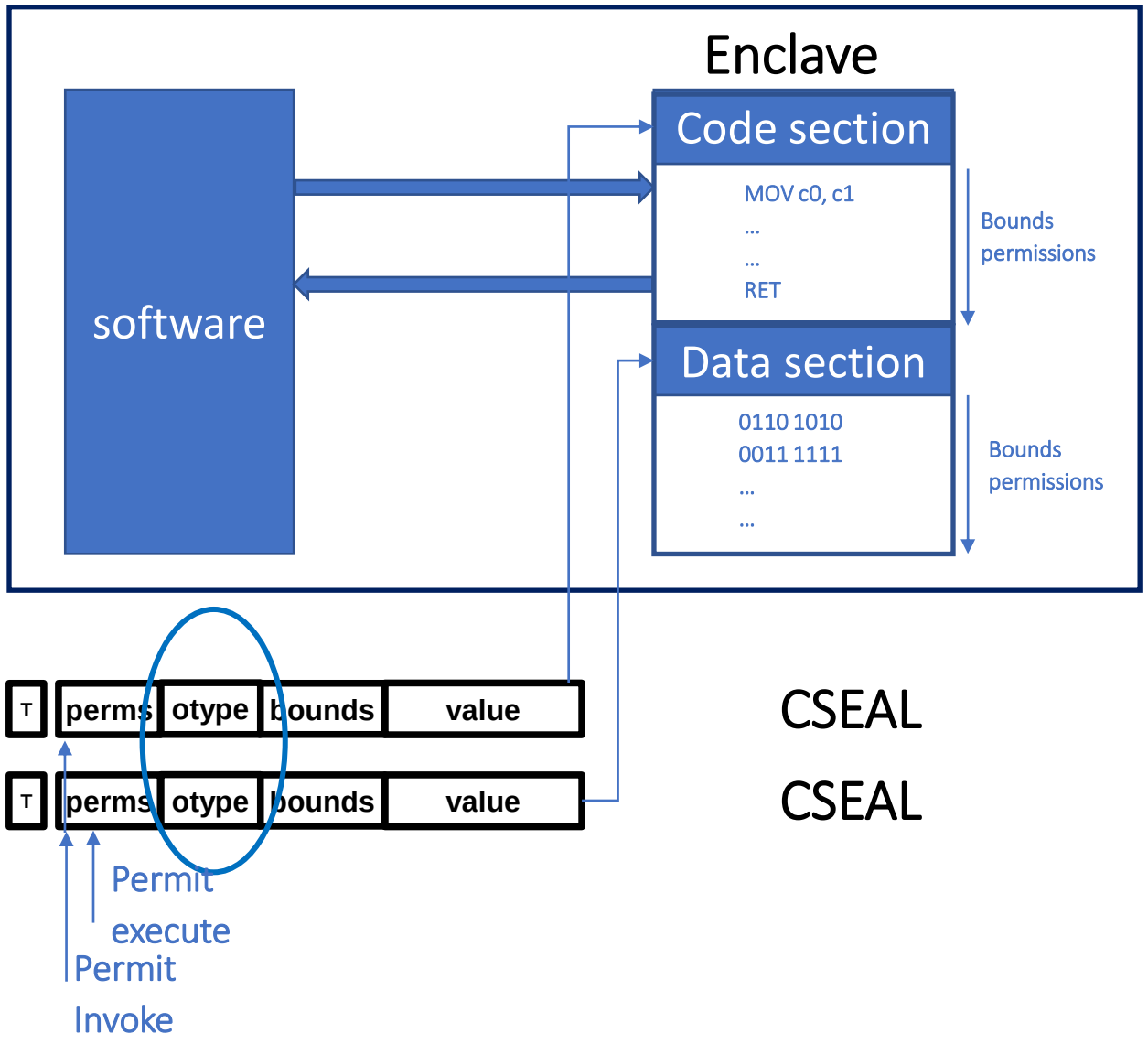
- Enclave consists of two parts, code section and data section
- Each section is represented by a capability with bounds and permissions
- Prevent execution in data region

