Elasticlave:
An Efficient Memory Model for Enclaves

Jason Zhijingcheng Yu, Shweta Shinde, Trevor E. Carlson, Prateek Saxena

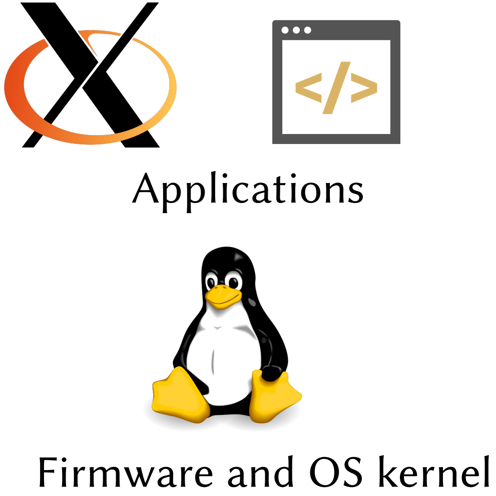
NUS National University of Singapore

ETH zürich

Spatial Isolation in Intel SGX

Spatial Isolation in Intel SGX

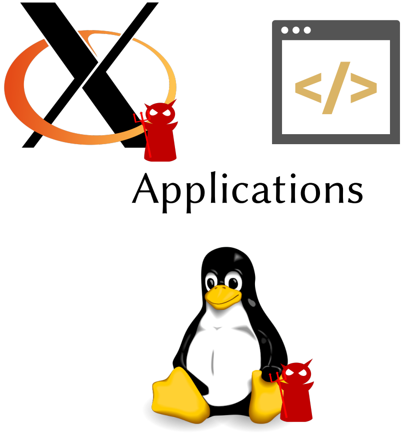
Spatial Isolation in Intel SGX



Applications

Firmware and OS kernel

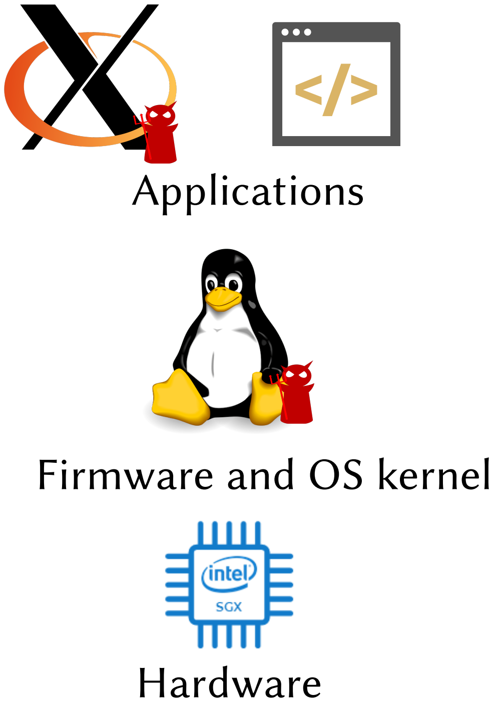
Spatial Isolation in Intel SGX



Applications

Firmware and OS kernel

Spatial Isolation in Intel SGX

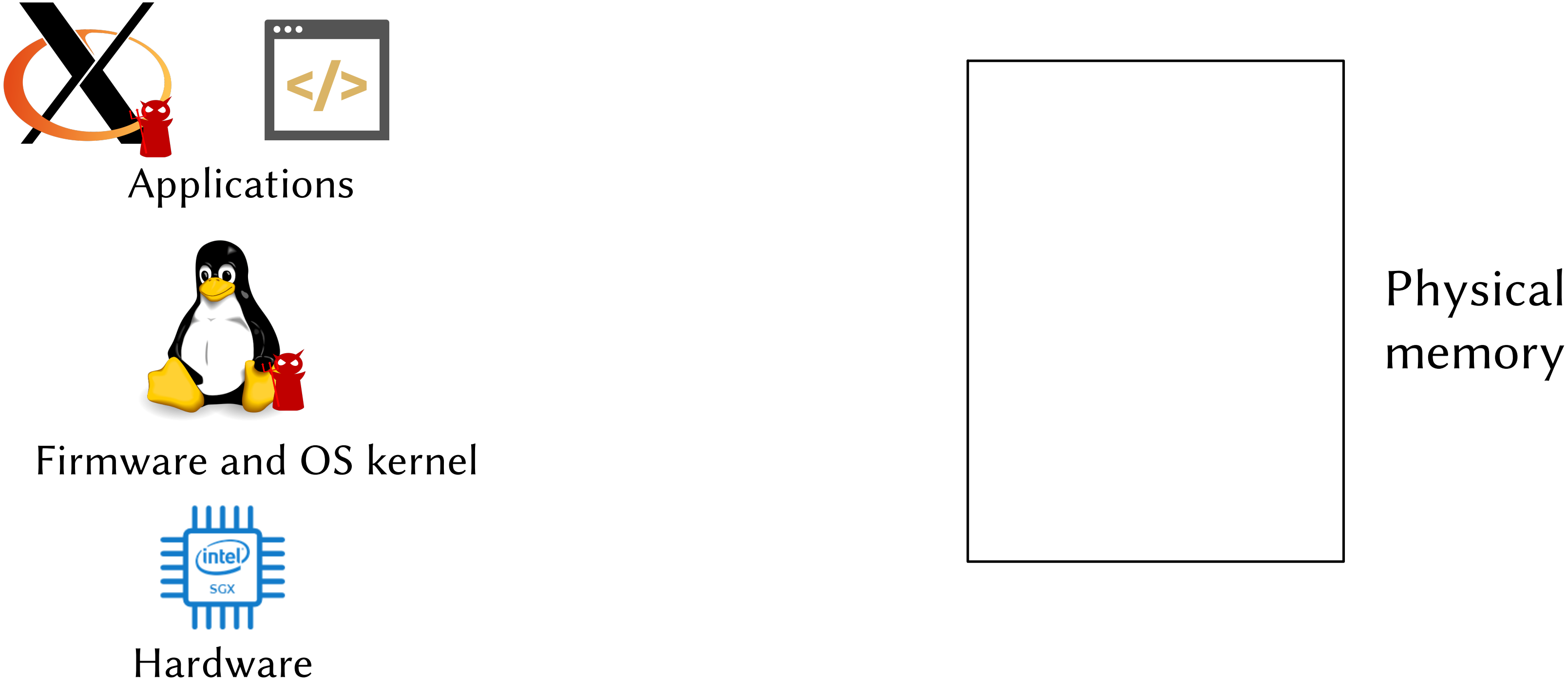


Applications

Firmware and OS kernel

Hardware

Spatial Isolation in Intel SGX



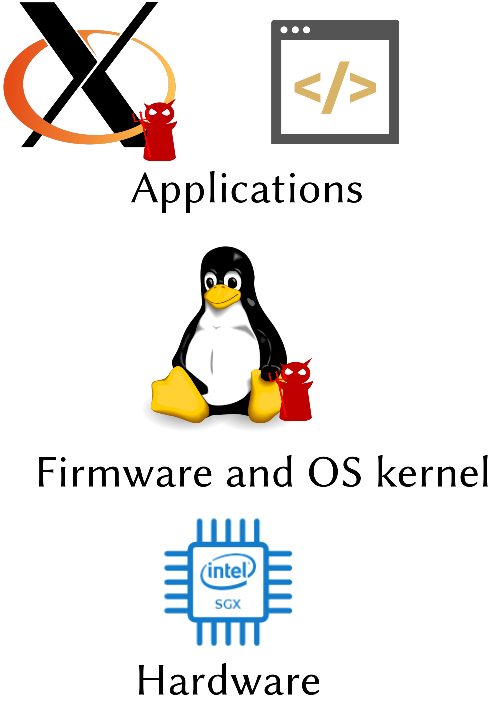
Applications

Firmware and OS kernel

Hardware

Physical memory

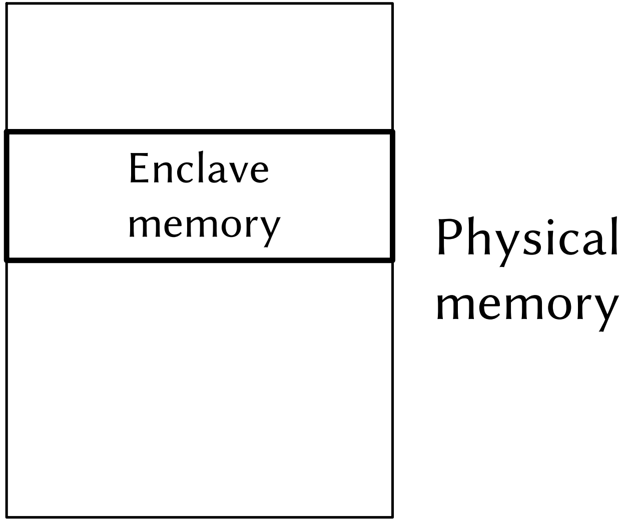
Spatial Isolation in Intel SGX



Applications

Firmware and OS kernel

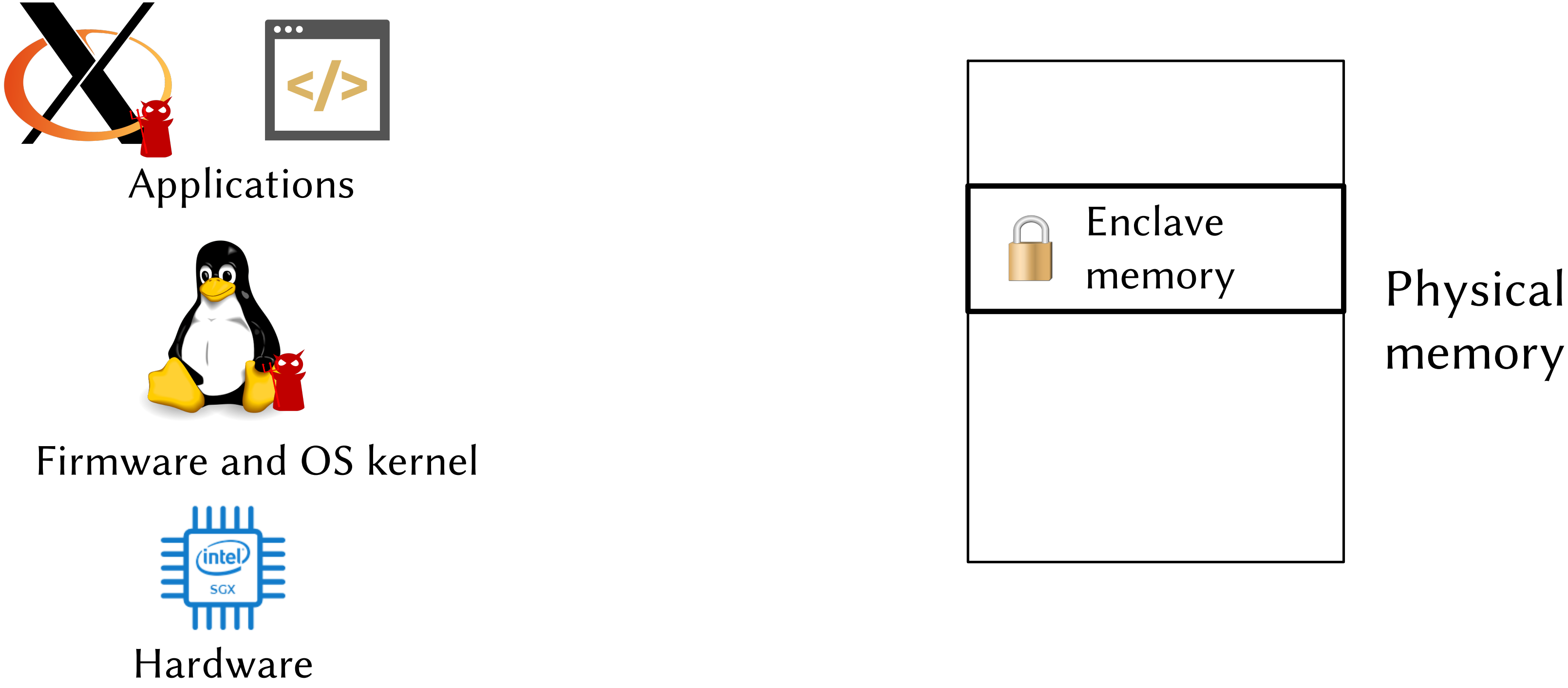
Hardware



Enclave memory

Physical memory

Spatial Isolation in Intel SGX



Applications

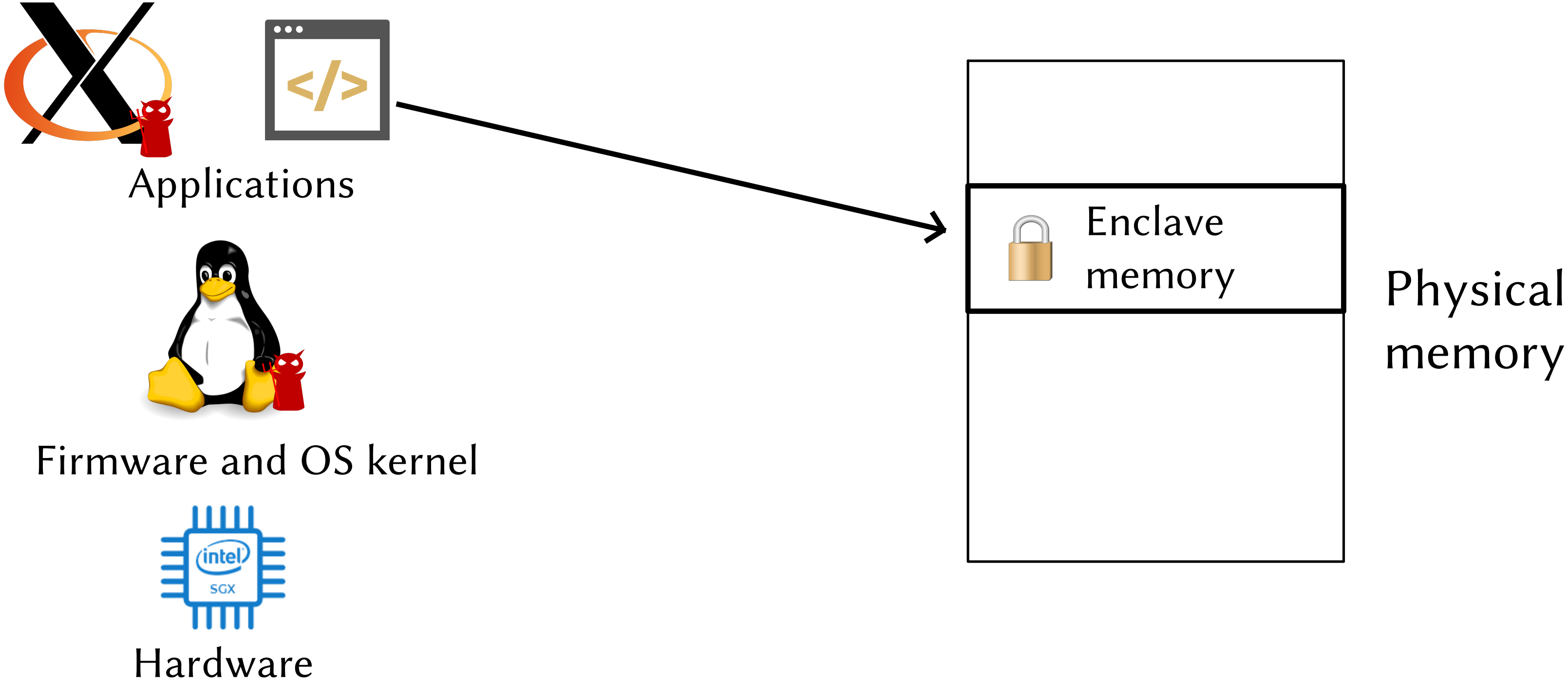
