Enabling Financial-Grade Secure Infrastructure with Confidential Computing

2021/04

Dr. Hongliang Tian (Tate)

System Architect, Confidential Computing Team, Ant Group

tate.thl@antgroup.com

ANT GROUP | Alipay

1 Confidential Computing & Ant Group

2 Intel SGX & the Occlum Project

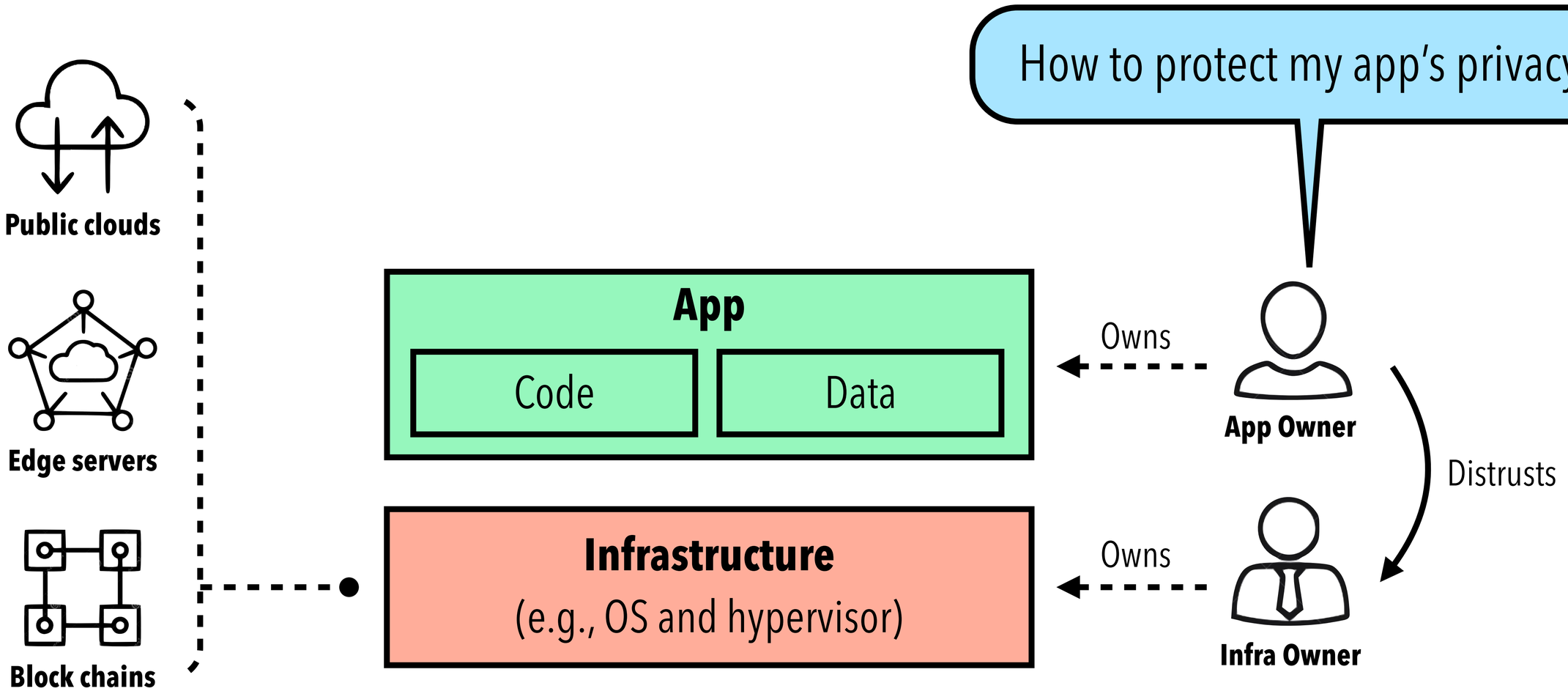
3 Re-architect Occlum with Async-Centric Design