Object Capabilities and domain switching



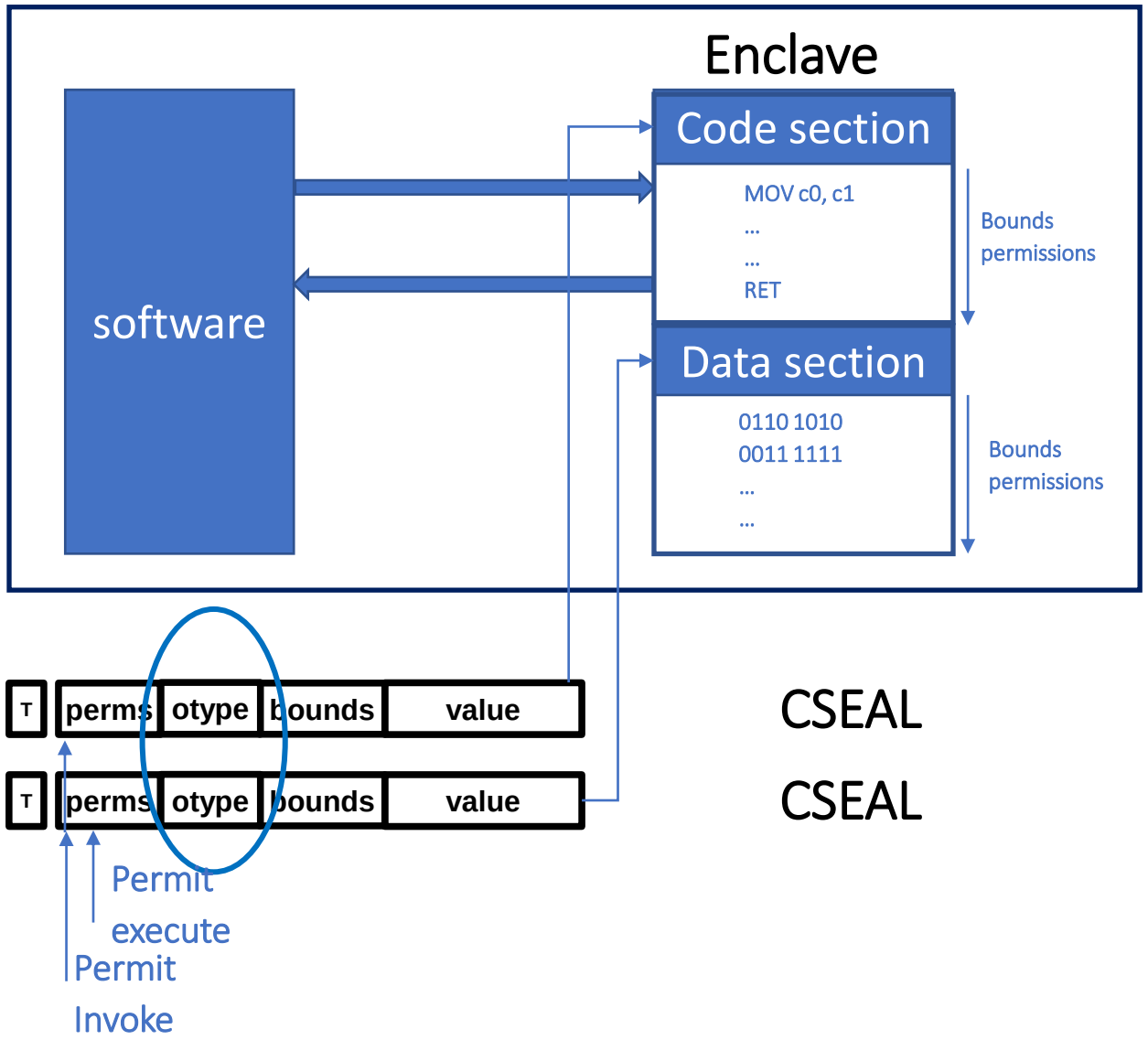
- Enclave consists of two parts, code section and data section
- Each section is represented by a capability with bounds and permissions
- Prevent execution in data region
- Uniquely pair capabilities

Object Capabilities and domain switching

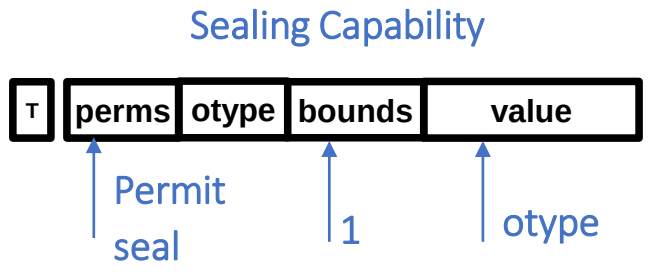


- Enclave consists of two parts, code section and data section
- Each section is represented by a capability with bounds and permissions
- Prevent execution in data region
- Uniquely pair capabilities
- Encapsulation done through sealing