Firmware and OS kernel

Hardware

Enclave memory

Physical memory

Spatial Isolation in Intel SGX



Applications

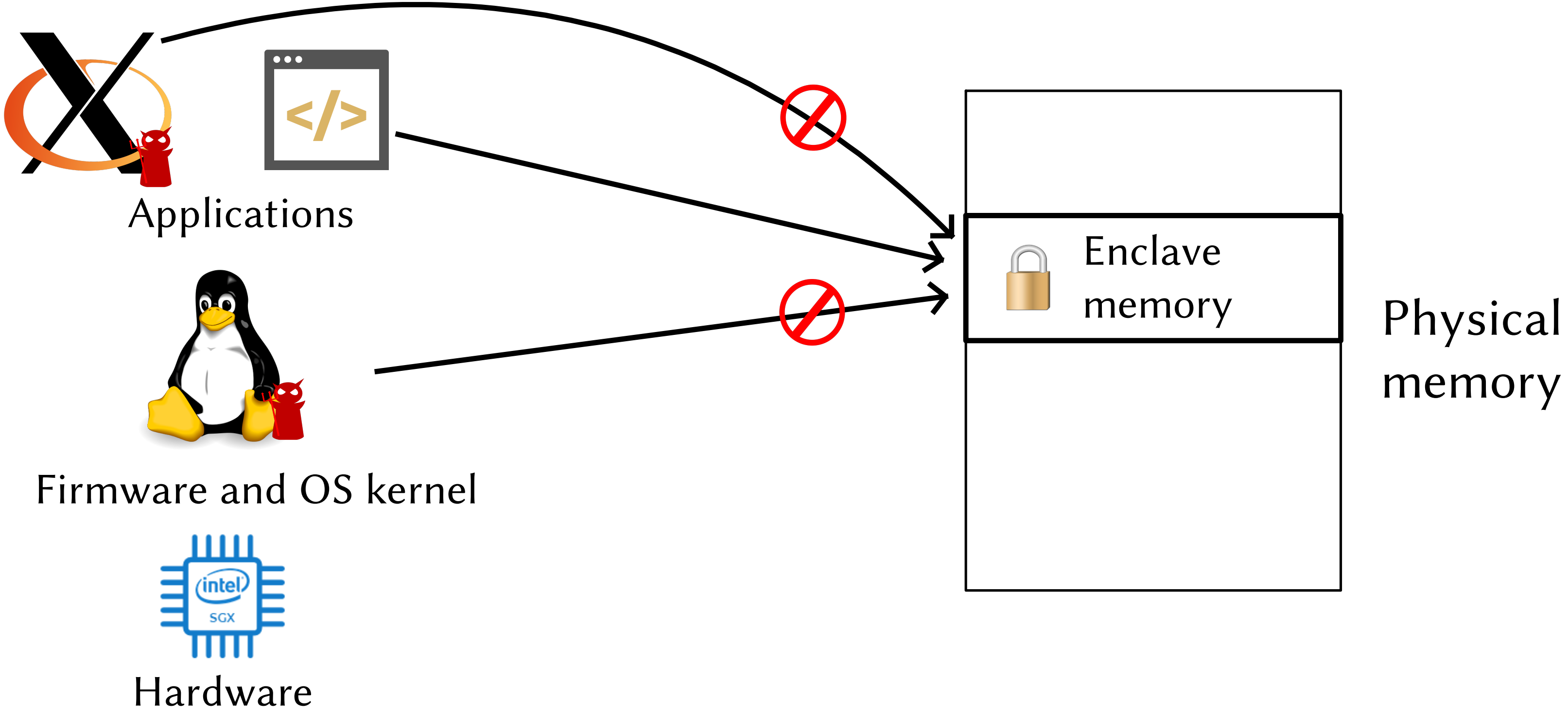
Firmware and OS kernel

Hardware

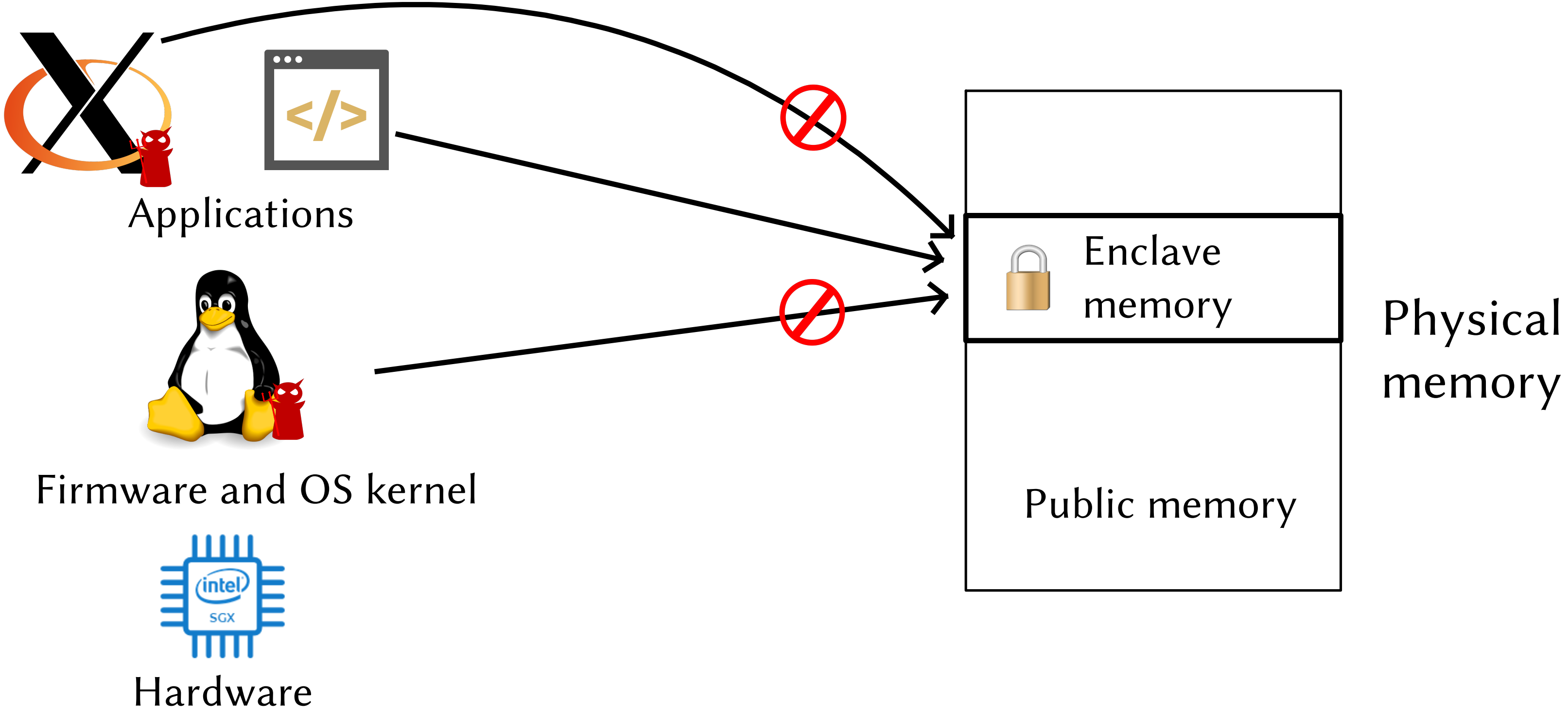
Enclave memory

Physical memory

Spatial Isolation in Intel SGX



Spatial Isolation in Intel SGX



Applications

Firmware and OS kernel

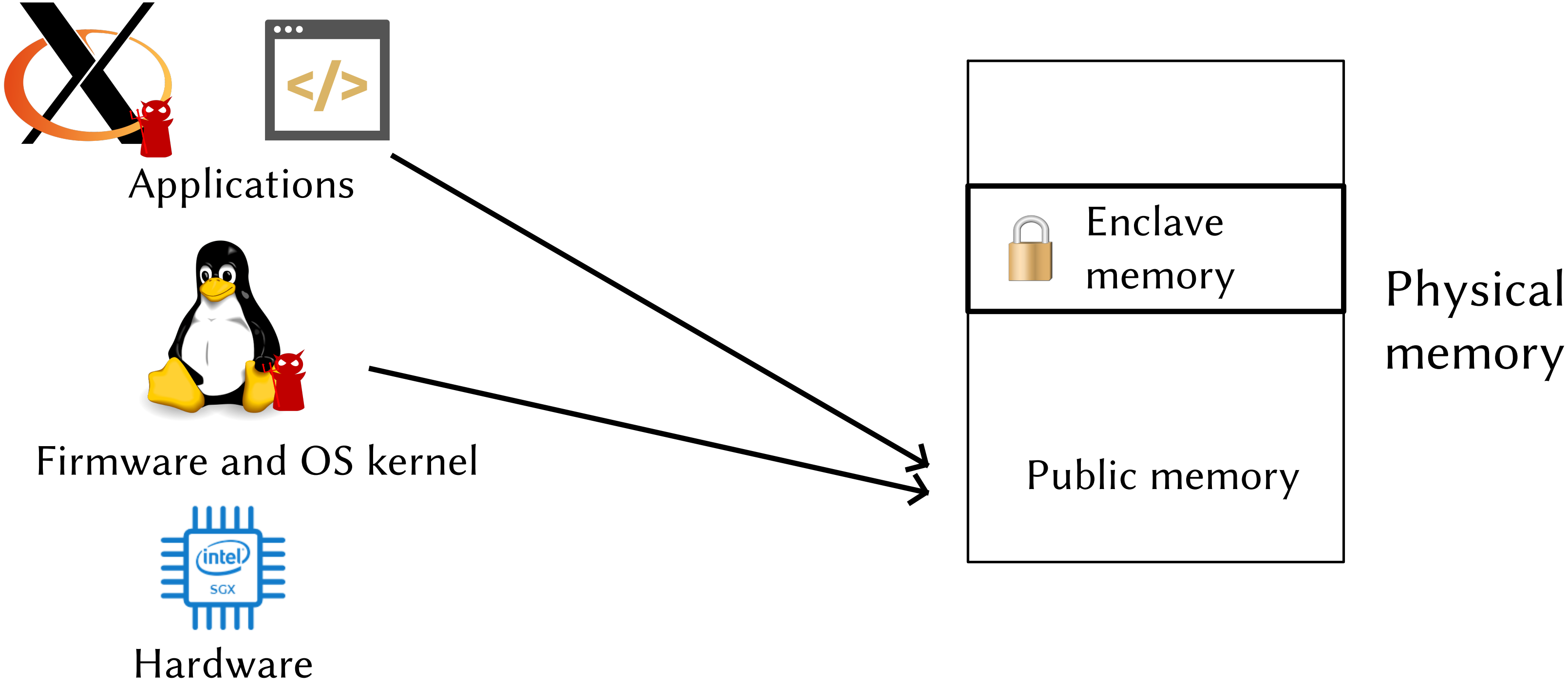
Hardware

Enclave memory

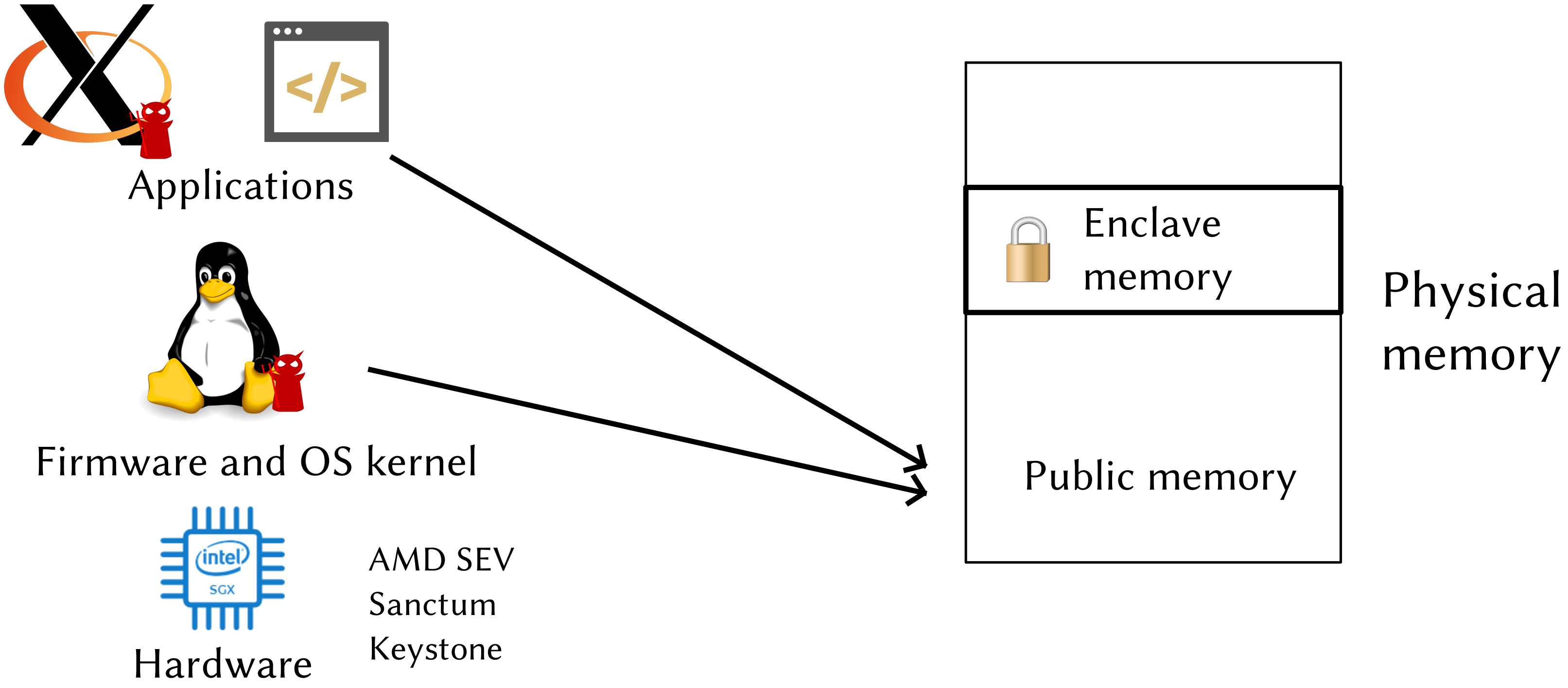
Public memory

Physical memory

Spatial Isolation in Intel SGX



Spatial Isolation in Intel SGX



Applications

Firmware and OS kernel

Hardware

AMD SEV
Sanctum
Keystone

Enclave memory

Public memory

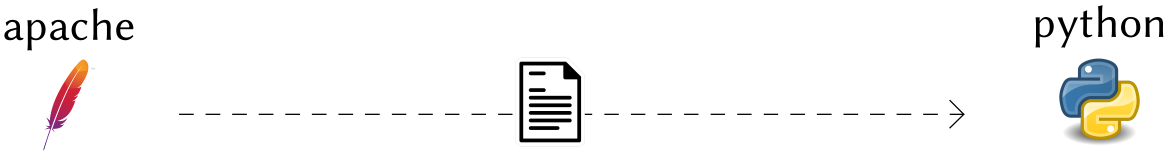
Physical memory

Problems due to Spatial Isolation

Limited in data sharing expressiveness

Problems due to Spatial Isolation

Limited in data sharing expressiveness

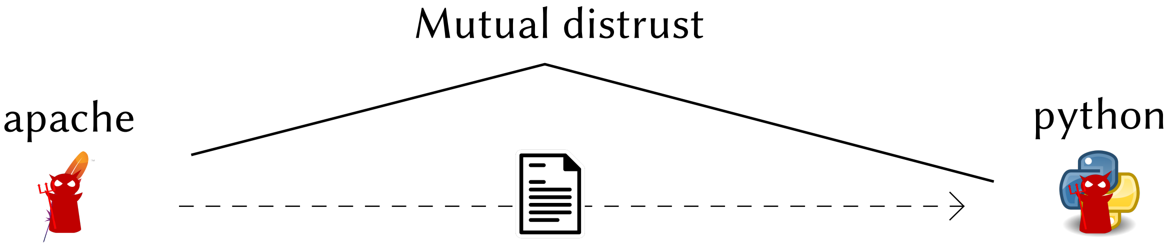


apache

python

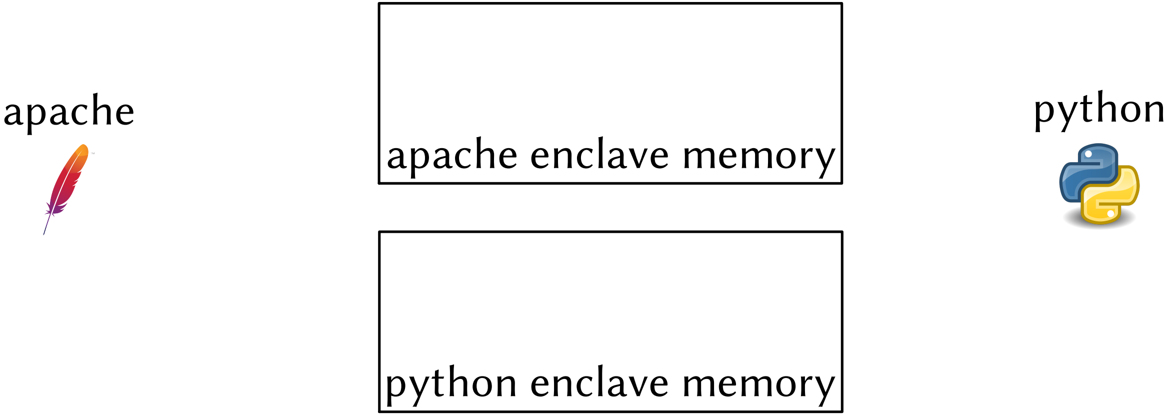
Problems due to Spatial Isolation