1 Confidential Computing & Ant Group

2 Intel SGX & the Occlum Project

3 Re-architect Occlum with Async-Centric Design

Confidential Computing: The Problem

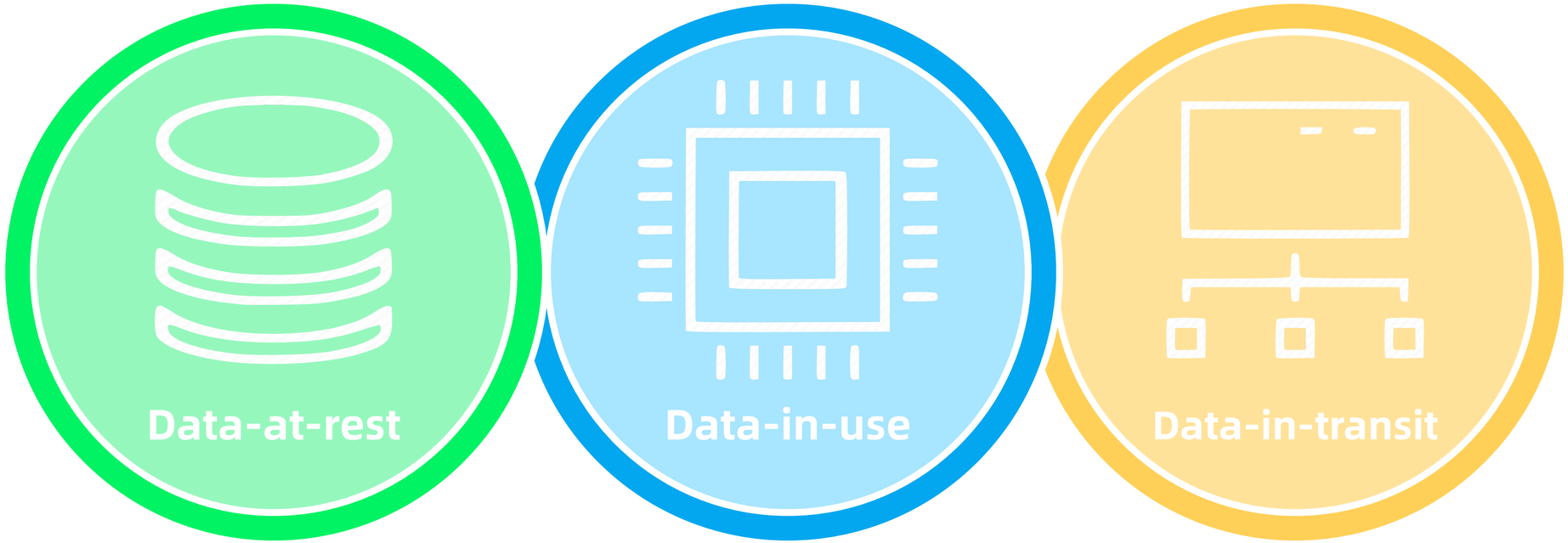


Confidential Computing: The Missing Link

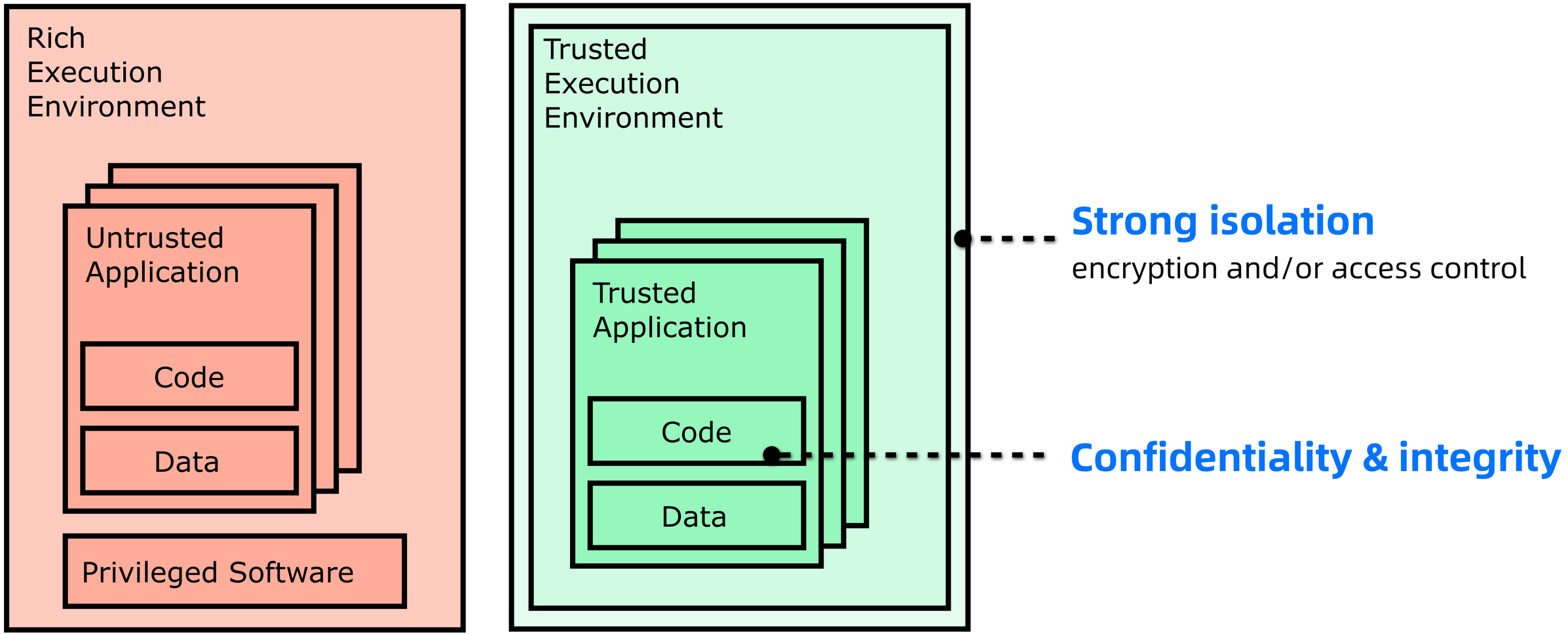
Disk Encryption (traditional)

Memory Encryption (new)

Network Encryption (traditional)



Trusted Execution Environment (TEE)

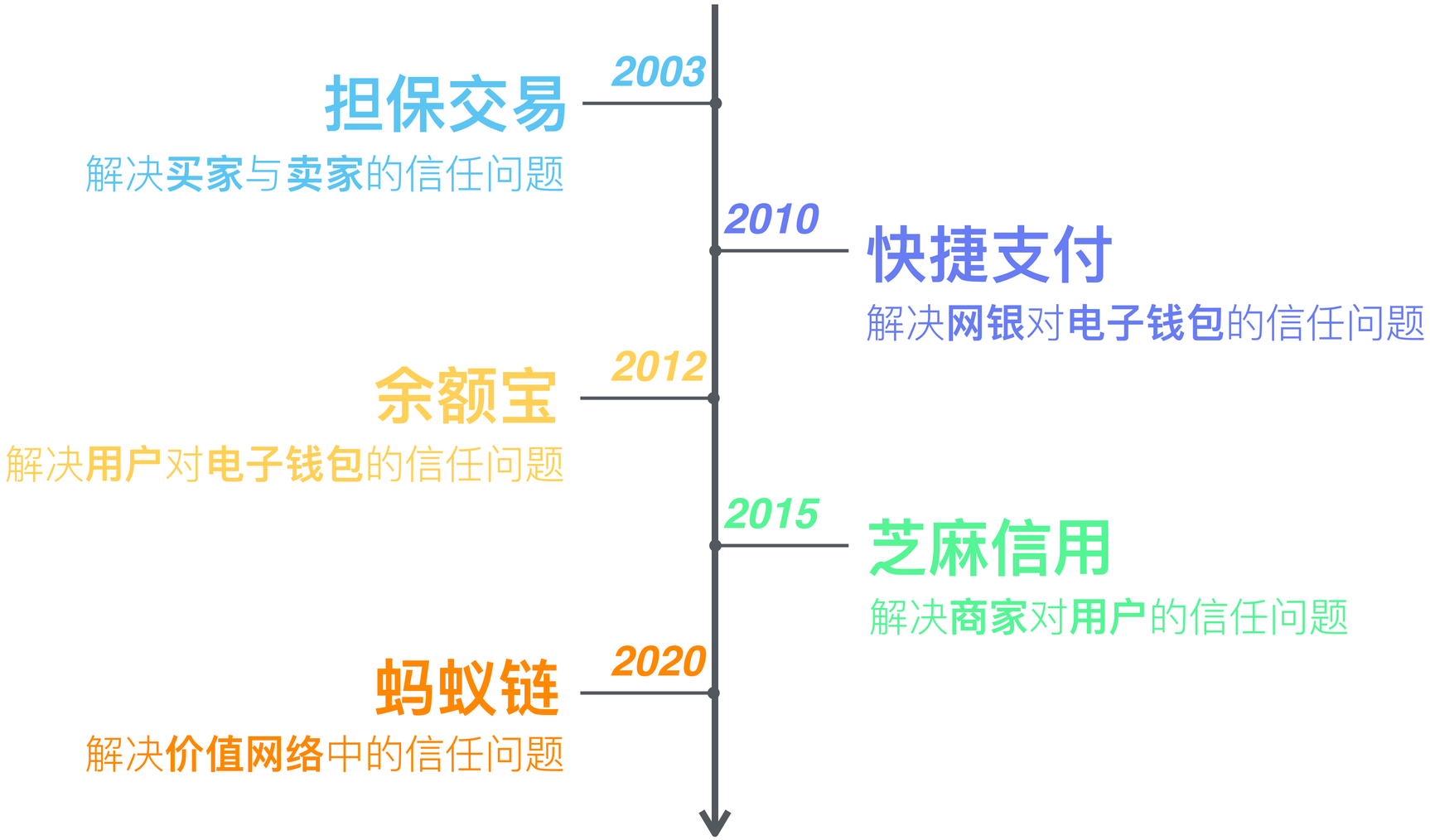


What's in confidential computing for 蚂蚁集团 ANT GROUP ?

支付宝 余额宝 花呗 芝麻信用

网商银行 相互宝 借呗 蚂蚁链

Milestones in the Growth of Ant Group



“16年来，蚂蚁最重要的产品就是建立信任”

——蚂蚁集团董事长井贤栋

Confidential computing as a Technical Foundation to Win the Trust of *Users*, *Partners*, and *Regulators*

Confidential computing as a Technical Foundation to Win the Trust of *Users*, *Partners*, and *Regulators*