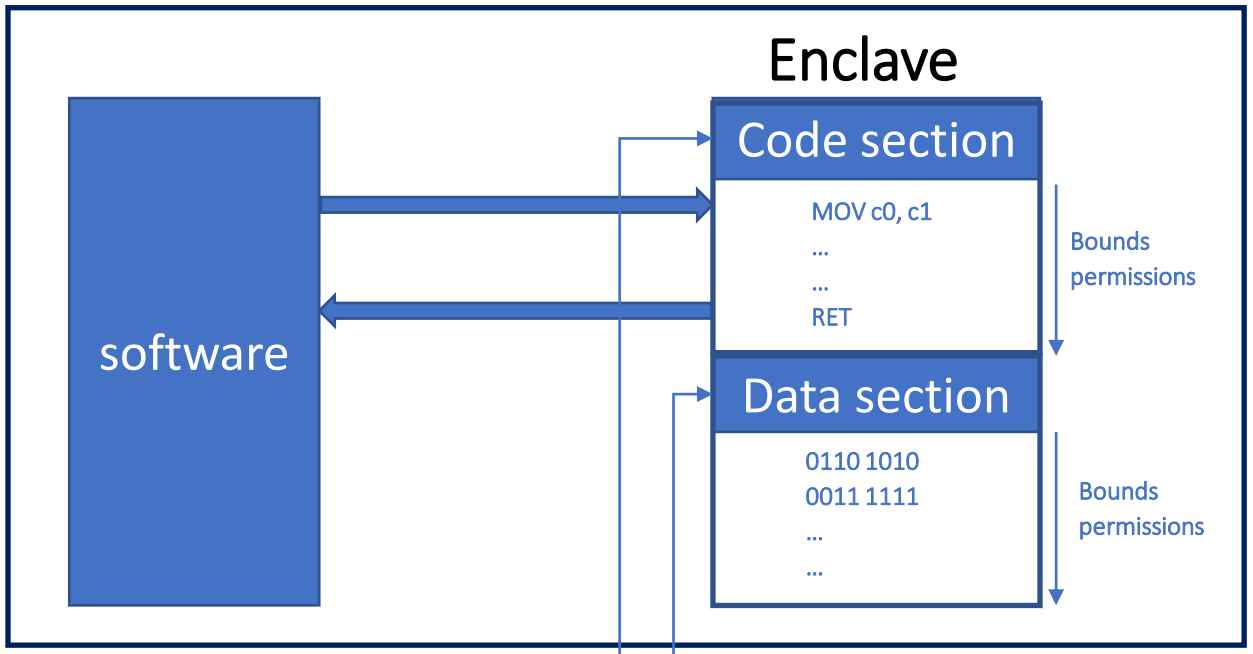
Object Capabilities and domain switching



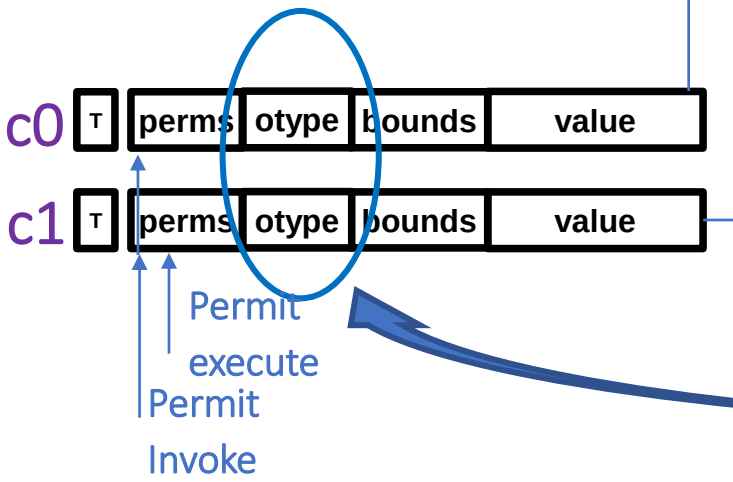
- Enclave consists of two parts, code section and data section
- Each section is represented by a capability with bounds and permissions
- Prevent execution in data region
- Uniquely pair capabilities
- Encapsulation done through sealing