Limited in data sharing expressiveness



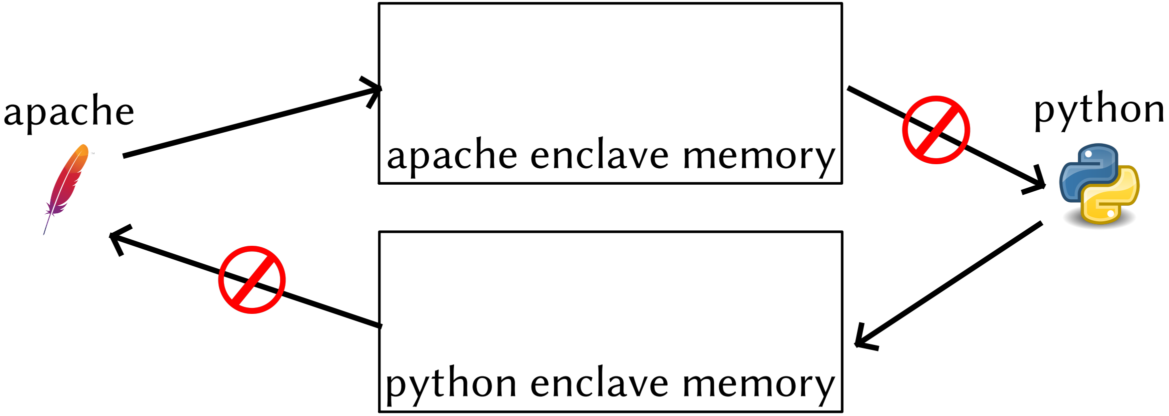
Problems due to Spatial Isolation

Limited in data sharing expressiveness



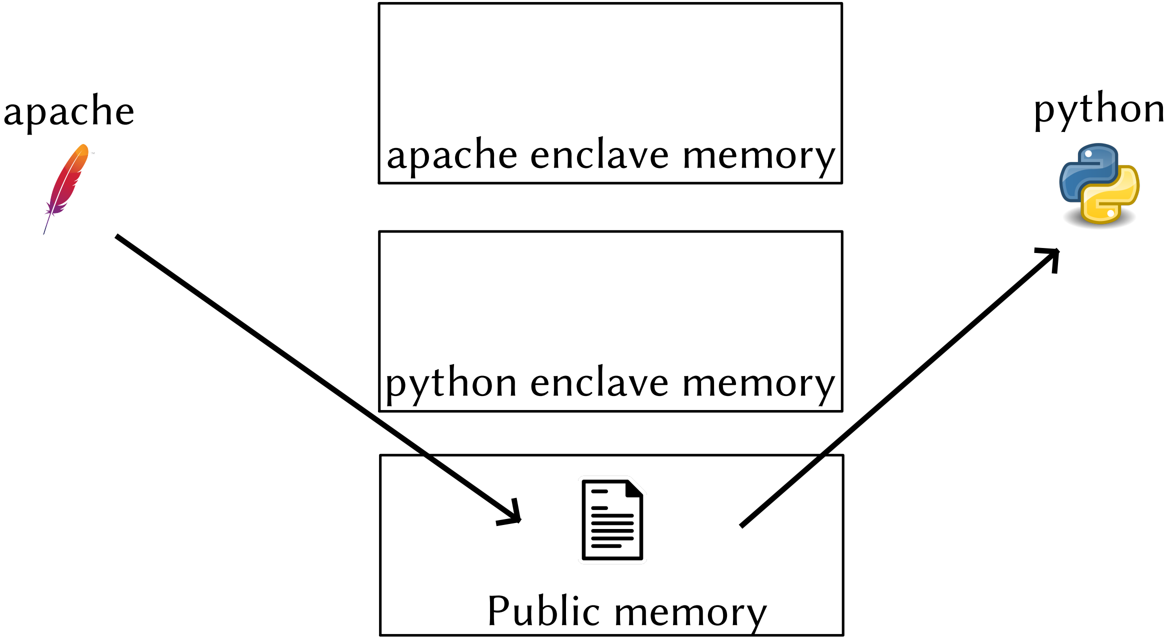
Problems due to Spatial Isolation

Limited in data sharing expressiveness



Problems due to Spatial Isolation

Limited in data sharing expressiveness



apache

apache enclave memory

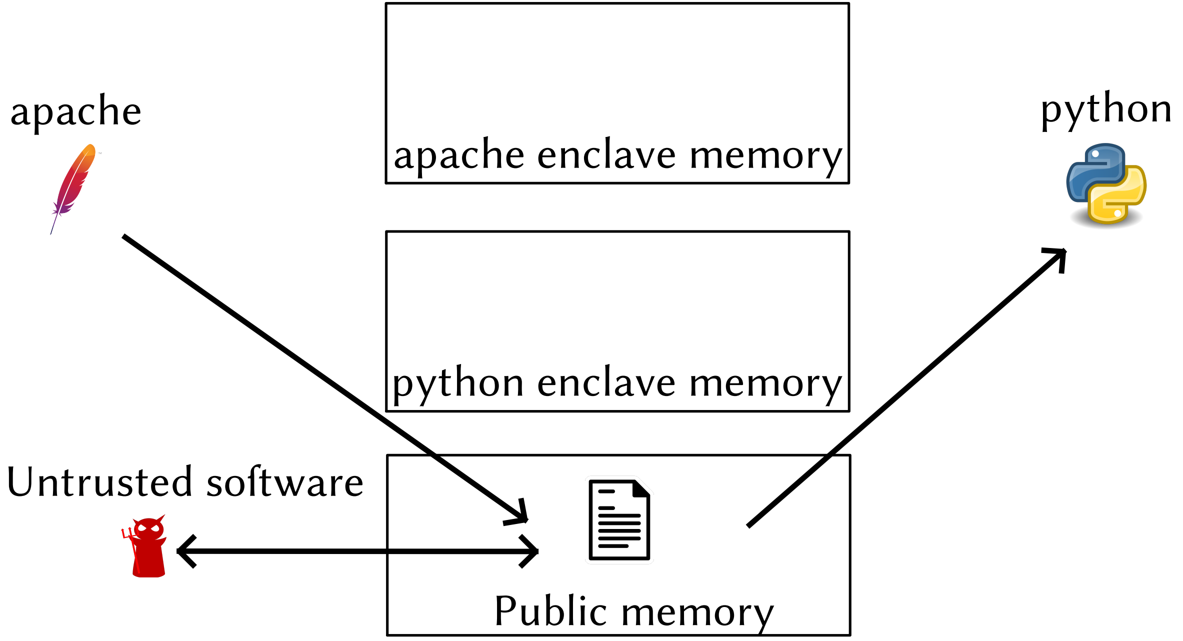
python enclave memory

Public memory

python

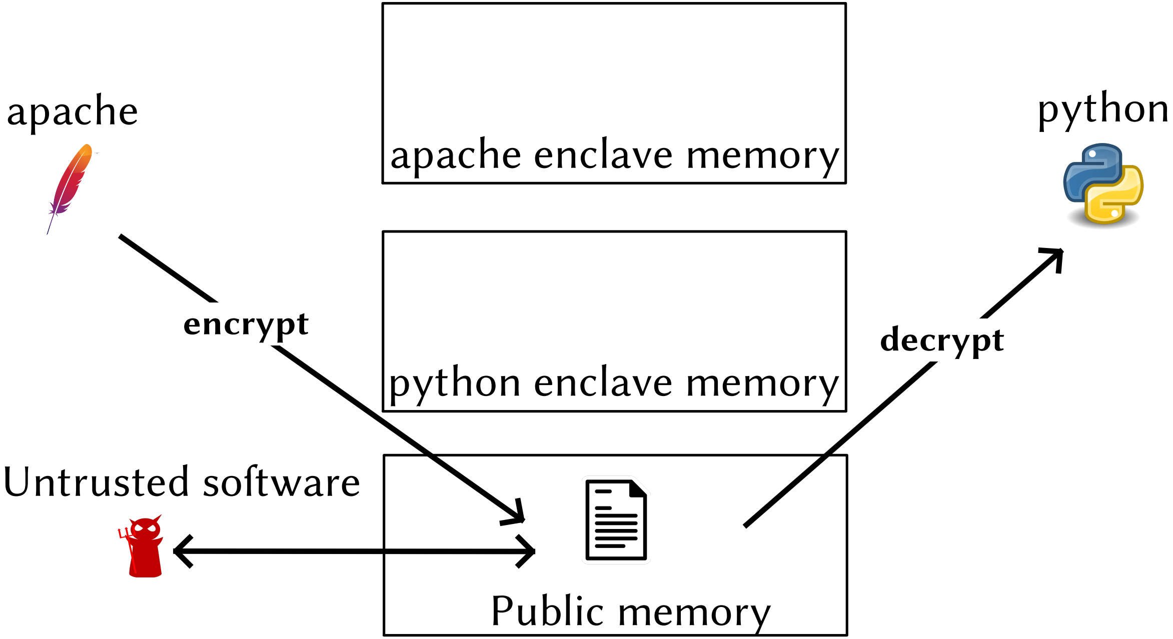
Problems due to Spatial Isolation

Limited in data sharing expressiveness



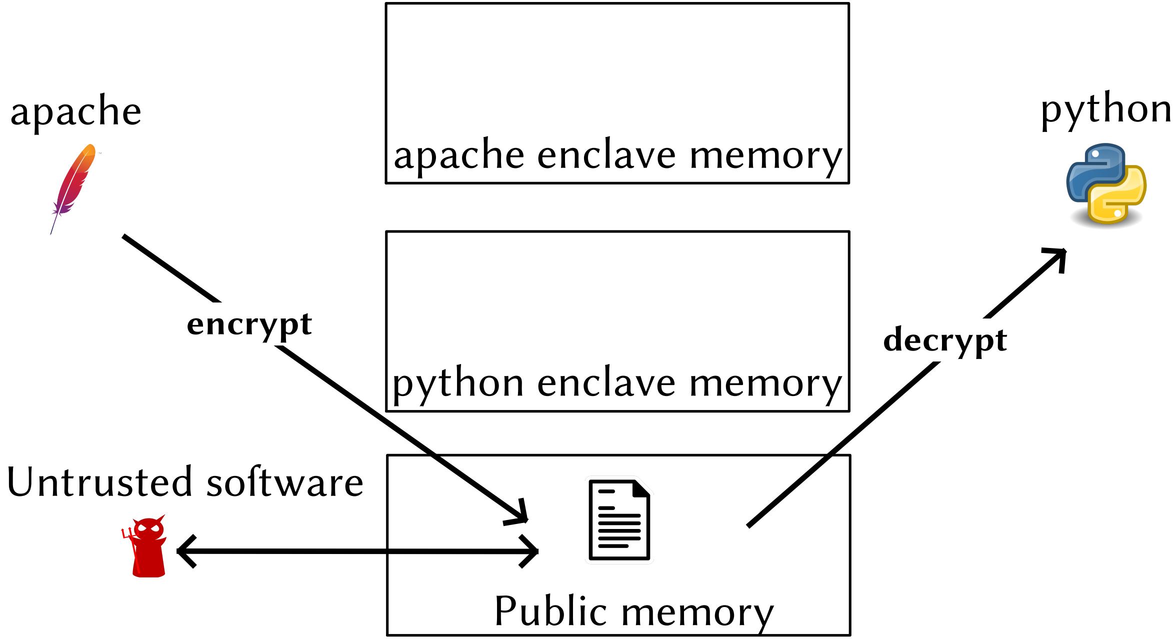
Problems due to Spatial Isolation

Limited in data sharing expressiveness



Problems due to Spatial Isolation

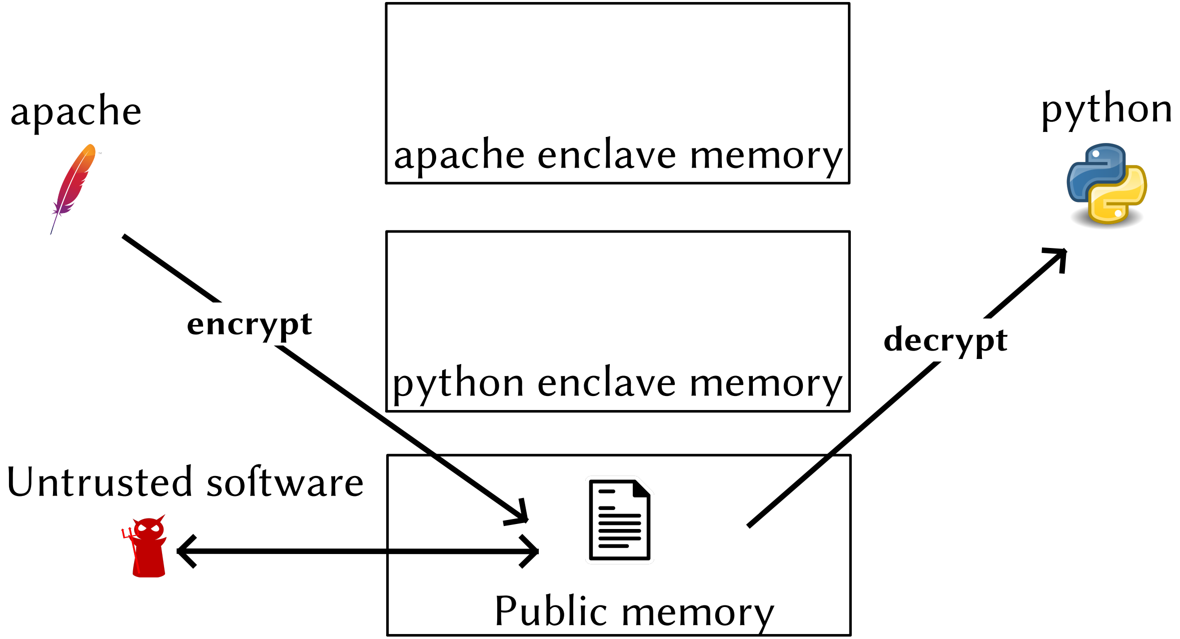
Limited in data sharing expressiveness



2 extra copies + encryption/decryption

Problems due to Spatial Isolation

Limited in data sharing expressiveness



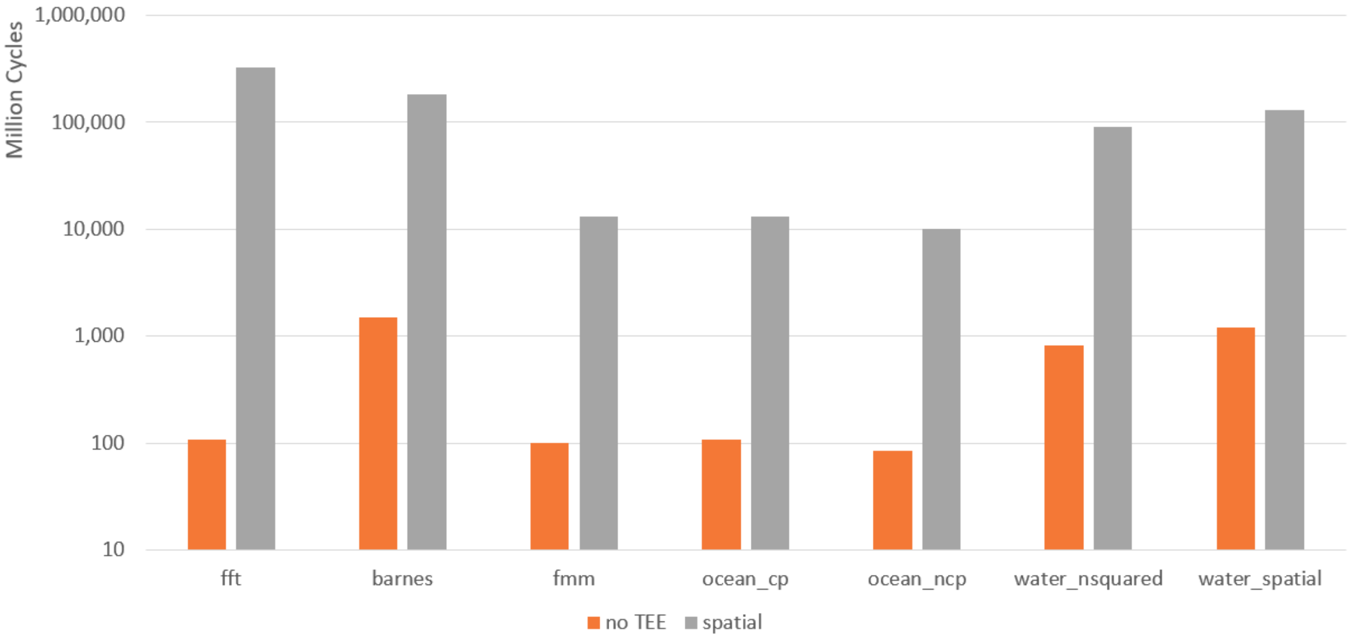
Client-server

2 extra copies + encryption/decryption

Similar in other patterns:

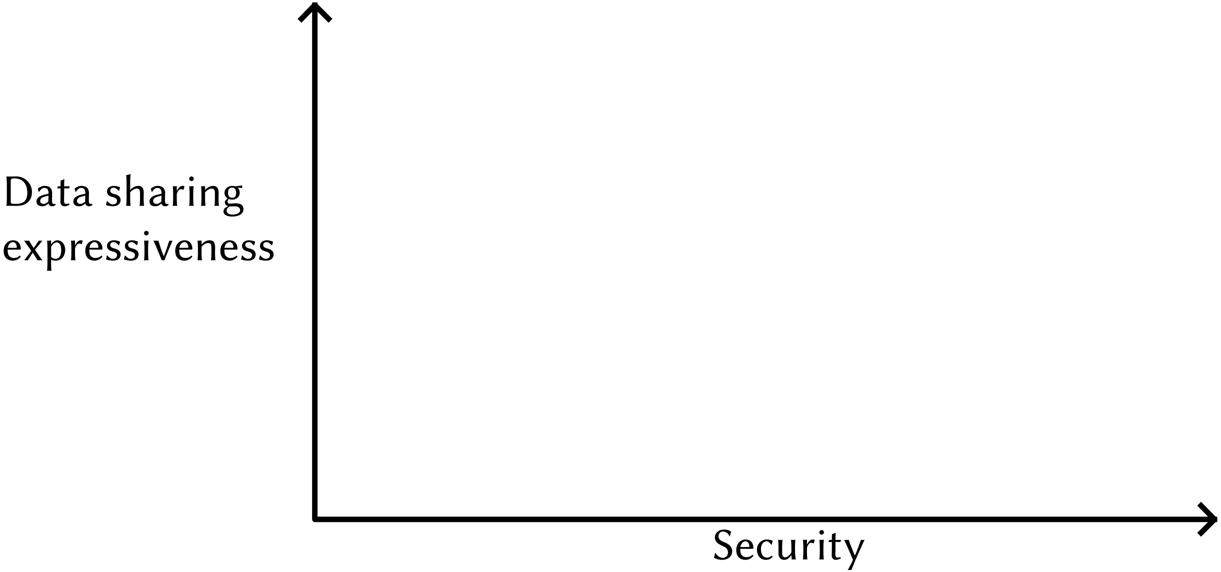
- Producer-consumer
- Proxy

Huge Overhead of Spatial Isolation

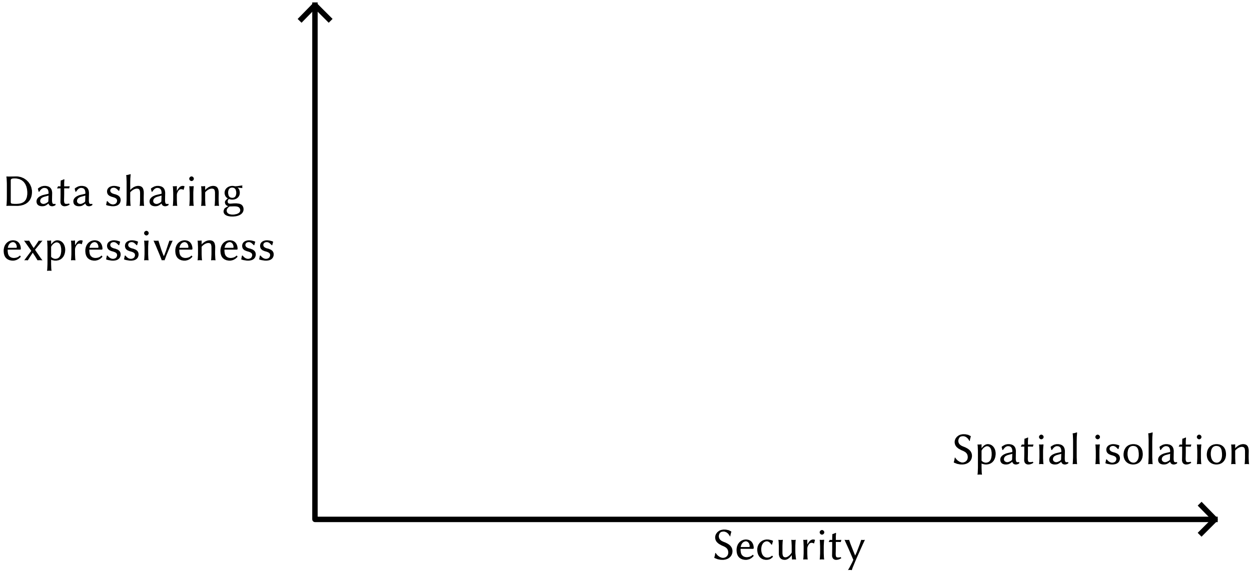


Contributions

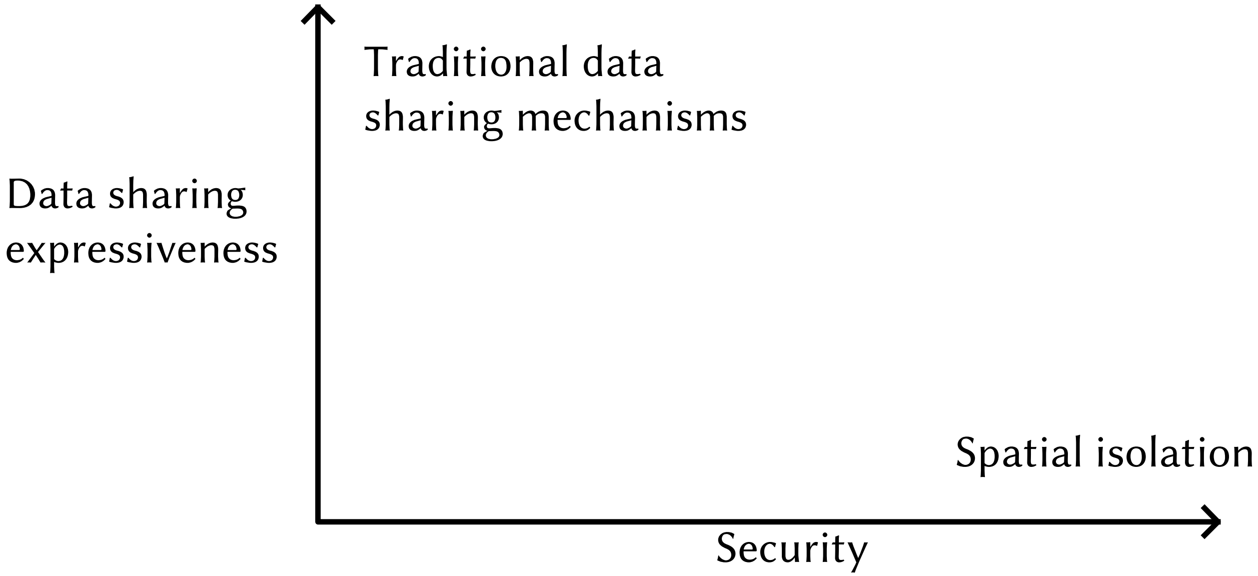
Contributions



Contributions



Contributions



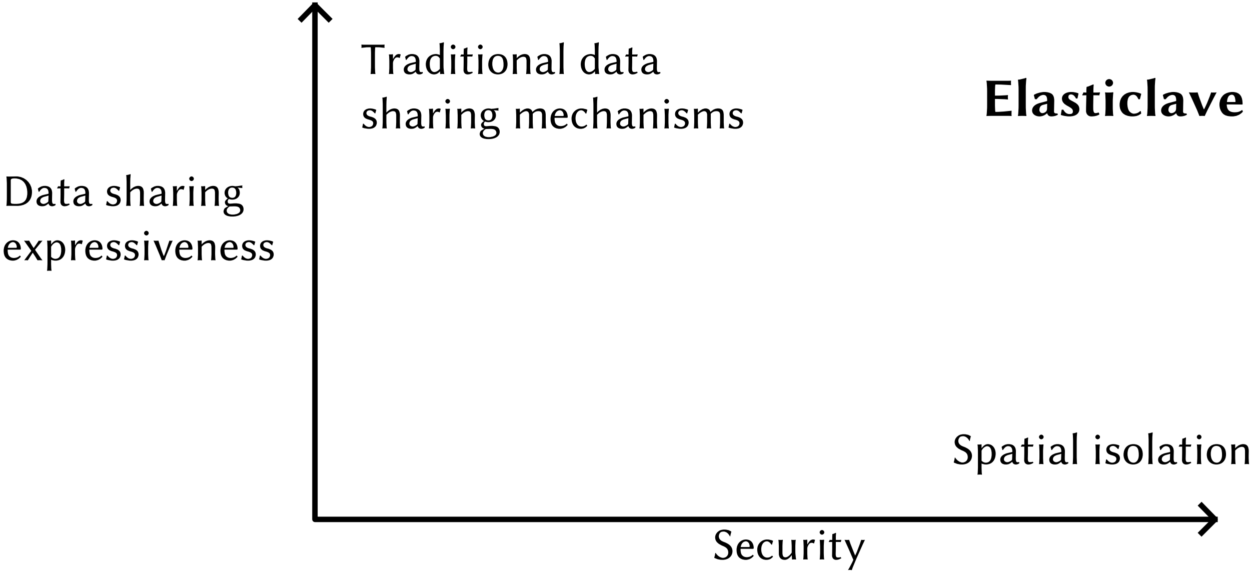
Traditional data sharing mechanisms

Data sharing expressiveness

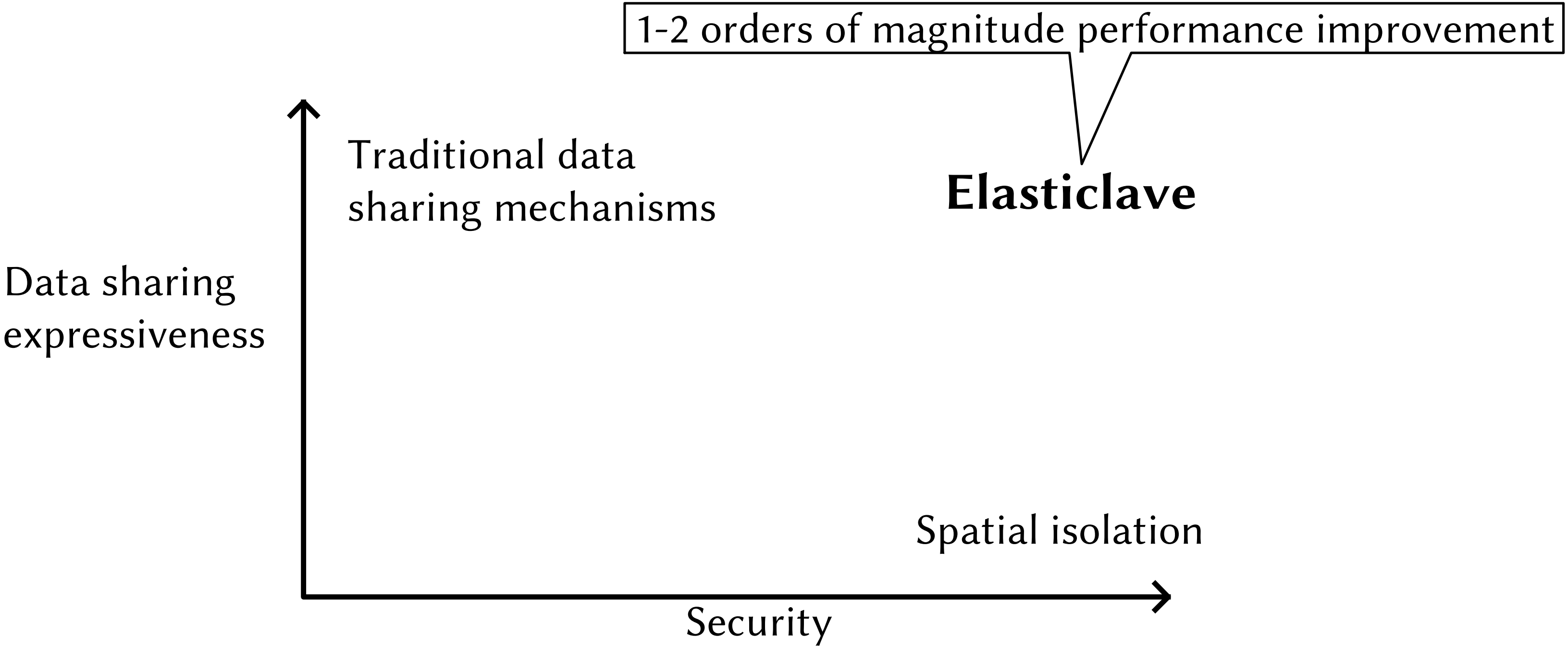
Spatial isolation

Security

Contributions


Traditional data sharing mechanisms
Elasticlave
Data sharing expressiveness
Spatial isolation
Security

Contributions



1-2 orders of magnitude performance improvement

Traditional data sharing mechanisms

Elasticlave

Data sharing expressiveness

Spatial isolation

Security

Threat Model

- Malicious OS

Threat Model

- Malicious OS
- Mutually distrusting applications (compromised during runtime)

Threat Model

- Malicious OS
- Mutually distrusting applications (compromised during runtime)
- DoS attacks are out of scope

Idea: Temporal Isolation

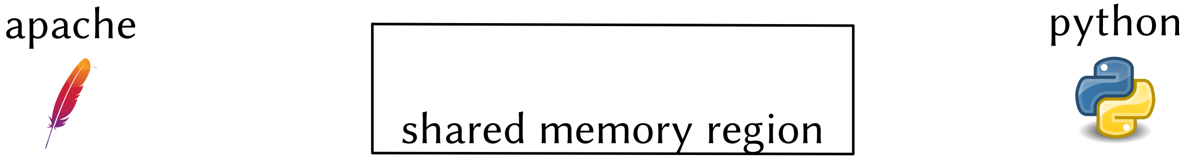
Spatial isolation: memory region is either always private or always public

Temporal isolation: different enclaves may access memory region at different times

Idea: Temporal Isolation

Spatial isolation: memory region is either always private or always public

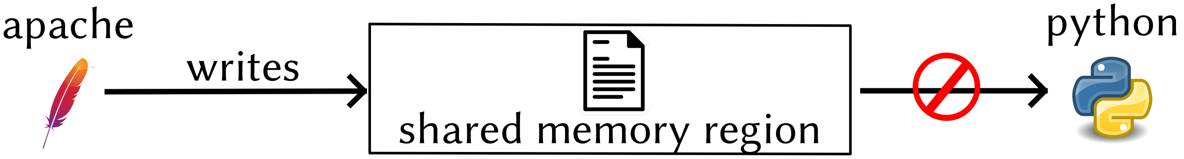
Temporal isolation: different enclaves may access memory region at different times



Idea: Temporal Isolation

Spatial isolation: memory region is either always private or always public

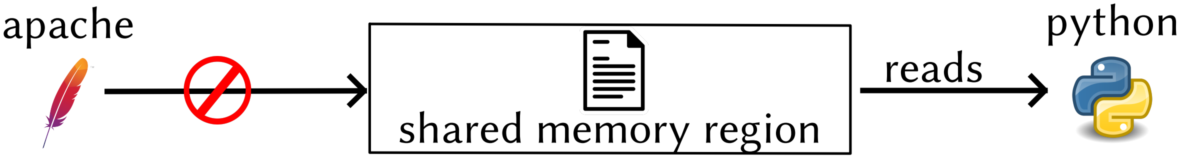
Temporal isolation: different enclaves may access memory region at different times



Idea: Temporal Isolation

Spatial isolation: memory region is either always private or always public

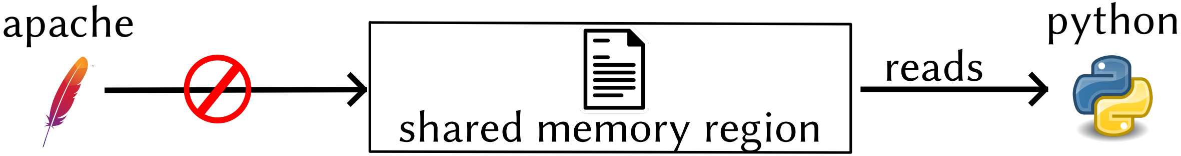
Temporal isolation: different enclaves may access memory region at different times



Idea: Temporal Isolation

Spatial isolation: memory region is either always private or always public

Temporal isolation: different enclaves may access memory region at different times



No extra copies or encryption/decryption

Temporal Isolation Challenge I

Temporal Isolation Challenge I

Each memory region has exactly one enclave as its owner

Temporal Isolation Challenge I

Each memory region has exactly one enclave as its owner

Only owner can access the memory region

Temporal Isolation Challenge I

Each memory region has exactly one enclave as its owner

Only owner can access the memory region

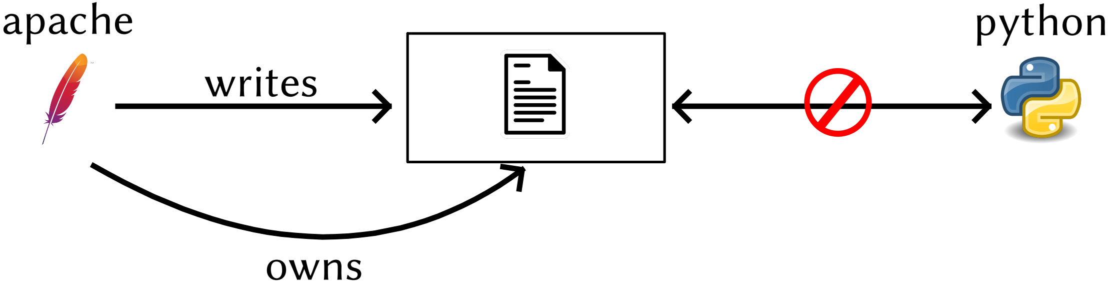
Owner can pass ownership to others

Temporal Isolation Challenge I

Each memory region has exactly one enclave as its owner

Only owner can access the memory region

Owner can pass ownership to others

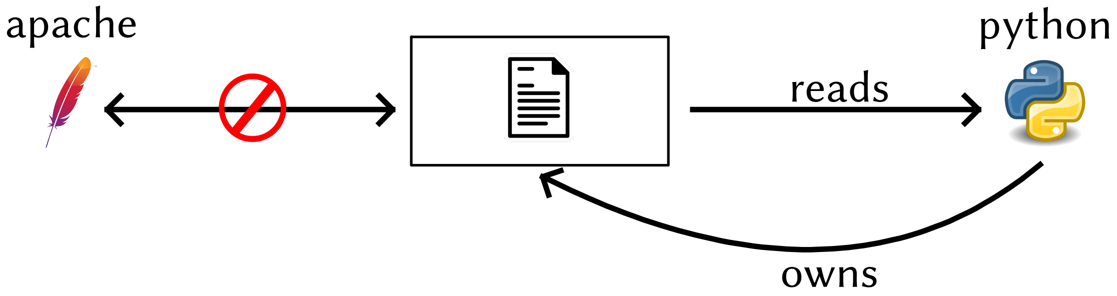


Temporal Isolation Challenge I

Each memory region has exactly one enclave as its owner

Only owner can access the memory region

Owner can pass ownership to others

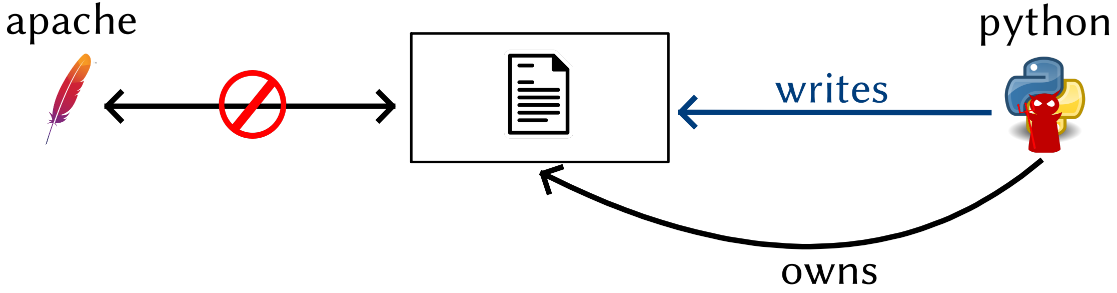


Temporal Isolation Challenge I

Each memory region has exactly one enclave as its owner

Only owner can access the memory region

Owner can pass ownership to others

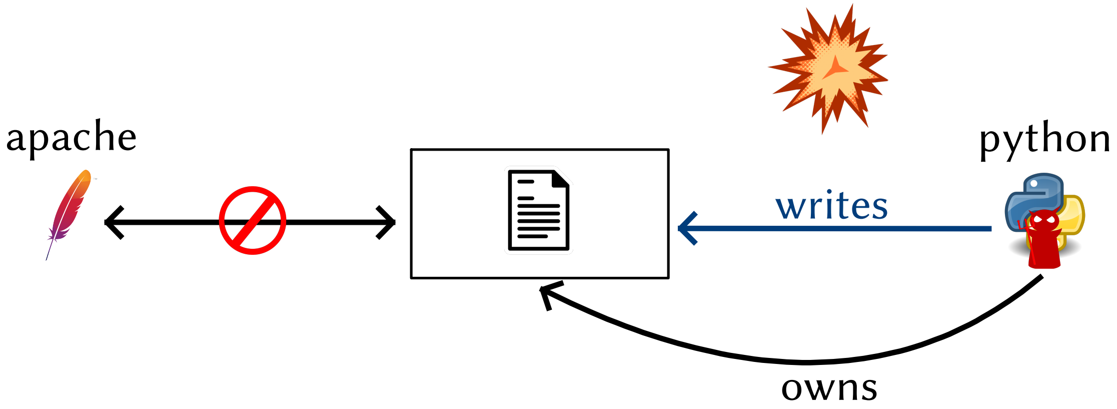


Temporal Isolation Challenge I

Each memory region has exactly one enclave as its owner

Only owner can access the memory region

Owner can pass ownership to others

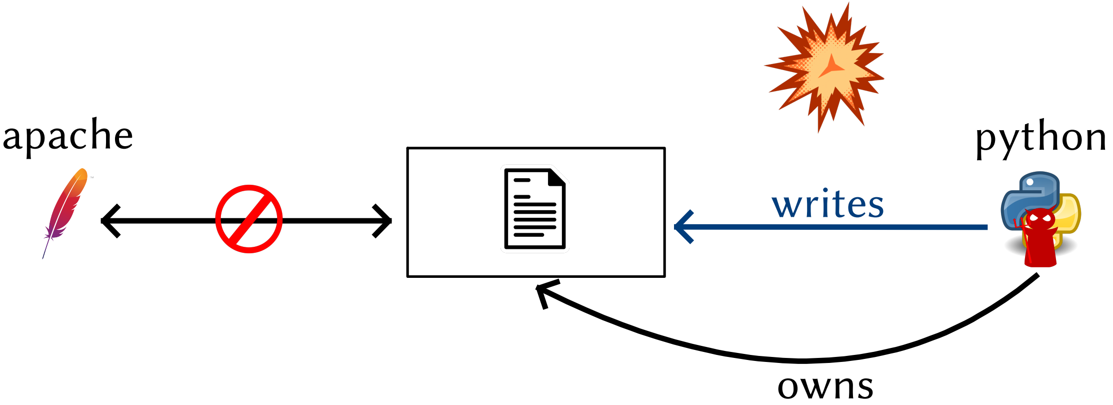


Temporal Isolation Challenge I

Each memory region has exactly one enclave as its owner

Only owner can access the memory region

Owner can pass ownership to others



Problem: Sharer has no control over how data is accessed after sharing

How does Elasticlave solve this?