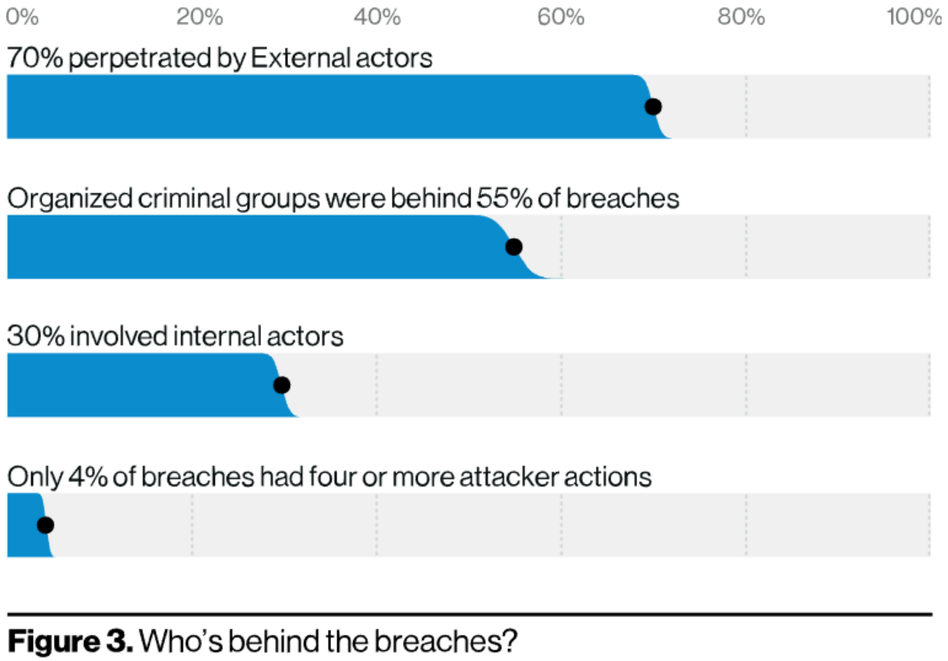
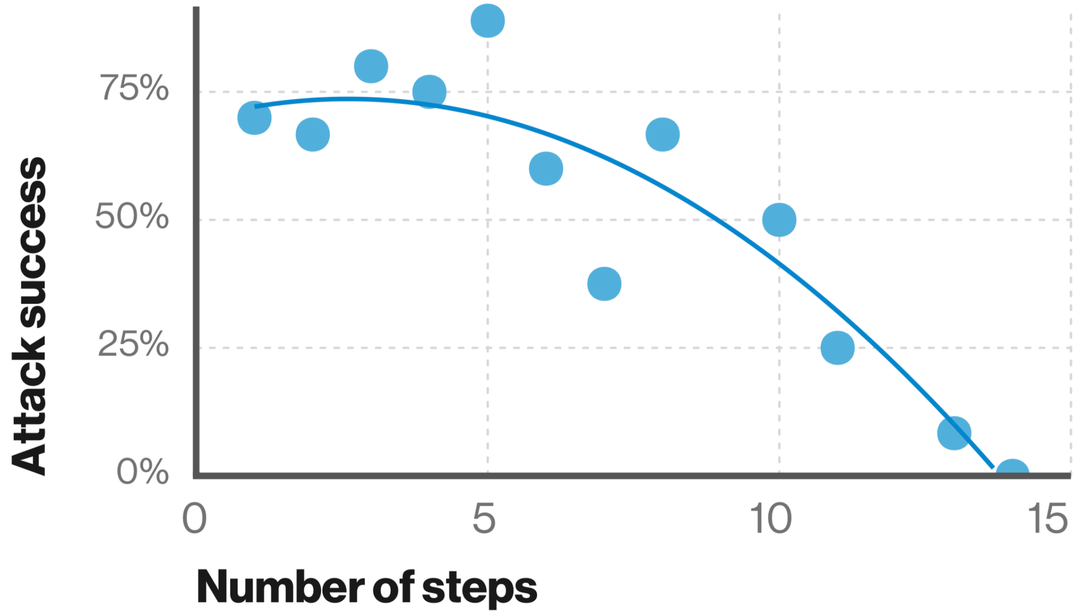


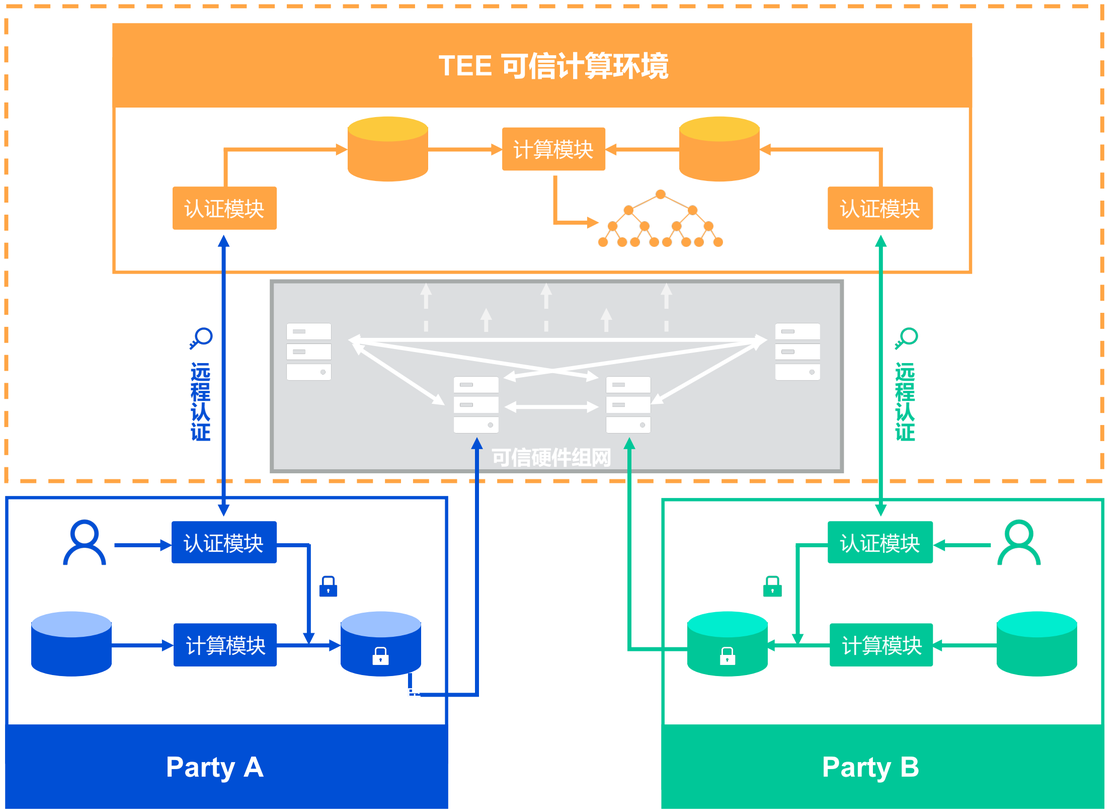
Figure 3. Who's behind the breaches?