Object Capabilities and domain switching

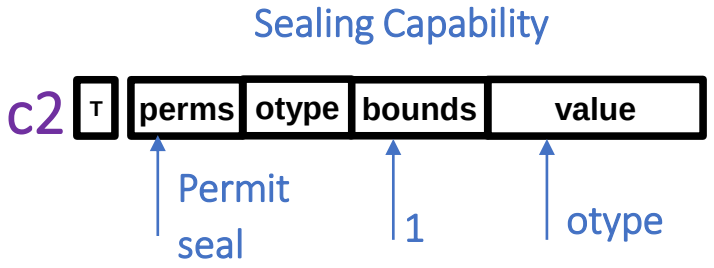


- Enclave consists of two parts, code section and data section
- Each section is represented by a capability with bounds and permissions
- Prevent execution in data region
- Uniquely pair capabilities
- Encapsulation done through sealing

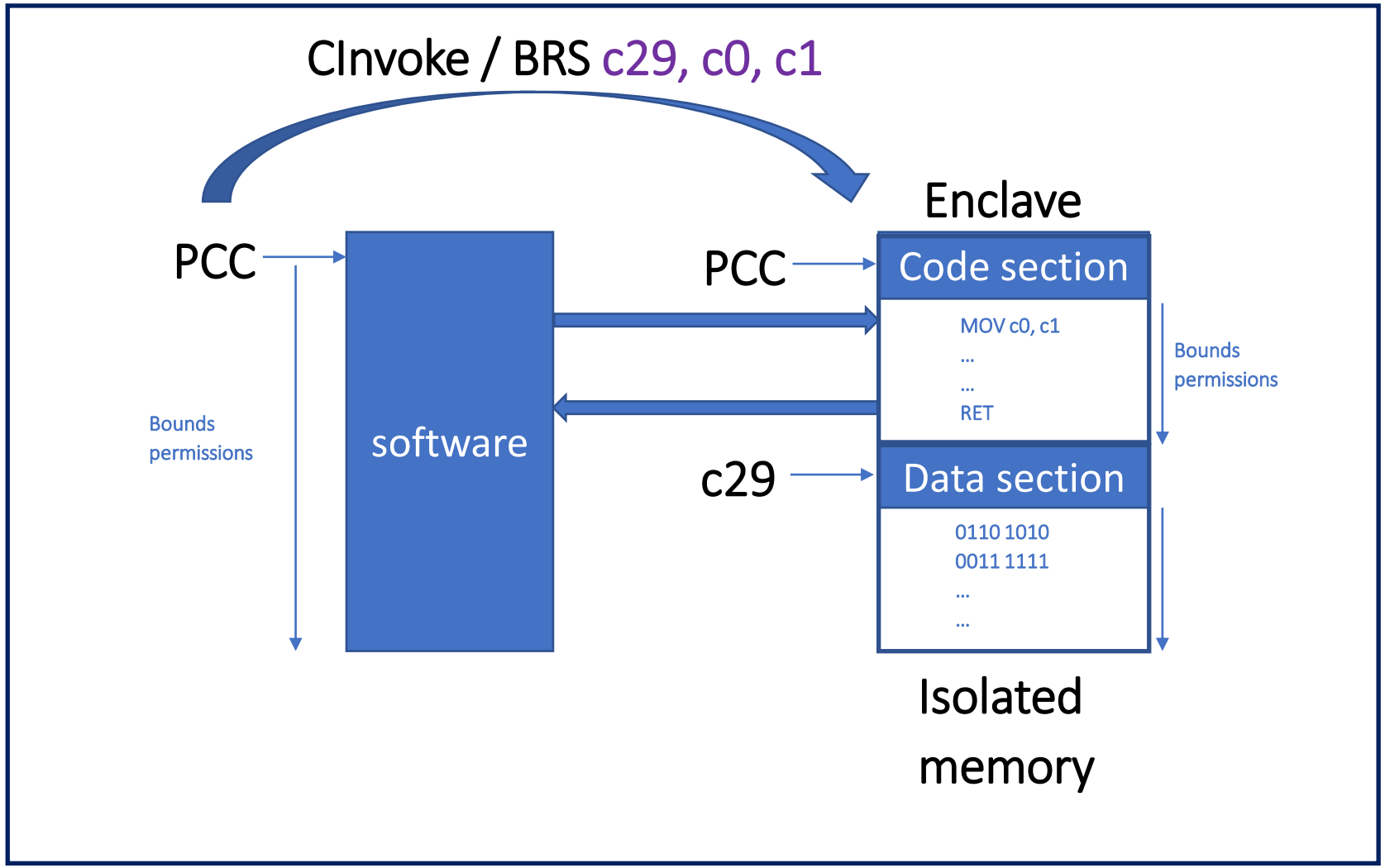


CSEAL c0, c0, c2

CSEAL c1, c1, c2



Object Capabilities and domain switching