Elasticlave Design: Maximum Permissions

Elasticlave Design: Maximum Permissions

~~Transferring ownership~~ fixed owner

Elasticlave Design: Maximum Permissions

~~Transferring ownership~~ fixed owner

Owner sets *maximum permissions* for other enclaves

Elasticlave Design: Maximum Permissions

~~Transferring ownership~~ fixed owner

Owner sets *maximum permissions* for other enclaves

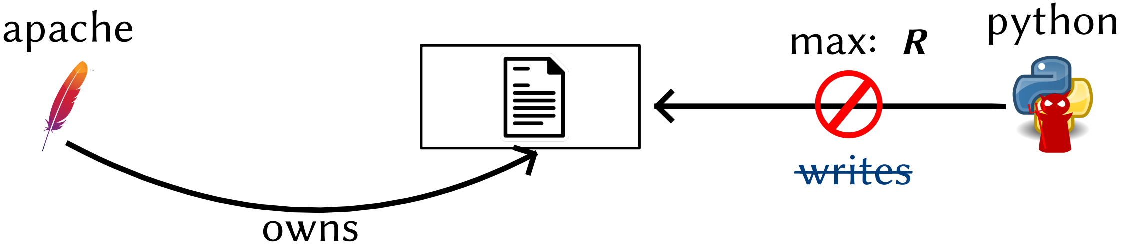
Maximum permissions limit how other enclaves access the memory region

Elasticlave Design: Maximum Permissions

~~Transferring ownership~~ fixed owner

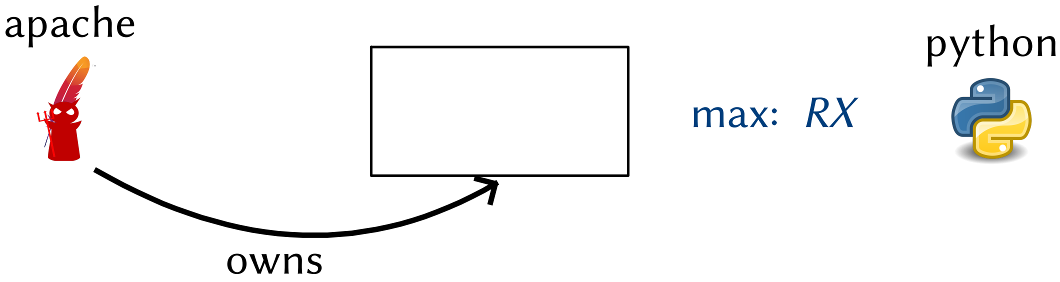
Owner sets *maximum permissions* for other enclaves

Maximum permissions limit how other enclaves access the memory region



Temporal Isolation Challenge II

Temporal Isolation Challenge II



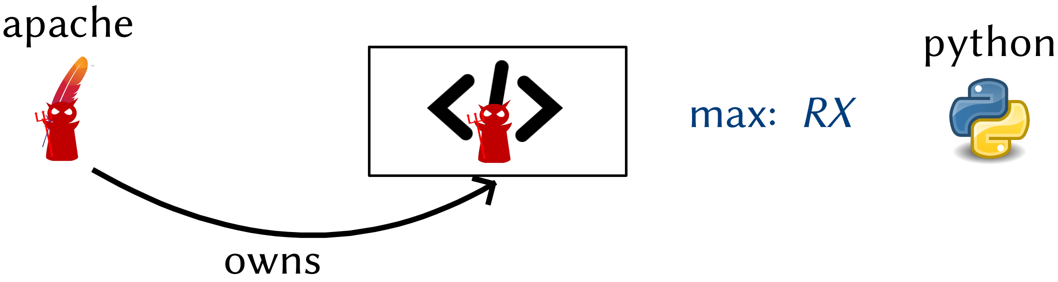
apache

owns

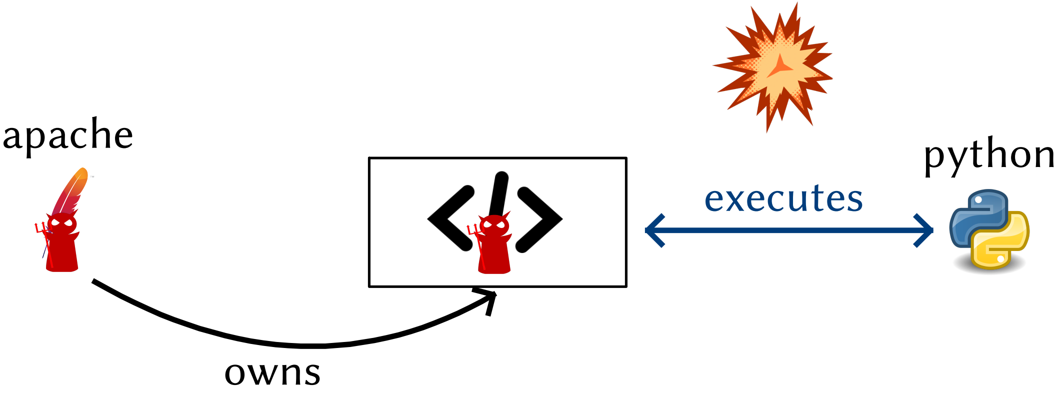
max: *RX*

python

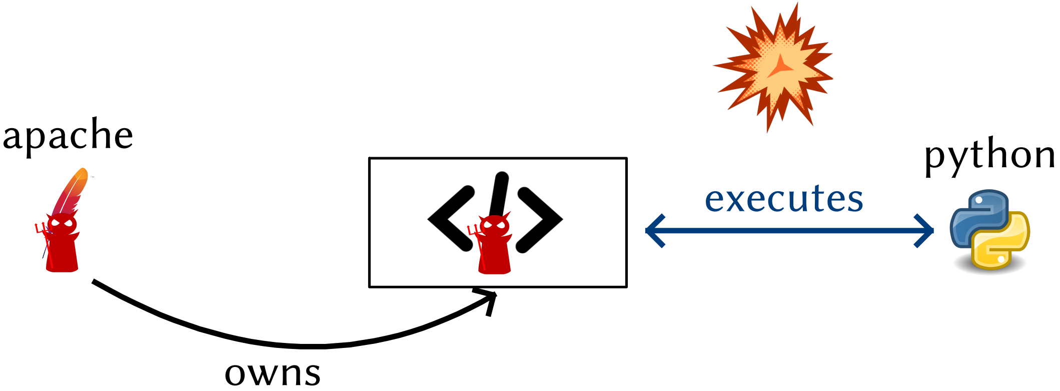
Temporal Isolation Challenge II



Temporal Isolation Challenge II



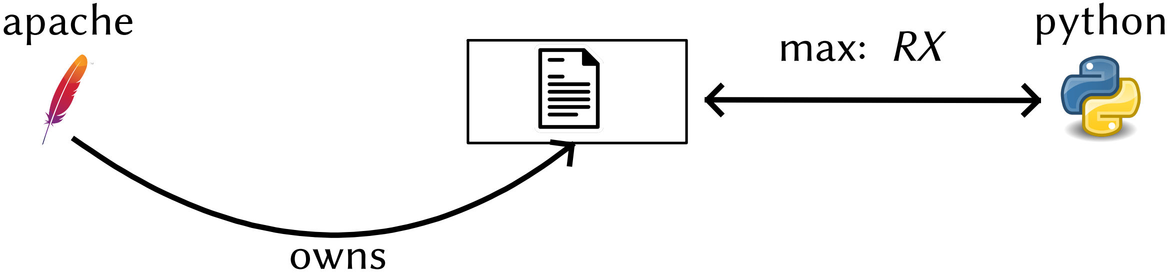
Temporal Isolation Challenge II



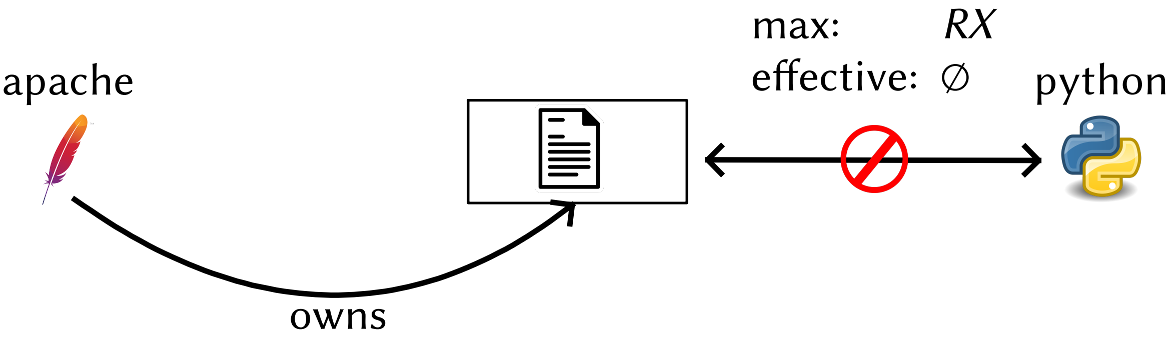
Problem: Accessors cannot enforce their own memory protection permissions

Elasticlave Design: Effective Permissions

Elasticlave Design: Effective Permissions

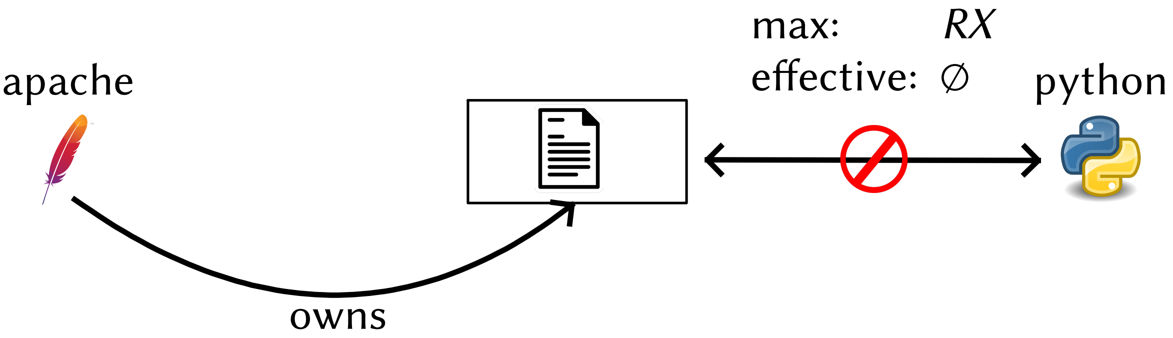


Elasticlave Design: Effective Permissions



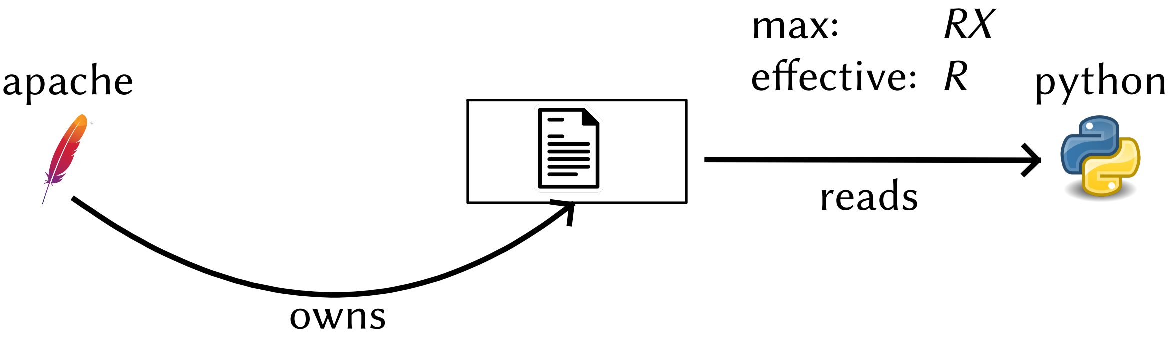
Elasticlave Design: Effective Permissions

Each enclave can request hardware to change *its own* effective permissions dynamically



Elasticlave Design: Effective Permissions

Each enclave can request hardware to change *its own* effective permissions dynamically



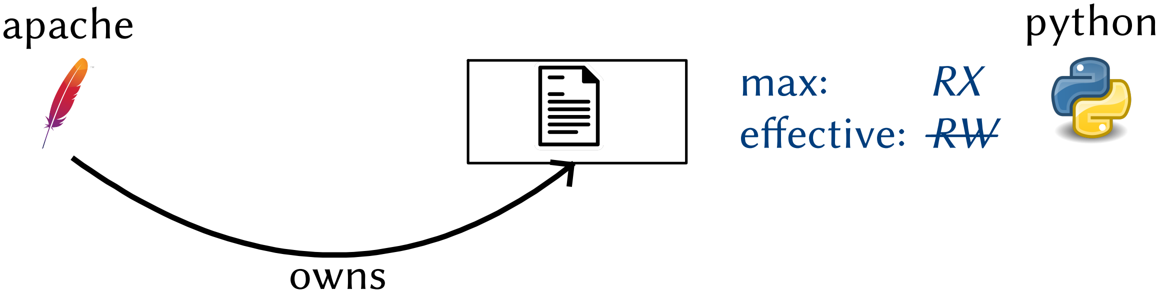
Connecting Maximum and Effective Permissions

Connecting Maximum and Effective Permissions

For any (enclave, memory region) pair,
effective permissions ≤ maximum permissions

Connecting Maximum and Effective Permissions

For any (enclave, memory region) pair,
effective permissions ≤ maximum permissions



apache

python

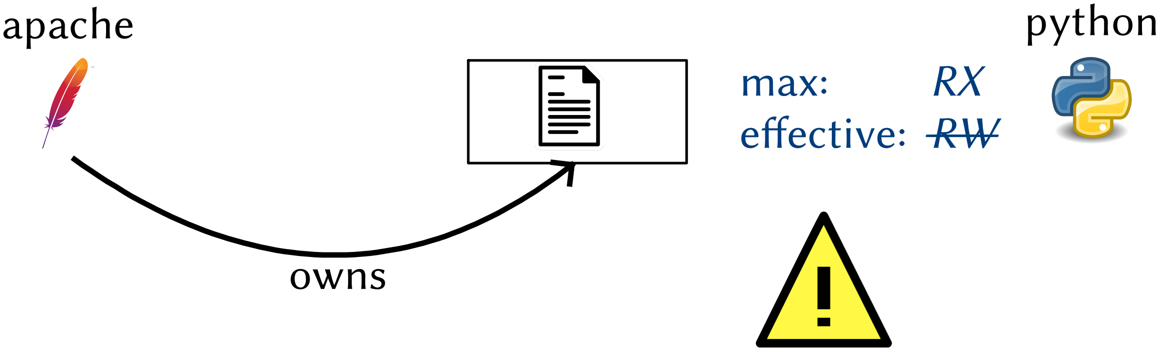
max: *RX*

effective: ~~*RW*~~

owns

Connecting Maximum and Effective Permissions

For any (enclave, memory region) pair,
effective permissions ≤ maximum permissions