- Source: Data Breach Investigations Report, 2019 & 2020

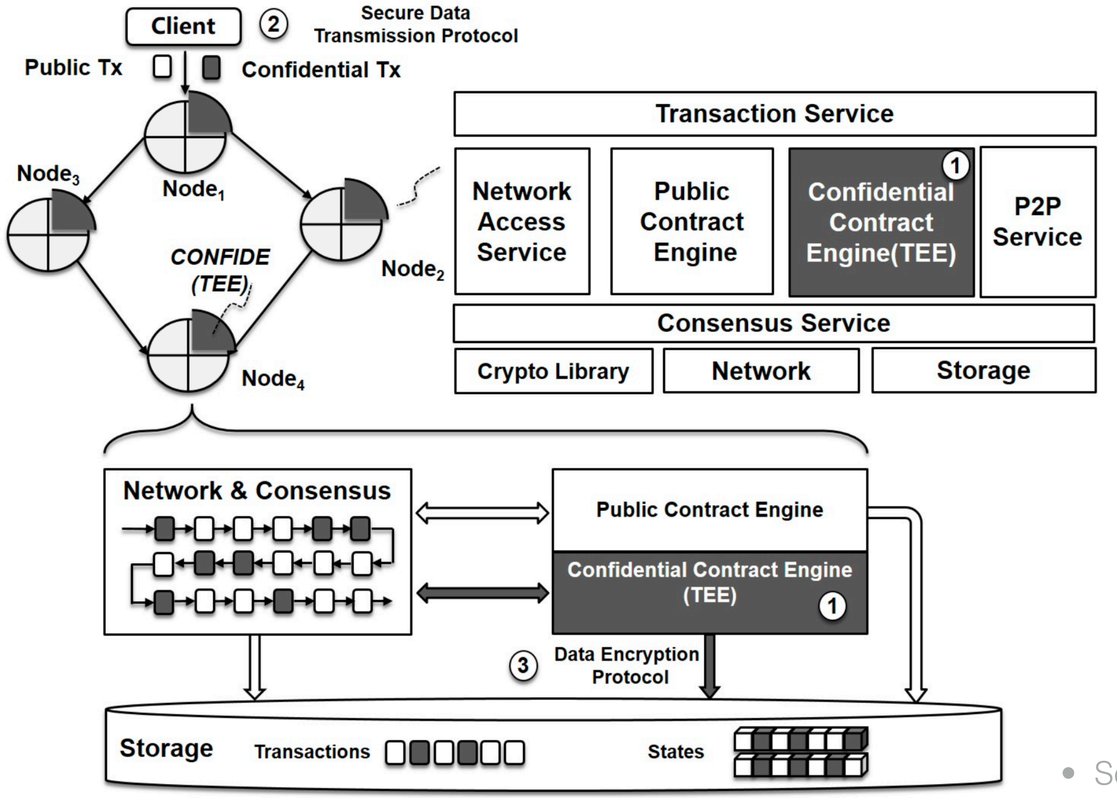
–> Defense-in-depth is effective in preventing data leakage

Confidential computing as a Technical Foundation to Win the Trust of *Users*, *Partners*, and *Regulators*



–> Coopetitive analytics can be enabled with TEEs

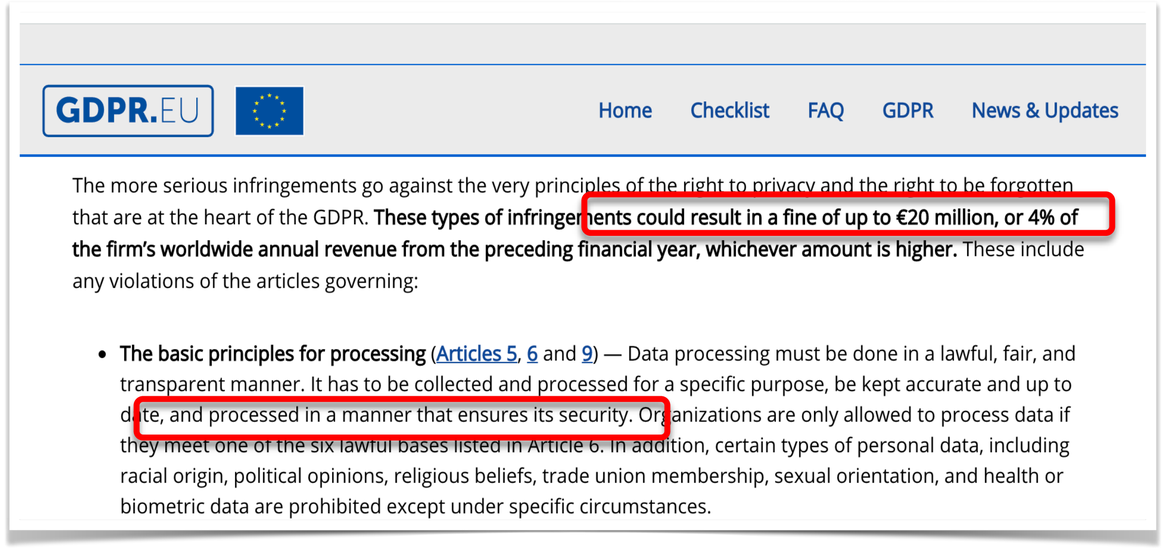
Confidential computing as a Technical Foundation to Win the Trust of *Users*, *Partners*, and *Regulators*



- Source: SIGMOD'202

–> Confidential blockchains can be enabled with TEEs

Confidential computing as a Technical Foundation to Win the Trust of *Users*, *Partners*, and *Regulators*



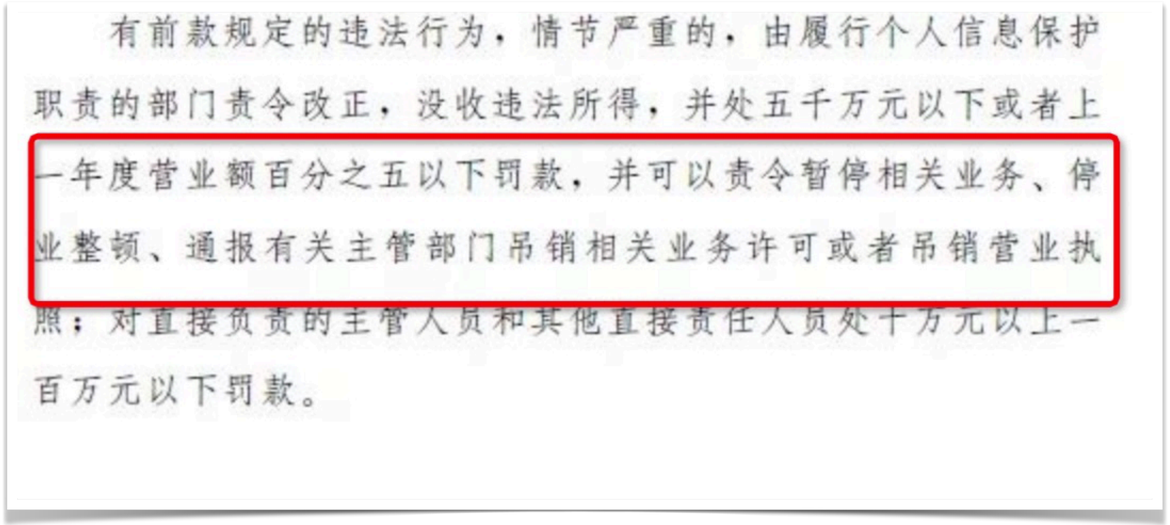
GDPR.EU

Home Checklist FAQ GDPR News & Updates

The more serious infringements go against the very principles of the right to privacy and the right to be forgotten that are at the heart of the GDPR. **These types of infringements could result in a fine of up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.** These include any violations of the articles governing:

- **The basic principles for processing** (Articles 5, 6 and 9) — Data processing must be done in a lawful, fair, and transparent manner. It has to be collected and processed for a specific purpose, be kept accurate and up to date, and processed in a manner that ensures its security. Organizations are only allowed to process data if they meet one of the six lawful bases listed in Article 6. In addition, certain types of personal data, including racial origin, political opinions, religious beliefs, trade union membership, sexual orientation, and health or biometric data are prohibited except under specific circumstances.