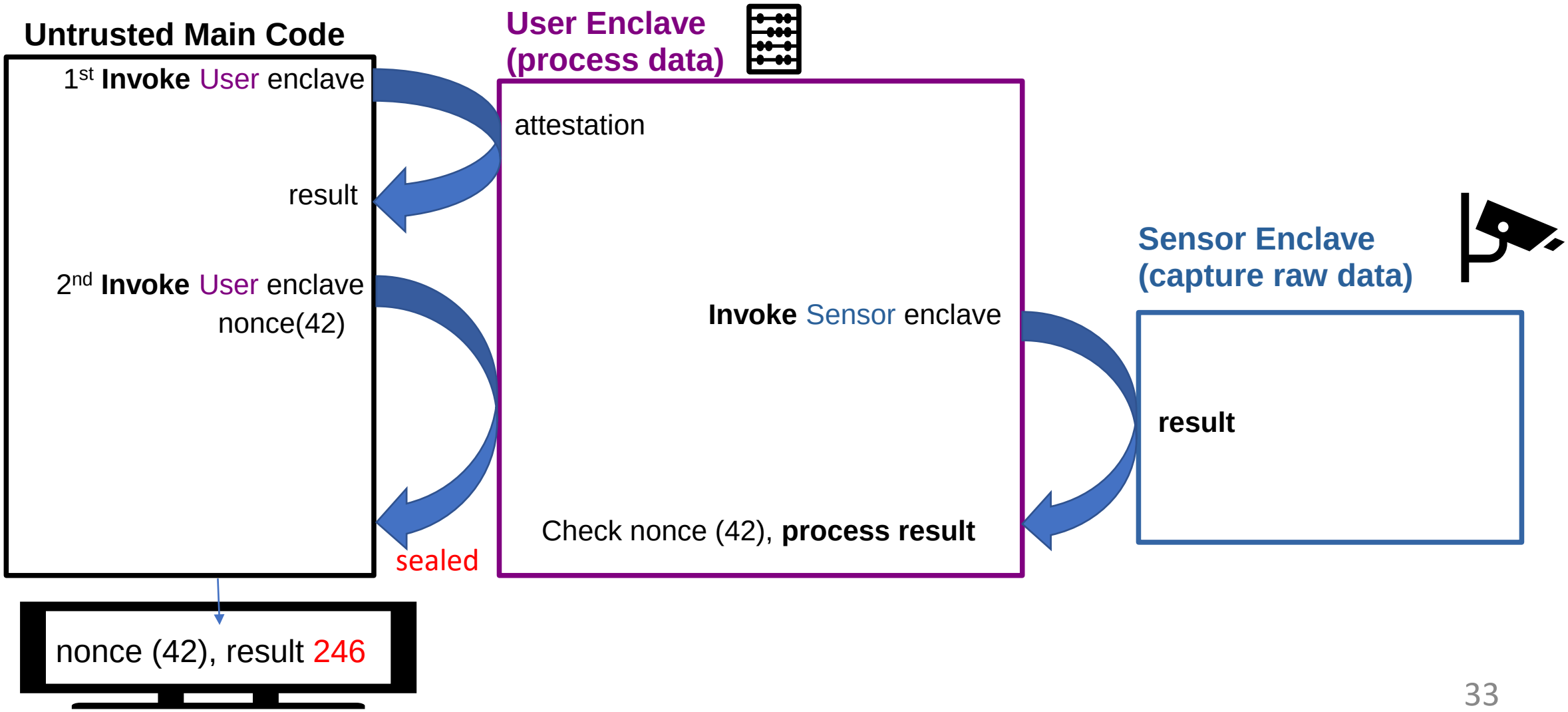


Only way to access Enclave

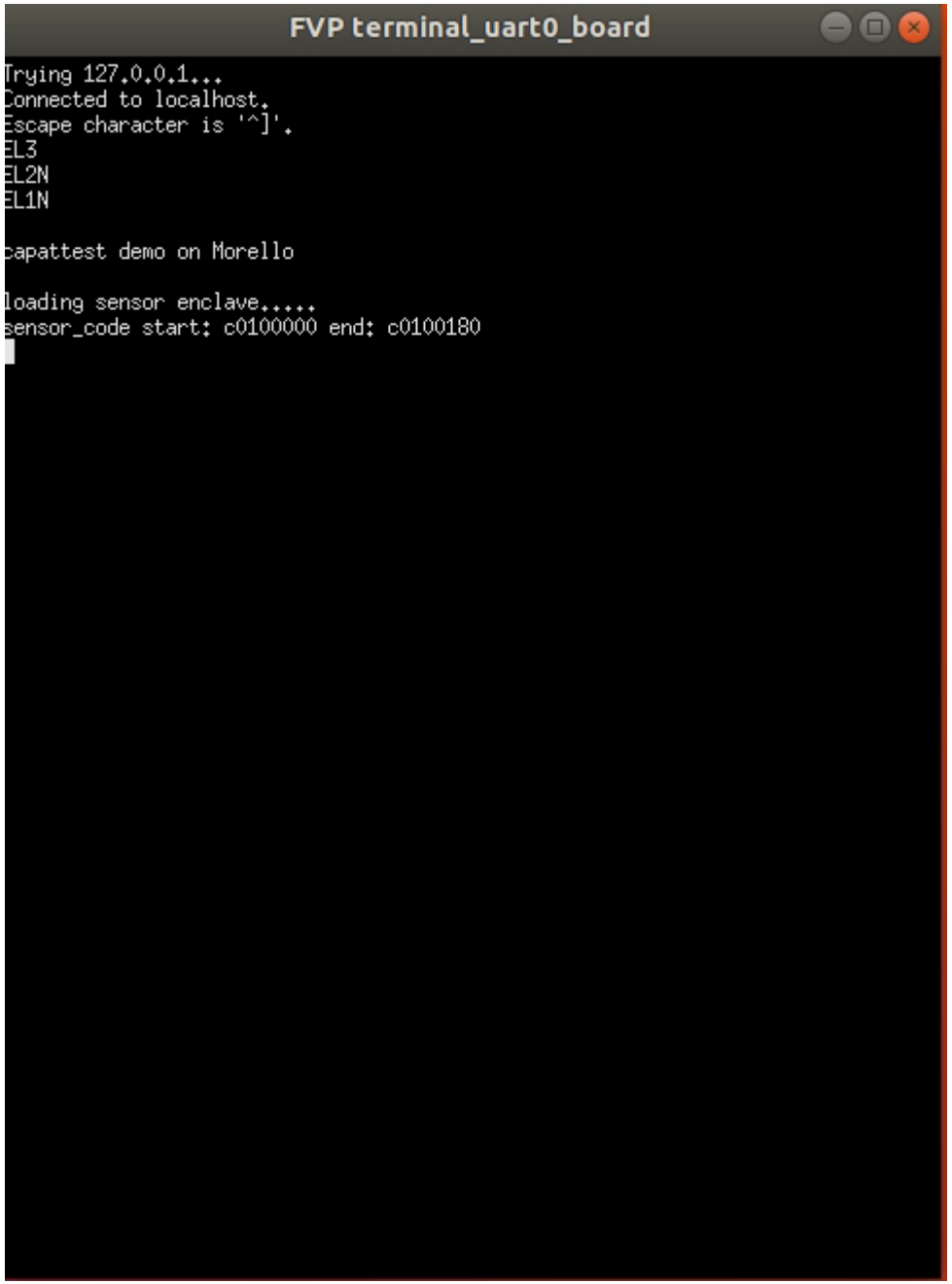
Code & data Unsealed

Run trusted code

Demo and data processing scenario



Demo and data processing scenario



End