apache

owns

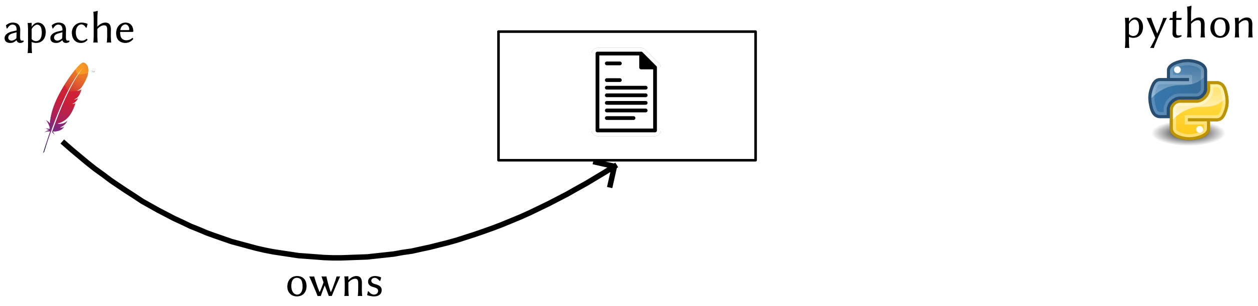
max: *RX*

effective: ~~*RW*~~

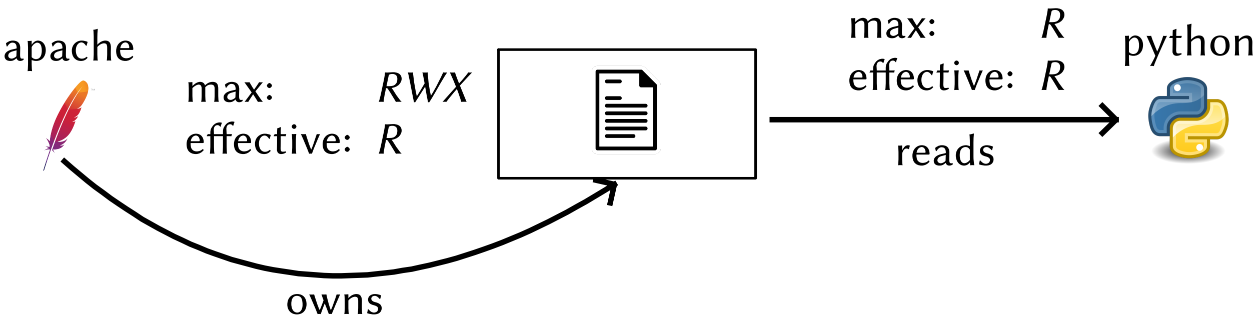
python

Exception

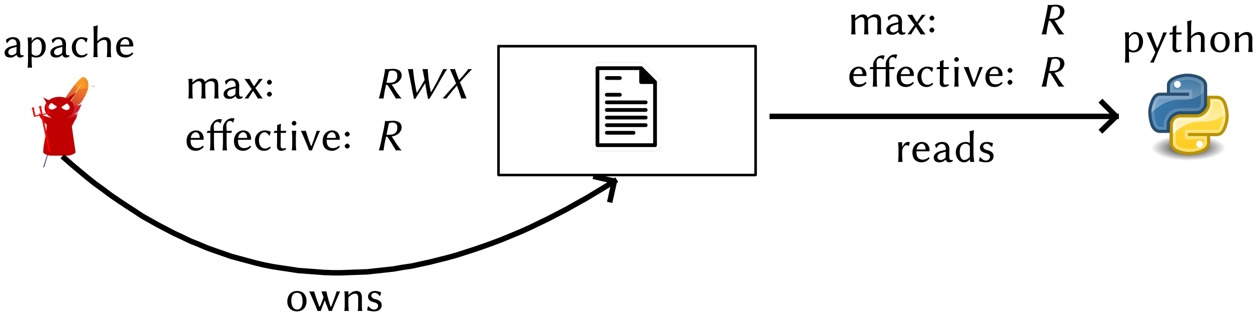
Temporal Isolation Challenge III



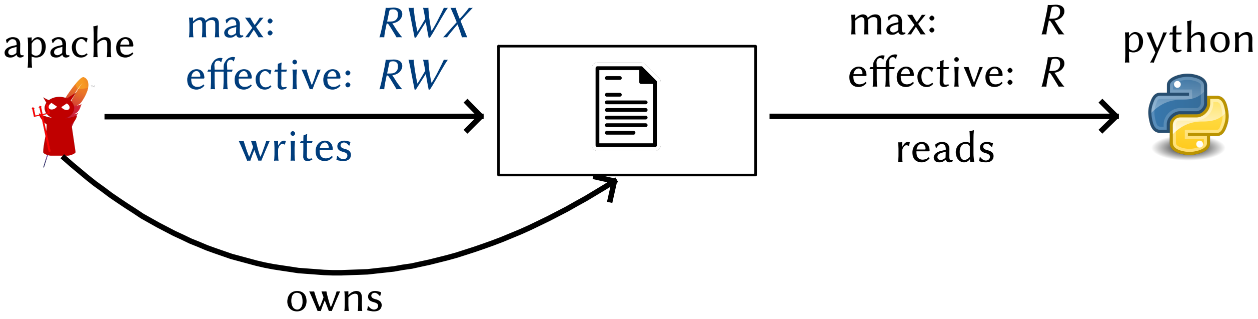
Temporal Isolation Challenge III



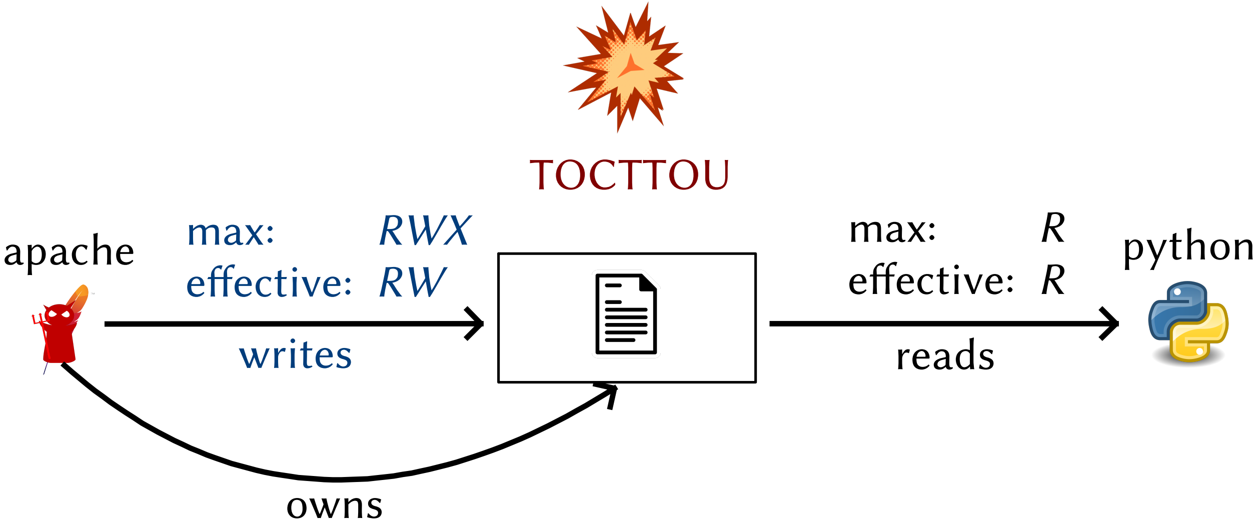
Temporal Isolation Challenge III



Temporal Isolation Challenge III



Temporal Isolation Challenge III



TOCTTOU

apache

max: *RWX*

effective: *RW*

writes

owns

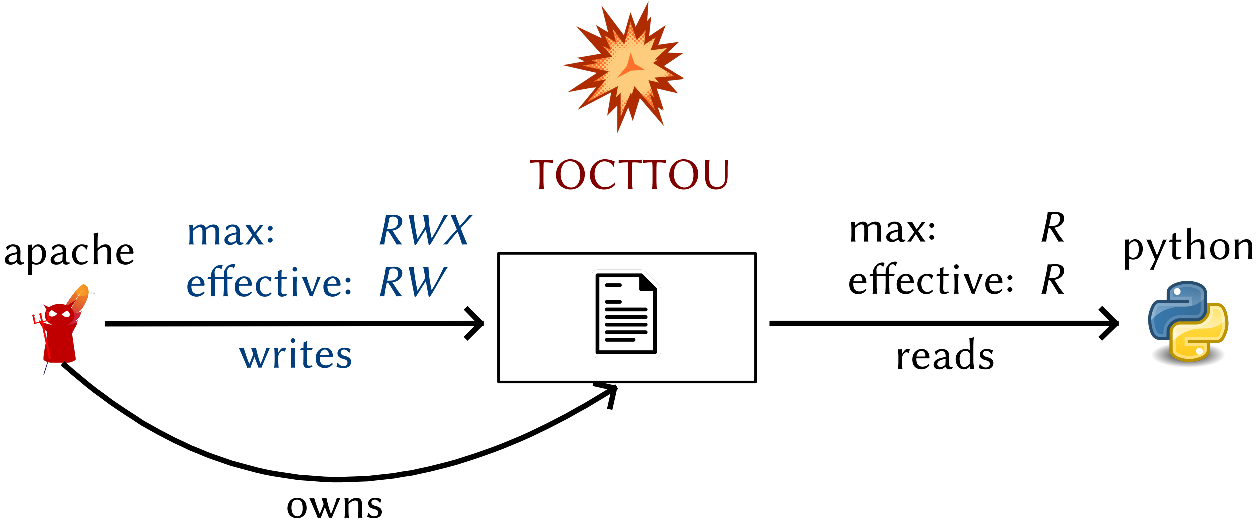
max: *R*

effective: *R*

reads

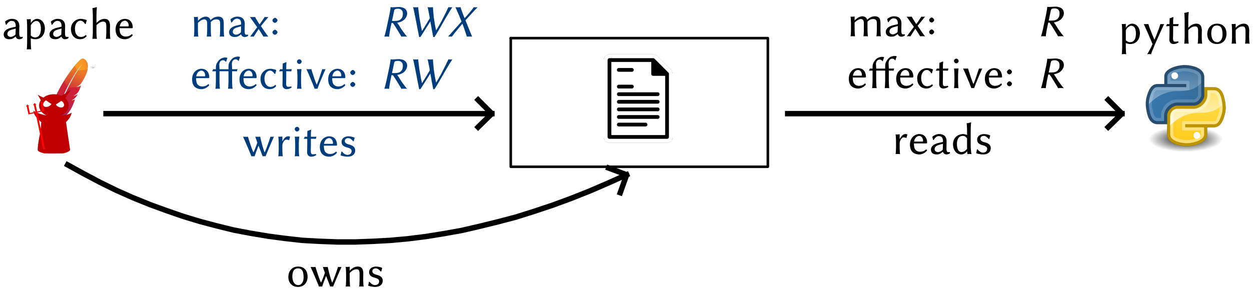
python

Temporal Isolation Challenge III

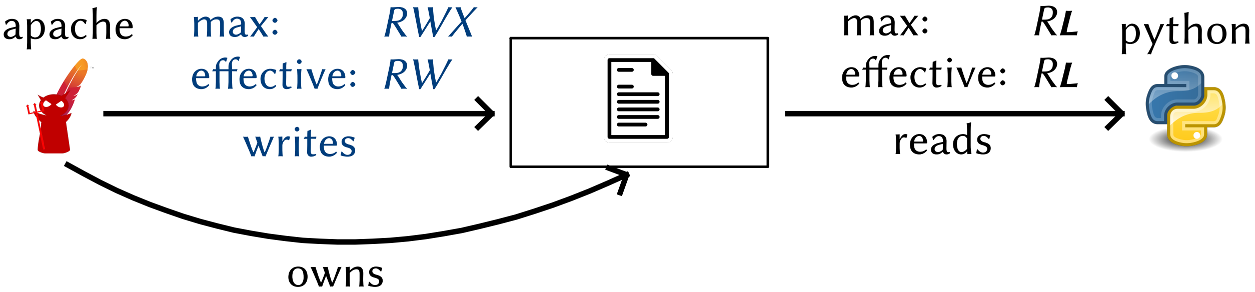


Problem: No mechanism for synchronization

Elasticlave: Lock Bit



Elasticlave: Lock Bit



apache

max: *RWX*

effective: *RW*

writes

owns

max: *R***L**

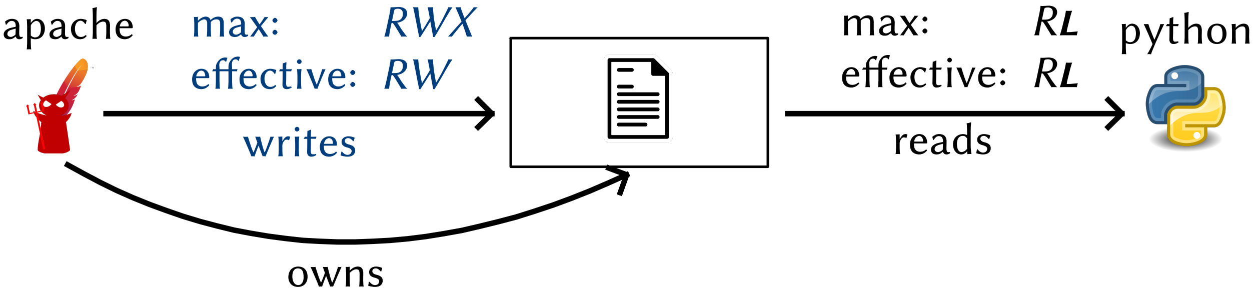
effective: *R***L**

reads

python

Elasticlave: Lock Bit

When held in effective permissions:
exclusive access guaranteed



apache

max: *RWX*
effective: *RW*

writes

owns

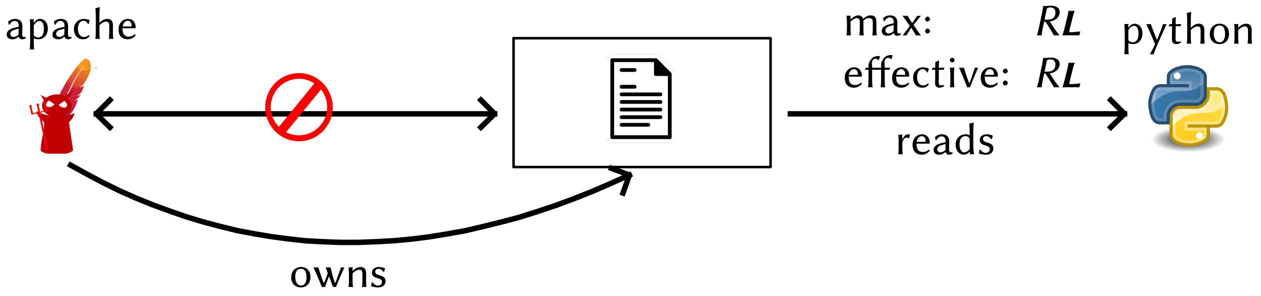
max: *R***L**
effective: *R***L**

reads

python

Elasticlave: Lock Bit

When held in effective permissions:
exclusive access guaranteed



Elasticlave Summary

Three elements:

- Maximum permissions

Elasticlave Summary

Three elements:

- Maximum permissions
- Effective permissions (≤ maximum permissions)

Elasticlave Summary

Three elements:

- Maximum permissions
- Effective permissions (≤ maximum permissions)
- Synchronization: lock bit