General Data Protection Regulation (GDPR)



有前款规定的违法行为，情节严重的，由履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务、停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

《个人信息保护法》

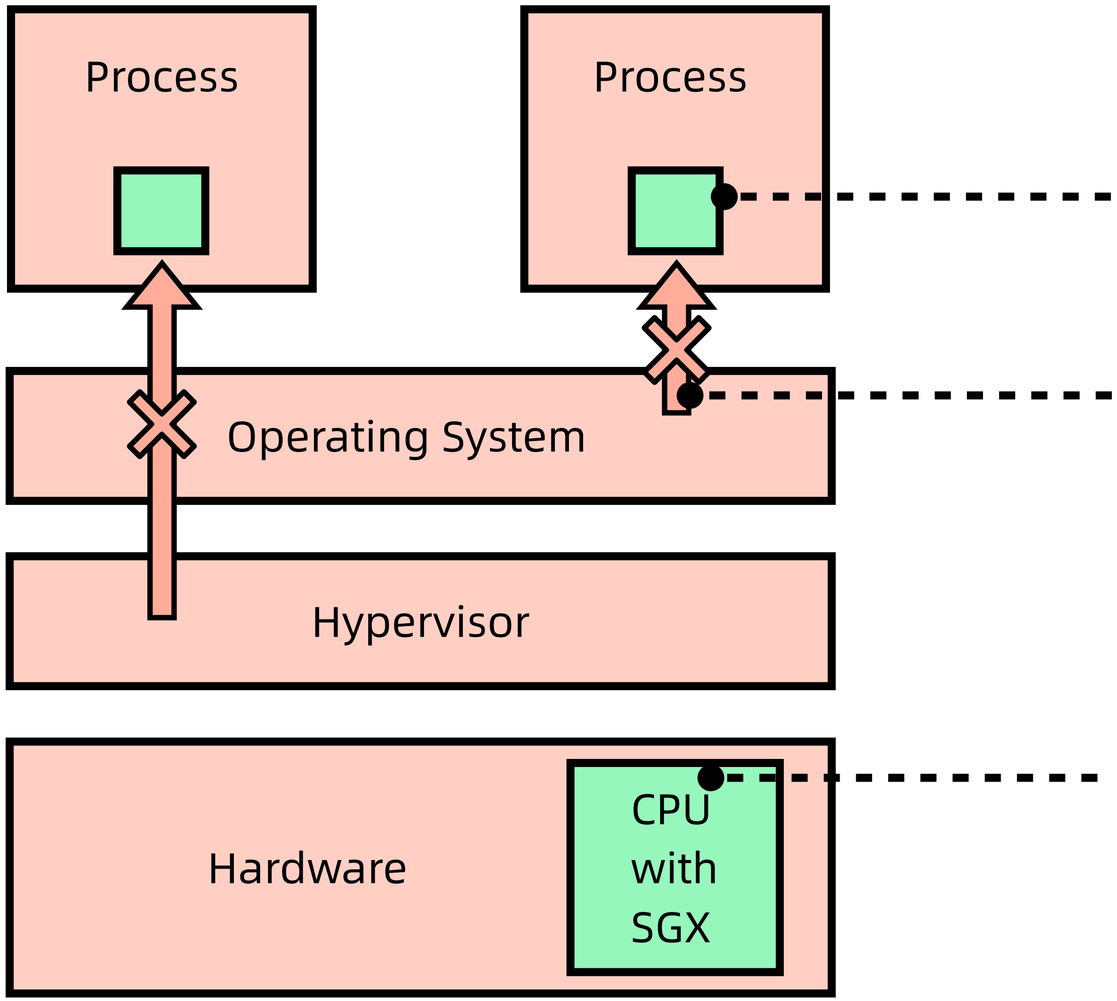
–> Legal compliance is increasingly important for enterprises

1 Confidential Computing & Ant Group

2 Intel SGX & the Occlum Project

3 Re-architect Occlum with Async-Centric Design

Intel Software Guard Extensions (SGX)