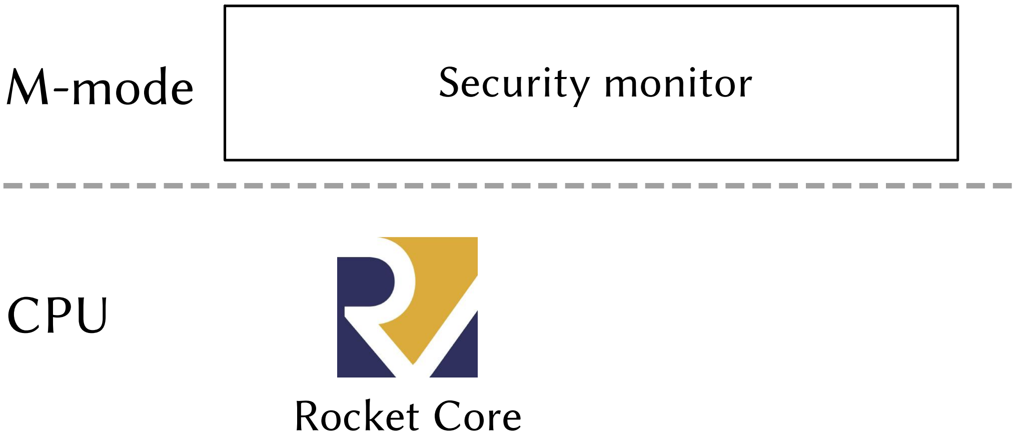
Implementation

Implementation

CPU

Rocket Core

Implementation



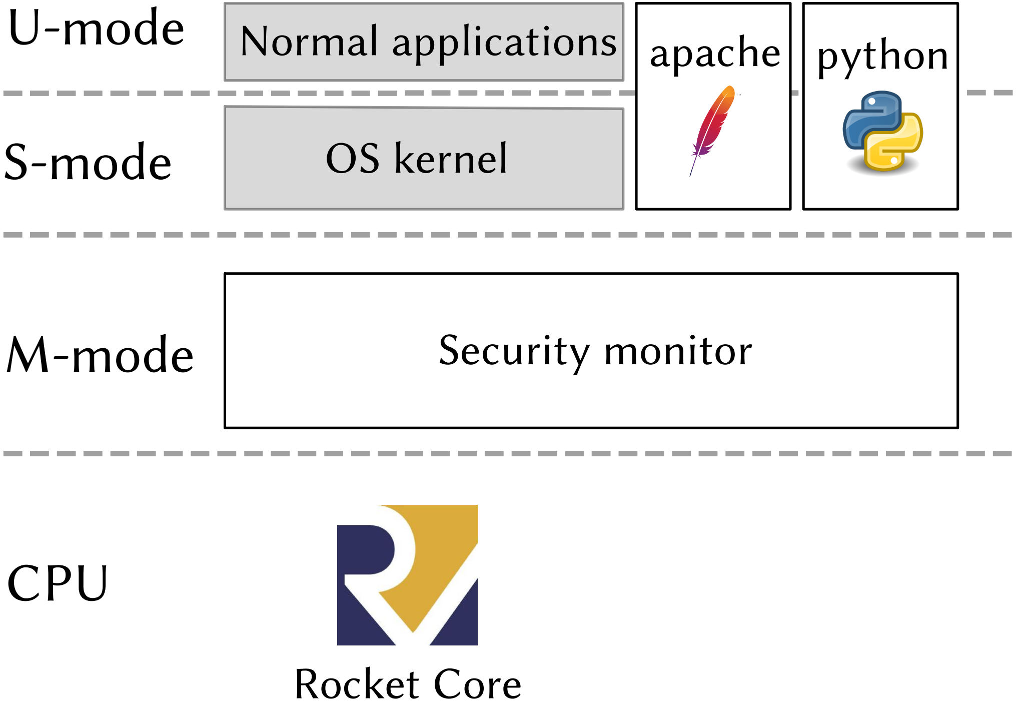
M-mode

Security monitor

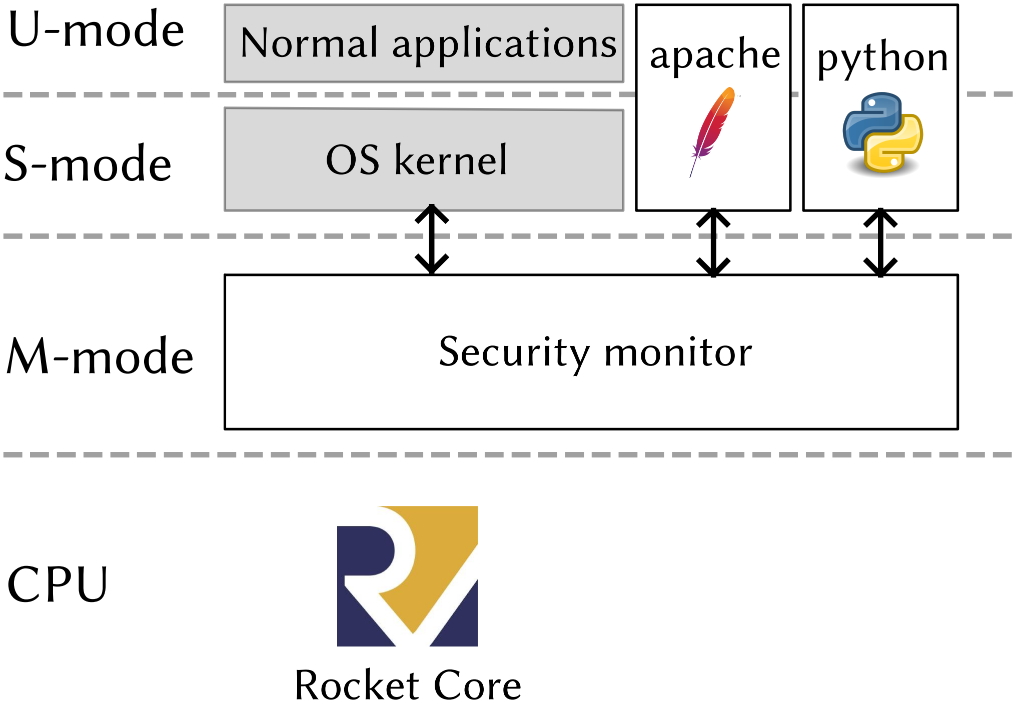
CPU

Rocket Core

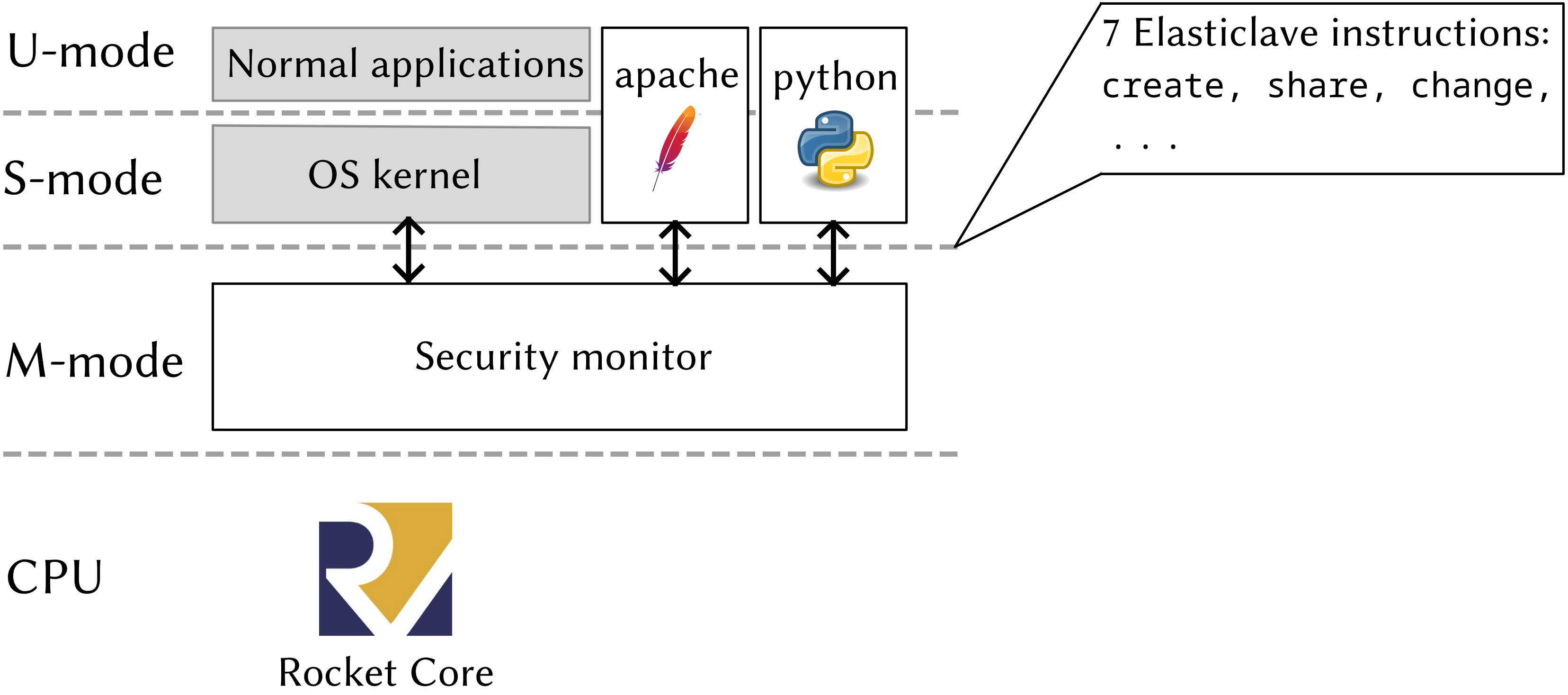
Implementation



Implementation

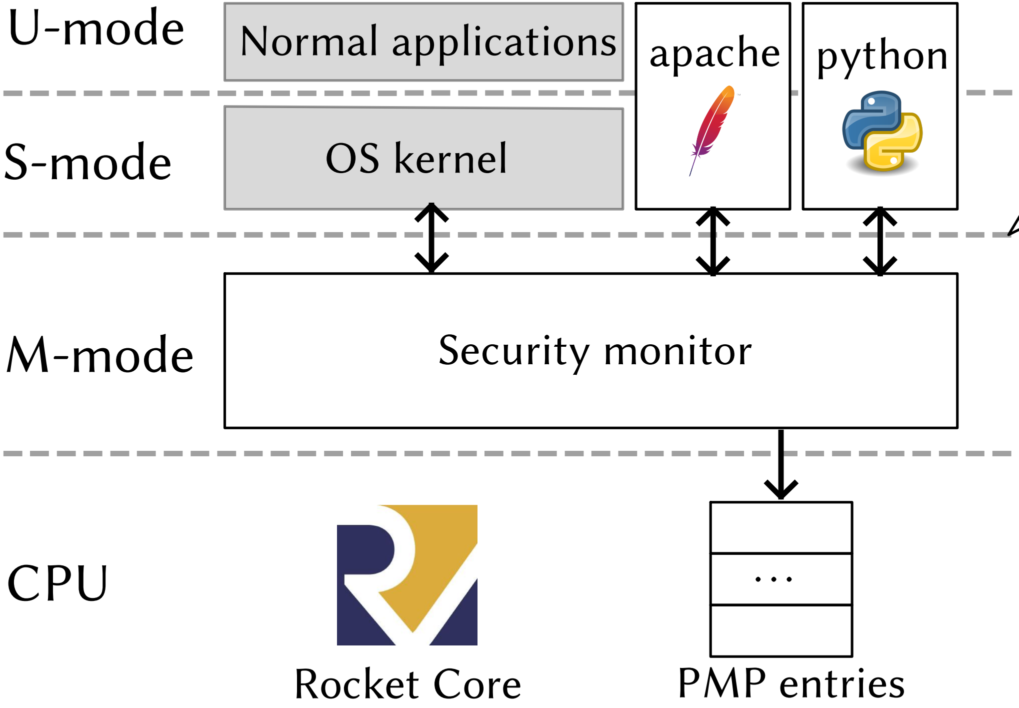


Implementation



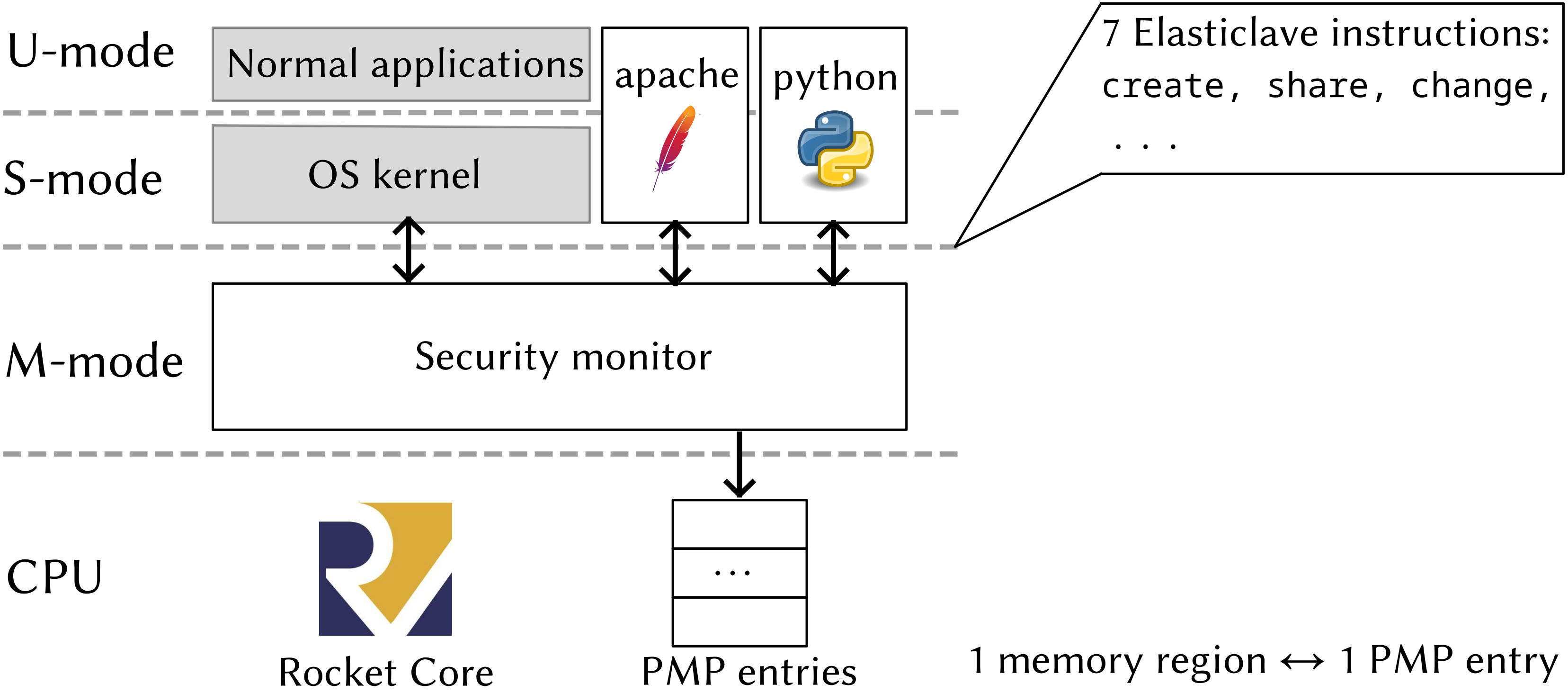
7 Elasticlave instructions: `create, share, change, ...`

Implementation



7 Elasticlave instructions:
`create, share, change, ...`

Implementation



U-mode

Normal applications

apache

python

S-mode

OS kernel

M-mode

Security monitor

CPU

Rocket Core

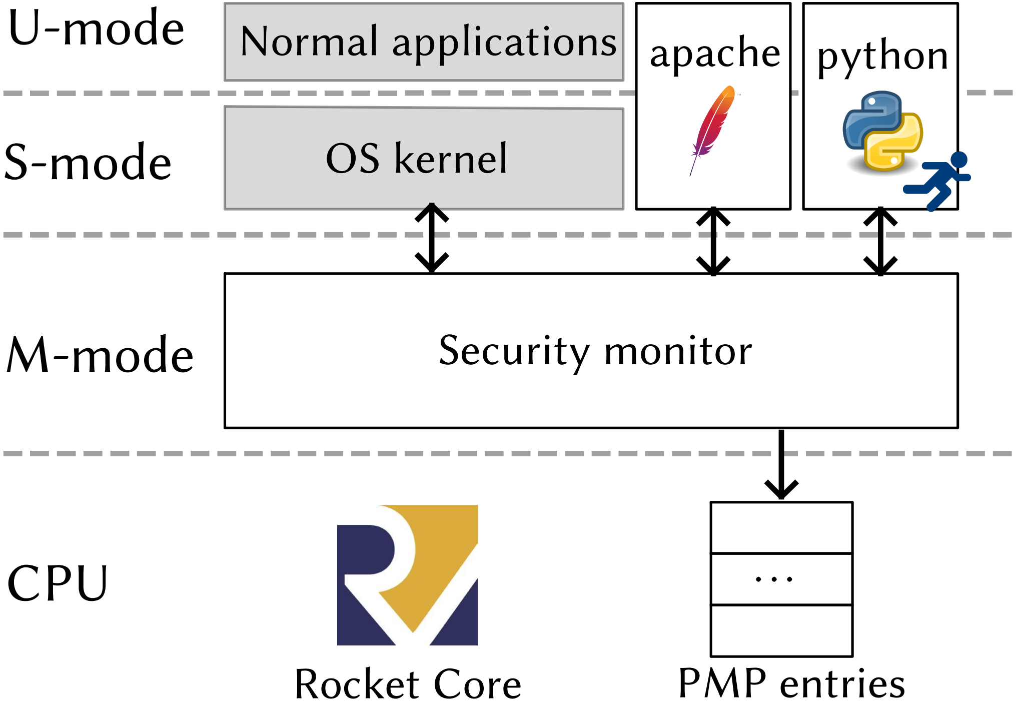
PMP entries

. . .