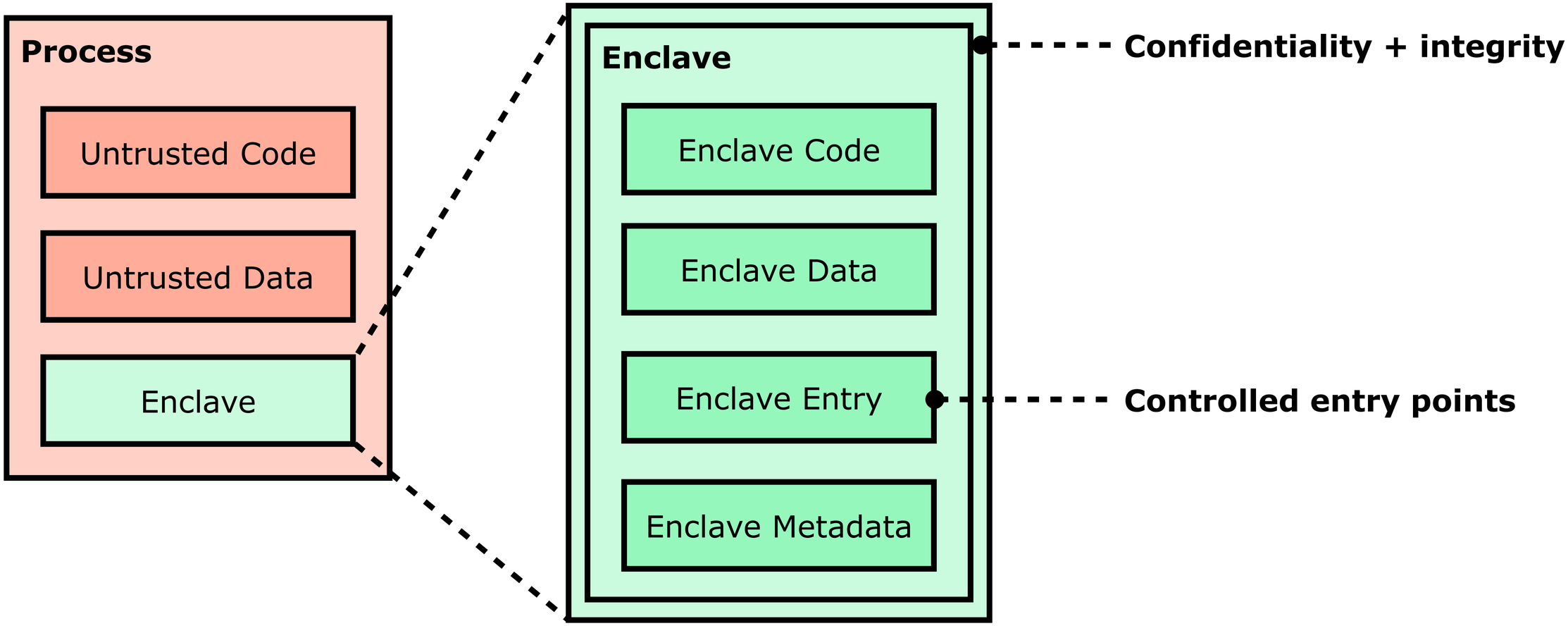


Private memory regions named enclaves

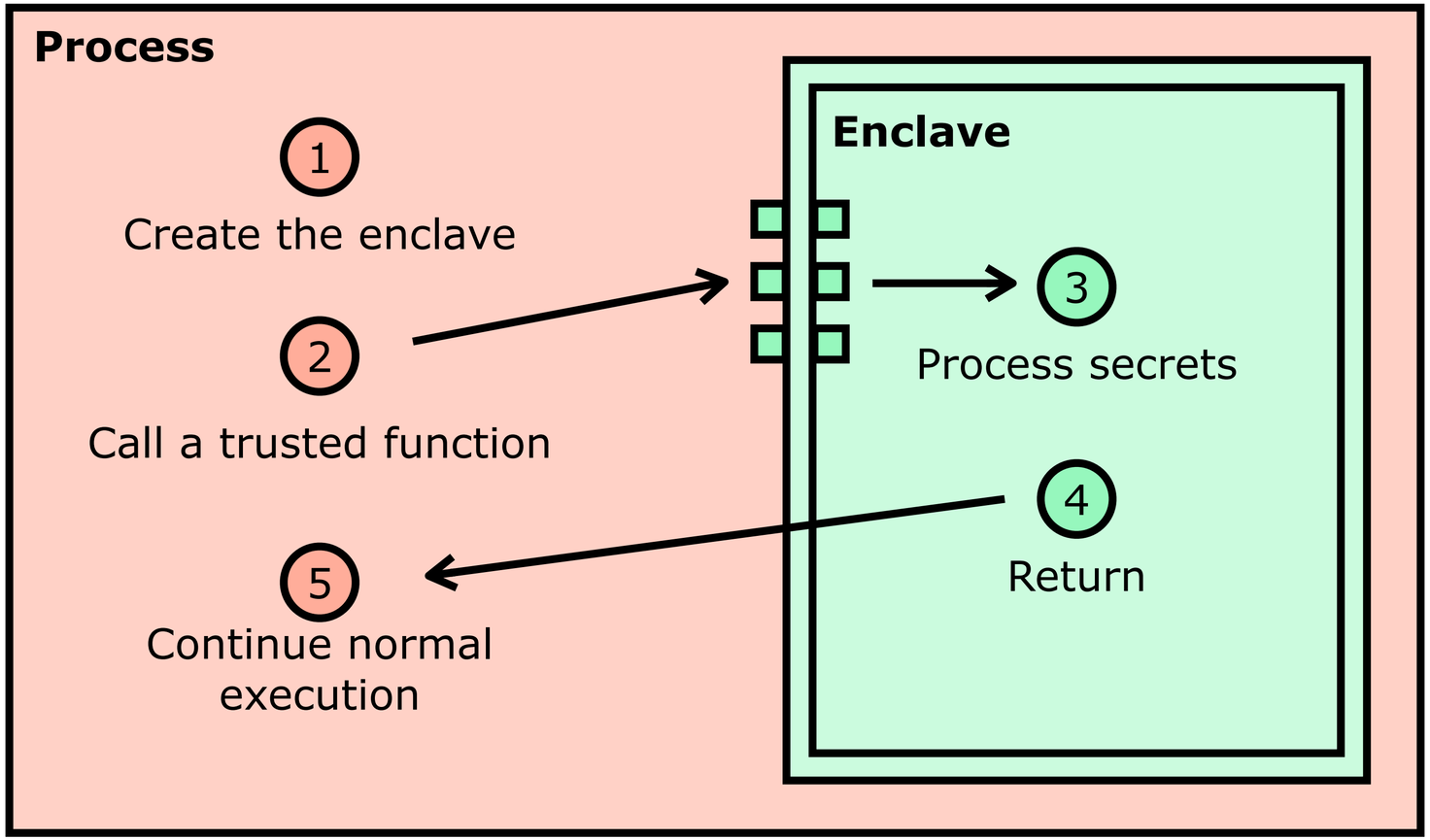
Privileged attacks prevented

Only the CPU is trusted, not any privileged software

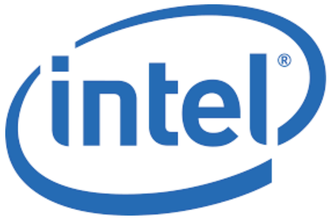
Intel SGX: The Memory Layout



Intel SGX: The Programming Model



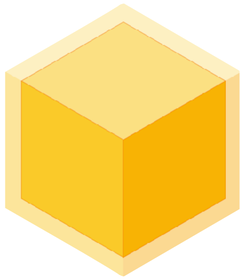
All Kinds of SGX SDKs



Intel SGX SDK

Open Enclave SDK

(Founded by Microsoft)



Google Asylo

Rust SGX SDK

(Founded by Baidu)

Are SGX SDK Satisfying?

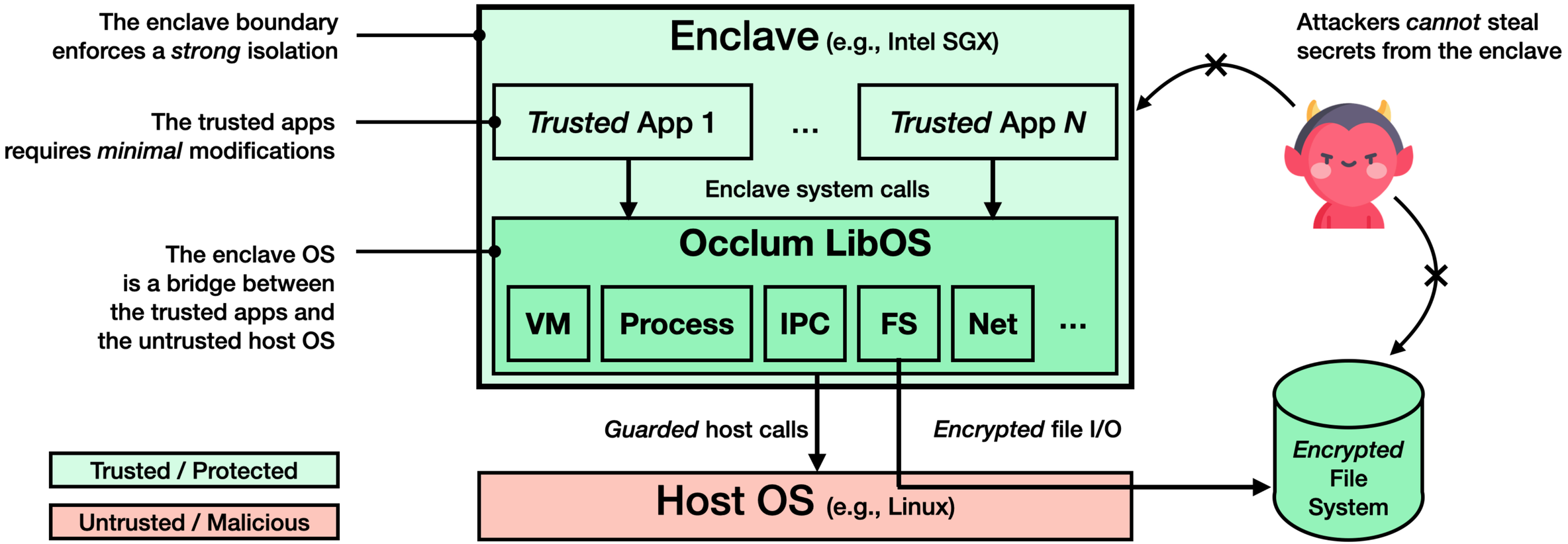
- The answer is **NO**
- Because the programmers
  - Have to learn the SGX programming model
  - Are bound to a specific programming language
  - Are only provided with a limited set of APIs

Occlum

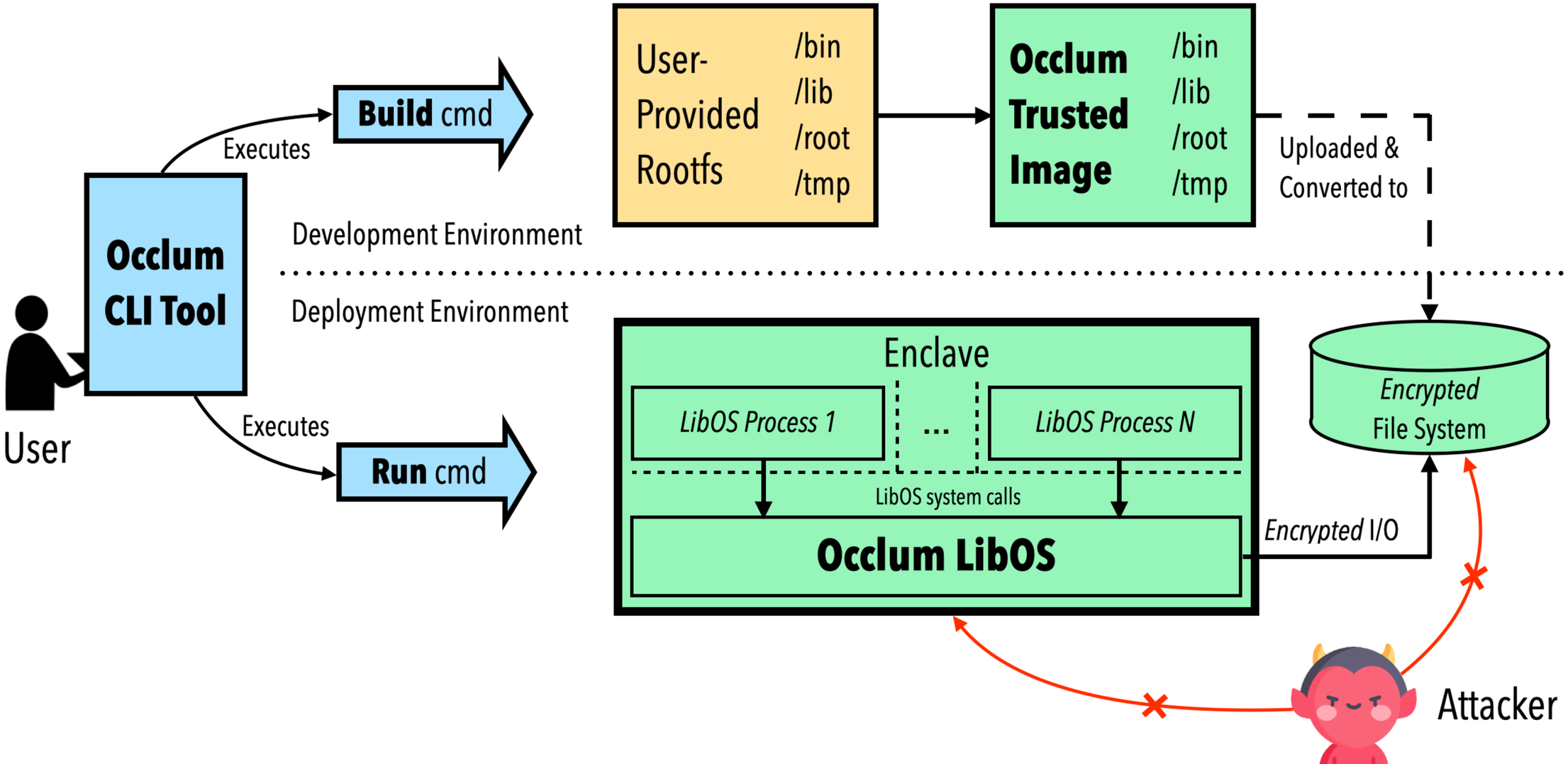
Empowering everyone to run every app in enclaves

https://github.com/occlum/occlum

Architecture Overview



Workflow Overview



Hello Occlum

More Demos

https://github.com/occlum/occlum/tree/master/demos

Programming Languages
C/C++
Java
Python
Go
Rust
Shell scripts

Popular Applications
Redis
Vault
SQLite
PyTorch
Flink
XGBoost

Confidential Computing Consortium (CCC)

+=

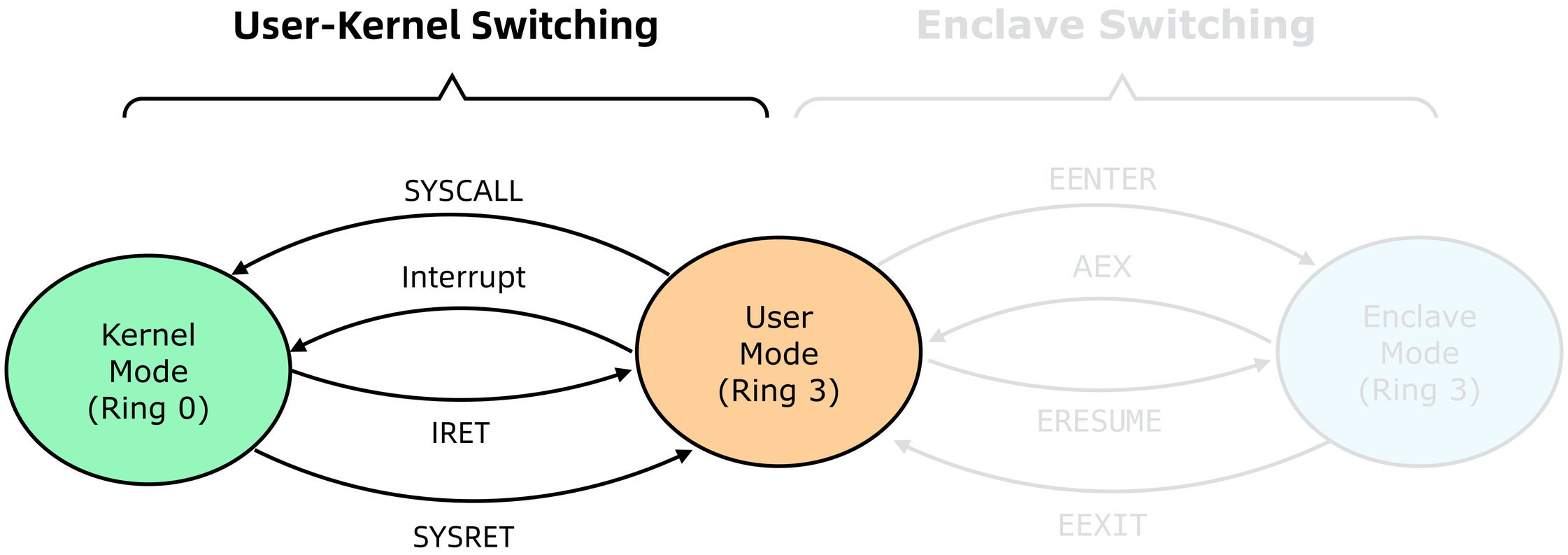
- A Linux Foundation project and community that aims at accelerating the adoption of confidential computing
- The first open-source project from China that is contributed to CCC