7 Elasticlave instructions:
`create, share, change,`
`. . .`

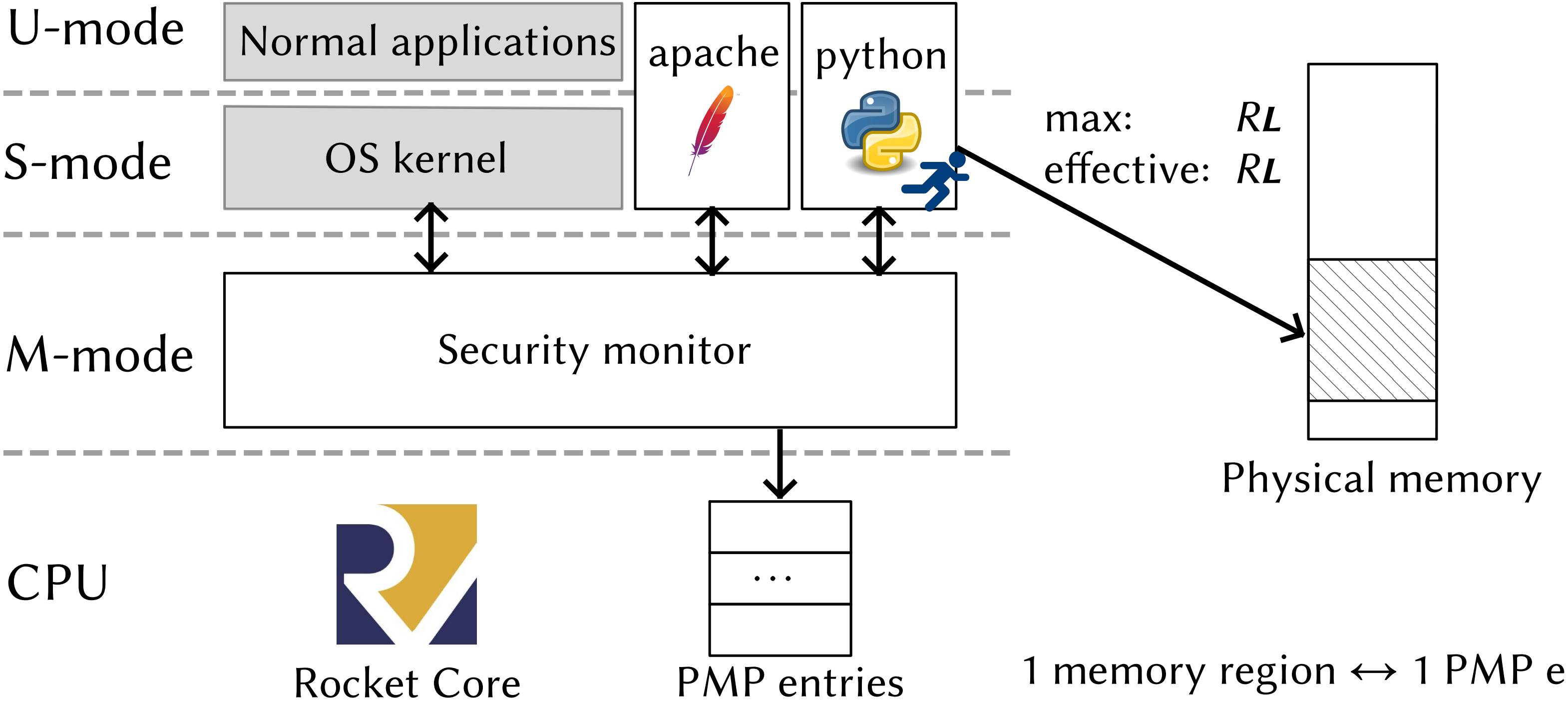
1 memory region ↔ 1 PMP entry

Implementation



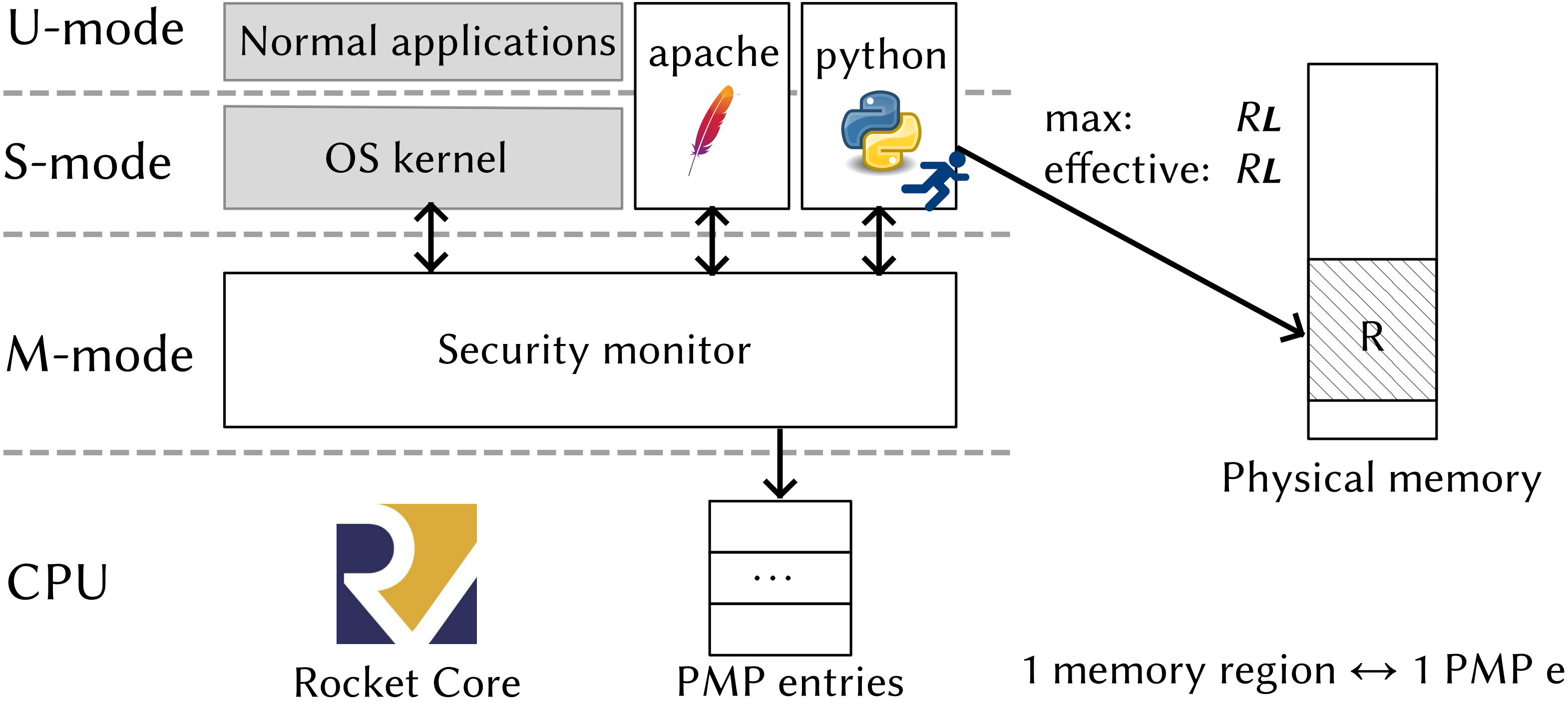
1 memory region ↔ 1 PMP entry

Implementation



1 memory region ↔ 1 PMP entry

Implementation



1 memory region ↔ 1 PMP entry

Evaluations

Evaluation question: Performance of Elasticlave compared to spatial isolation

Evaluations

Evaluation question: Performance of Elasticlave compared to spatial isolation

Benchmarks:

Evaluations

Evaluation question: Performance of Elasticlave compared to spatial isolation

Benchmarks:

- Handcrafted microbenchmarks for data sharing patterns

Evaluations

Evaluation question: Performance of Elasticlave compared to spatial isolation

Benchmarks:

- Handcrafted microbenchmarks for data sharing patterns
- Standard benchmarks: IOZone (I/O), SPLASH-2 (sharing)

Evaluations

Evaluation question: Performance of Elasticlave compared to spatial isolation

Benchmarks:

- Handcrafted microbenchmarks for data sharing patterns
- Standard benchmarks: IOZone (I/O), SPLASH-2 (sharing)

Baselines:

Evaluations

Evaluation question: Performance of Elasticlave compared to spatial isolation

Benchmarks:

- Handcrafted microbenchmarks for data sharing patterns
- Standard benchmarks: IOZone (I/O), SPLASH-2 (sharing)

Baselines:

- Spatial isolation (Keystone)

Evaluations

Evaluation question: Performance of Elasticlave compared to spatial isolation

Benchmarks:

- Handcrafted microbenchmarks for data sharing patterns
- Standard benchmarks: IOZone (I/O), SPLASH-2 (sharing)

Baselines:

- Spatial isolation (Keystone)
- Native Linux execution

Evaluations

Evaluation question: Performance of Elasticlave compared to spatial isolation

Benchmarks:

- Handcrafted microbenchmarks for data sharing patterns
- Standard benchmarks: IOZone (I/O), SPLASH-2 (sharing)

Baselines:

- Spatial isolation (Keystone)
- Native Linux execution

Run on cycle-accurate FPGA-accelerated simulator (FireSim)

SPLASH-2 (sharing-intensive)

Two enclaves performing parallel computation

SPLASH-2 (sharing-intensive)

Two enclaves performing parallel computation

Elasticlave: memory region accessible to both enclaves

SPLASH-2 (sharing-intensive)

Two enclaves performing parallel computation

Elasticlave: memory region accessible to both enclaves

Spatial isolation: passing data through extra copies and encryption/decryption

SPLASH-2 (sharing-intensive)

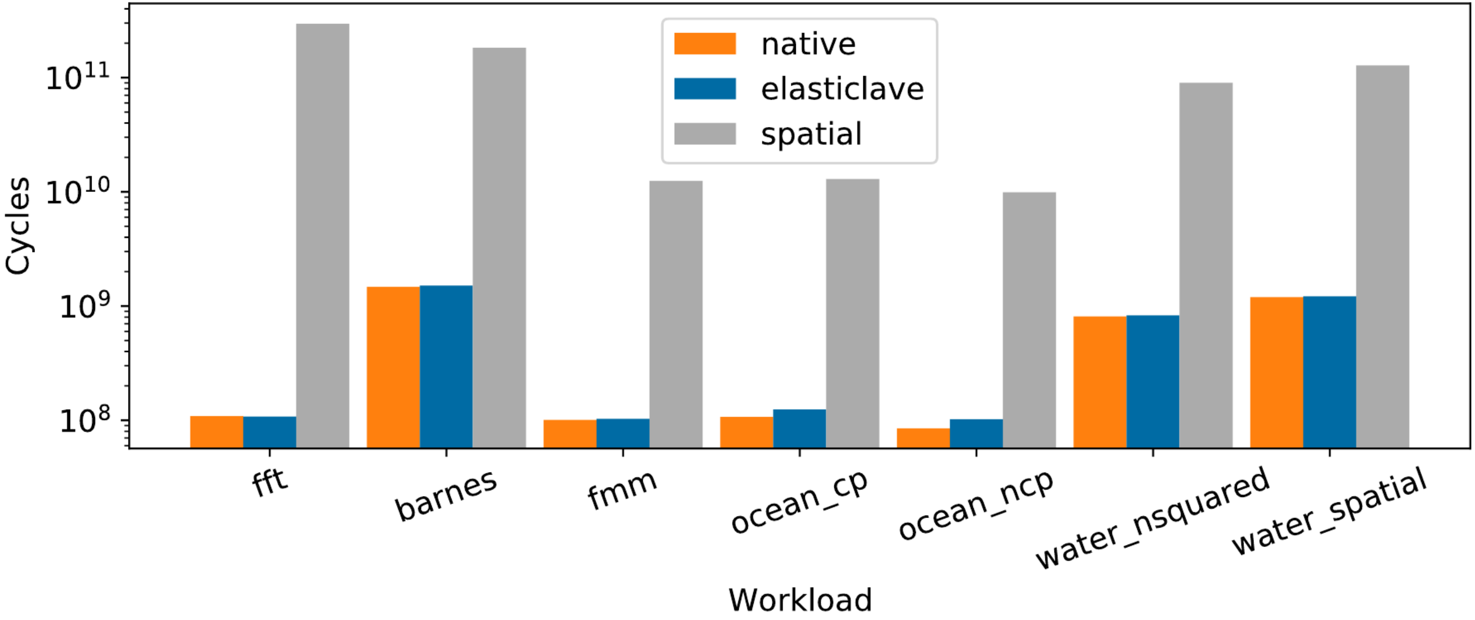
Two enclaves performing parallel computation

Elasticlave: memory region accessible to both enclaves

Spatial isolation: passing data through extra copies and encryption/decryption

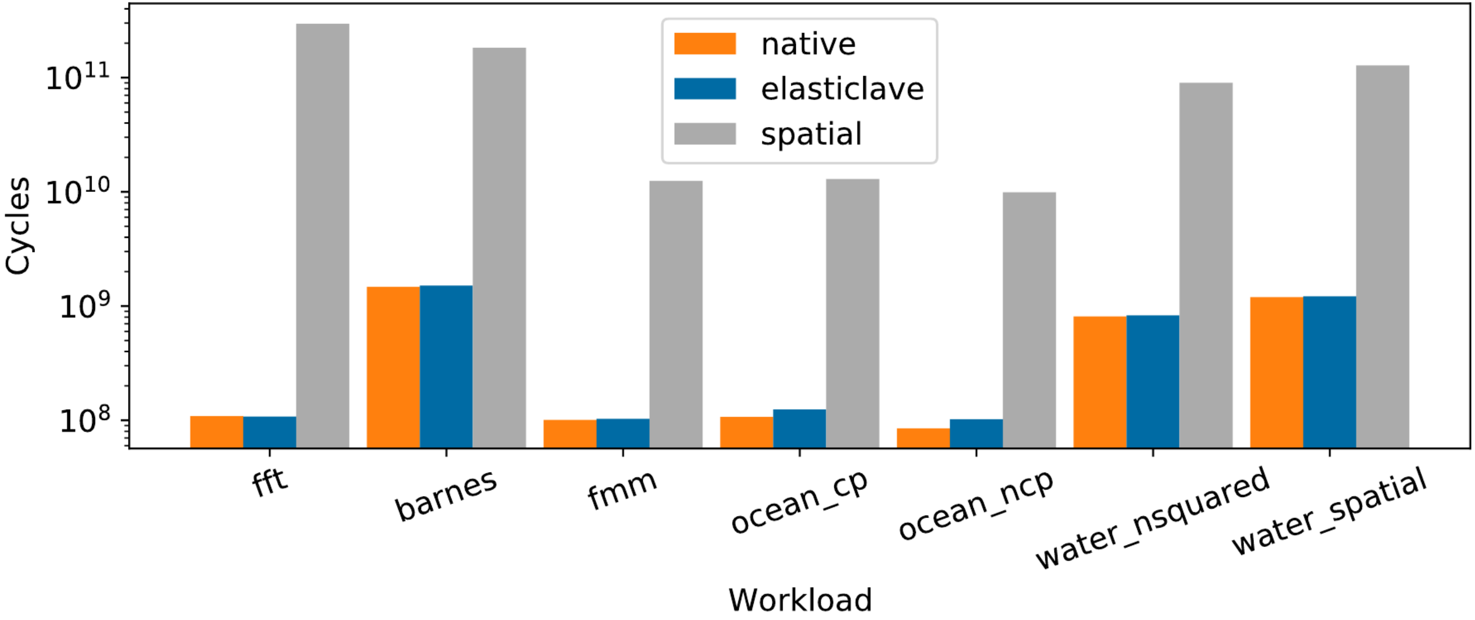
Native: two threads

Evaluation Results on SPLASH-2 (sharing-intensive)



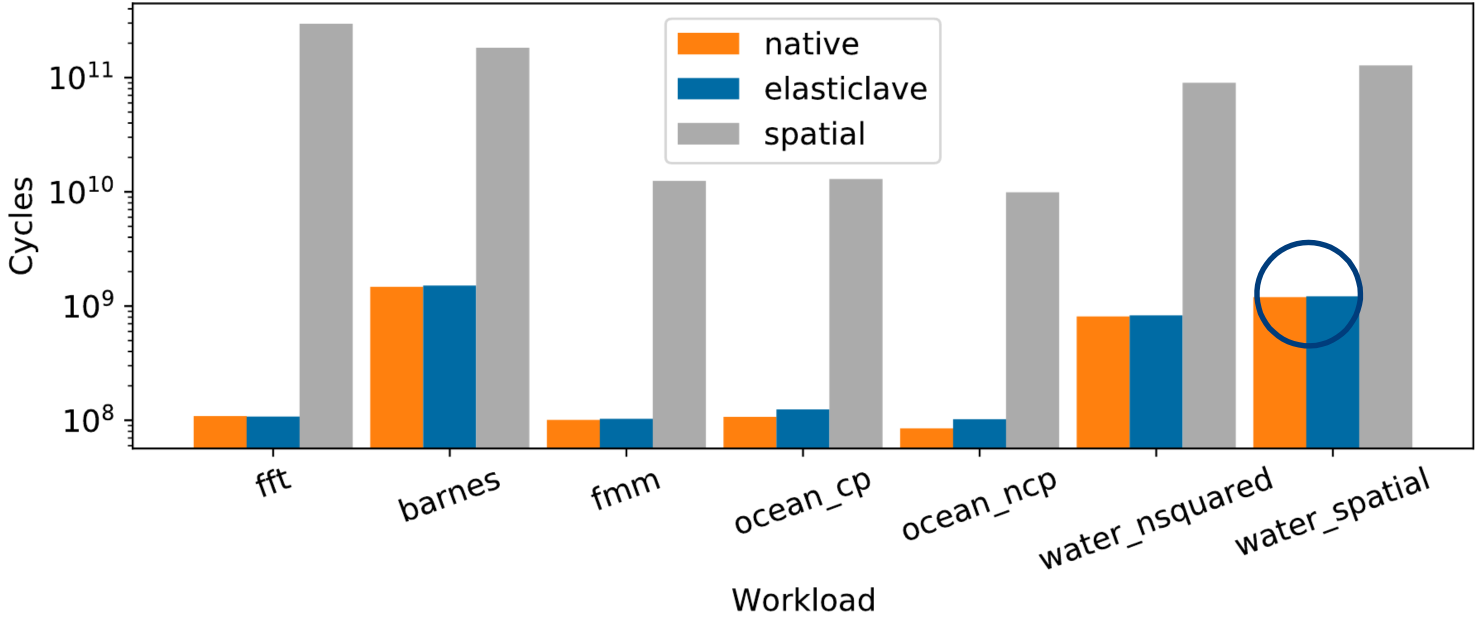
Evaluation Results on SPLASH-2 (sharing-intensive)

100x performance improvement

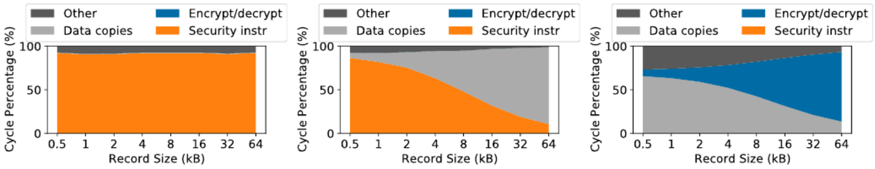


Evaluation Results on SPLASH-2 (sharing-intensive)

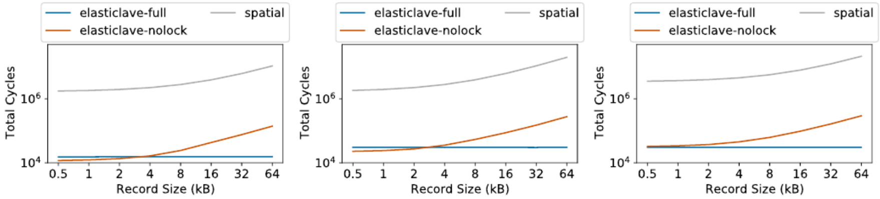
Comparable to native Linux



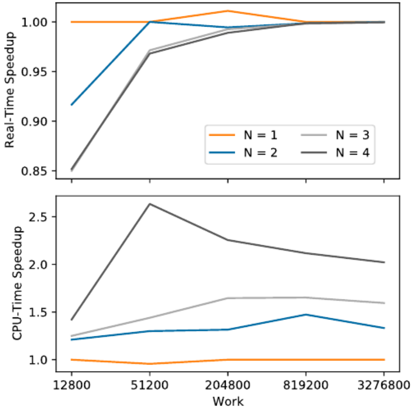
More in Paper

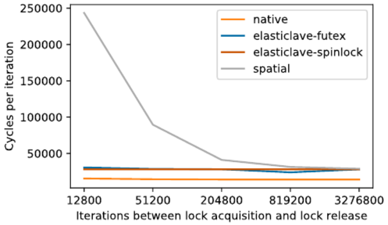


(a) ELASTICLAVE-full (b) ELASTICLAVE-nolock (c) spatial



(a) Producer-consumer (b) Client-server (c) Proxy





Conclusions

- Elasticlave: maximum permissions, effective permissions, lock bit

Conclusions

- Elasticlave: maximum permissions, effective permissions, lock bit
- Prototype implementation on RISC-V

Conclusions

- Elasticlave: maximum permissions, effective permissions, lock bit
- Prototype implementation on RISC-V (using PMP)

Conclusions

- Elasticlave: maximum permissions, effective permissions, lock bit
- Prototype implementation on RISC-V (using PMP)
- Evaluation: 1-2 orders of magnitude performance improvement

Conclusions

- Elasticlave: maximum permissions, effective permissions, lock bit
- Prototype implementation on RISC-V (using PMP)
- Evaluation: 1-2 orders of magnitude performance improvement

ARTIFACT EVALUATED
usenix ASSOCIATION
AVAILABLE

Artifact available: `https://github.com/jasonyu1996/elasticlave`

Conclusions

- Elasticlave: maximum permissions, effective permissions, lock bit
- Prototype implementation on RISC-V (using PMP)
- Evaluation: 1-2 orders of magnitude performance improvement

ARTIFACT
EVALUATED
usenix
ASSOCIATION
AVAILABLE

Artifact available: `https://github.com/jasonyu1996/elasticlave`

Thanks for listening!