1 Confidential Computing & Intel SGX

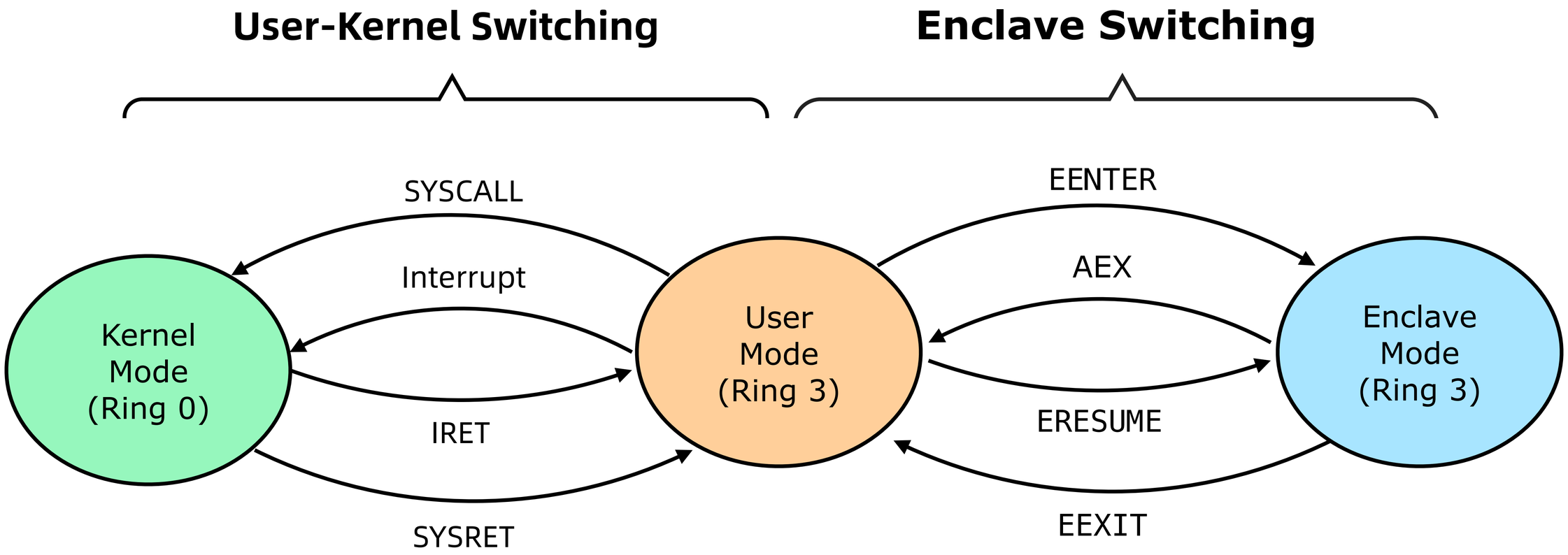
2 Ant Group & the Occlum Project

3 Re-architect Occlum with Async-Centric Design

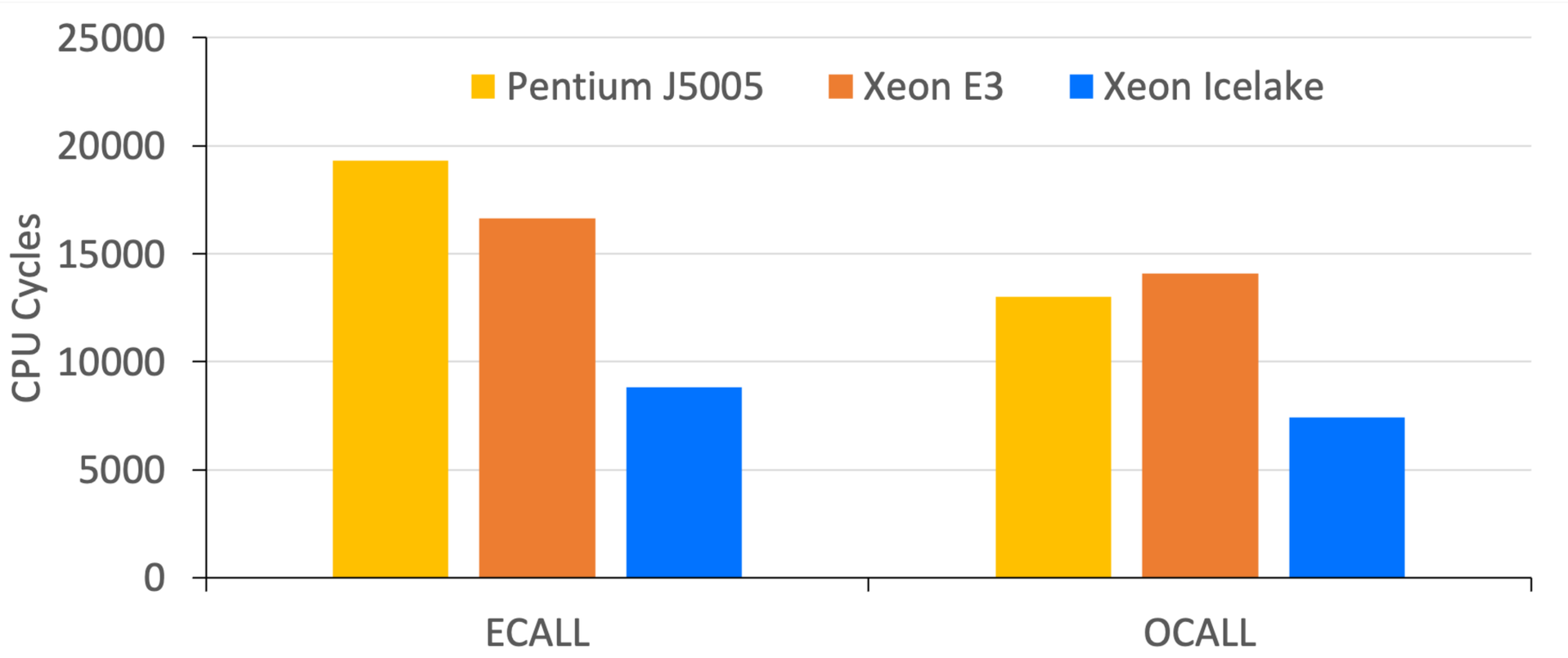
The Curse of SGX: Enclave Switching



The Curse of SGX: Enclave Switching



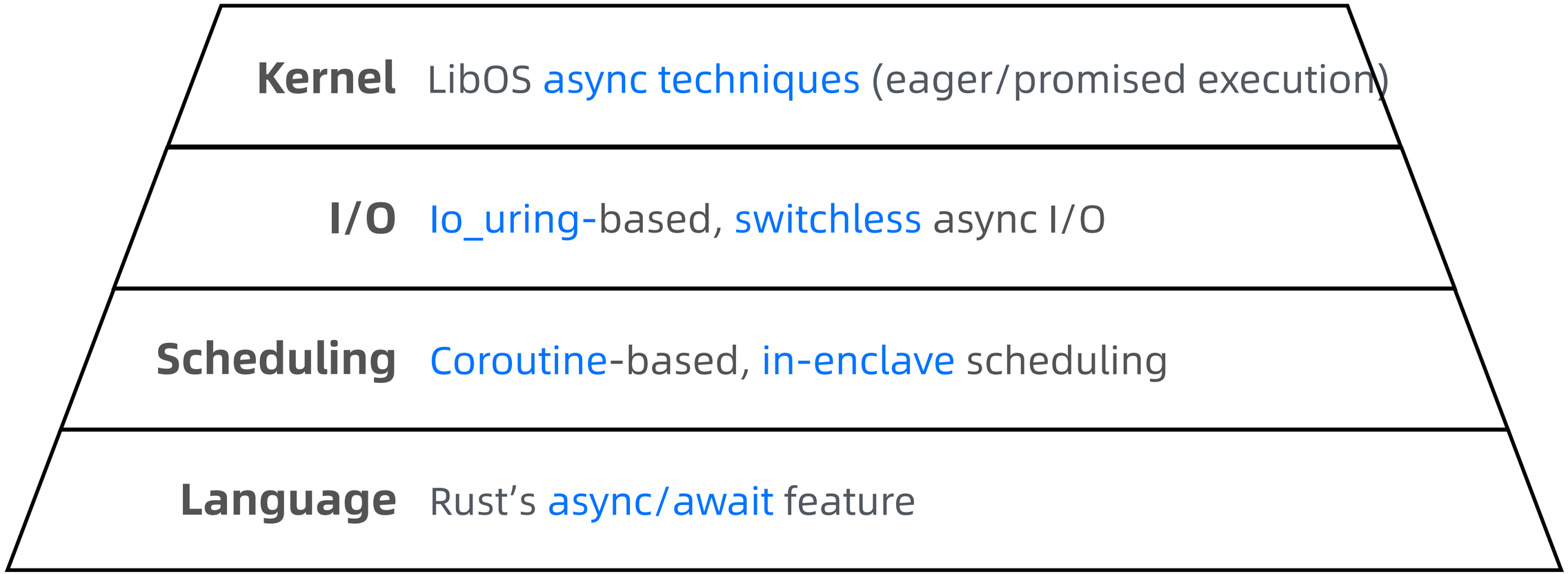
The Cost of Enclave Switching



–> The enclave switching is *very expensive* compared to user-kernel switching

Next-Gen Occlum (NGO): Asynchrony-Centric Design

To help eliminate enclave switching and increases parallelism



Coroutine-Based, In-Enclave Scheduling

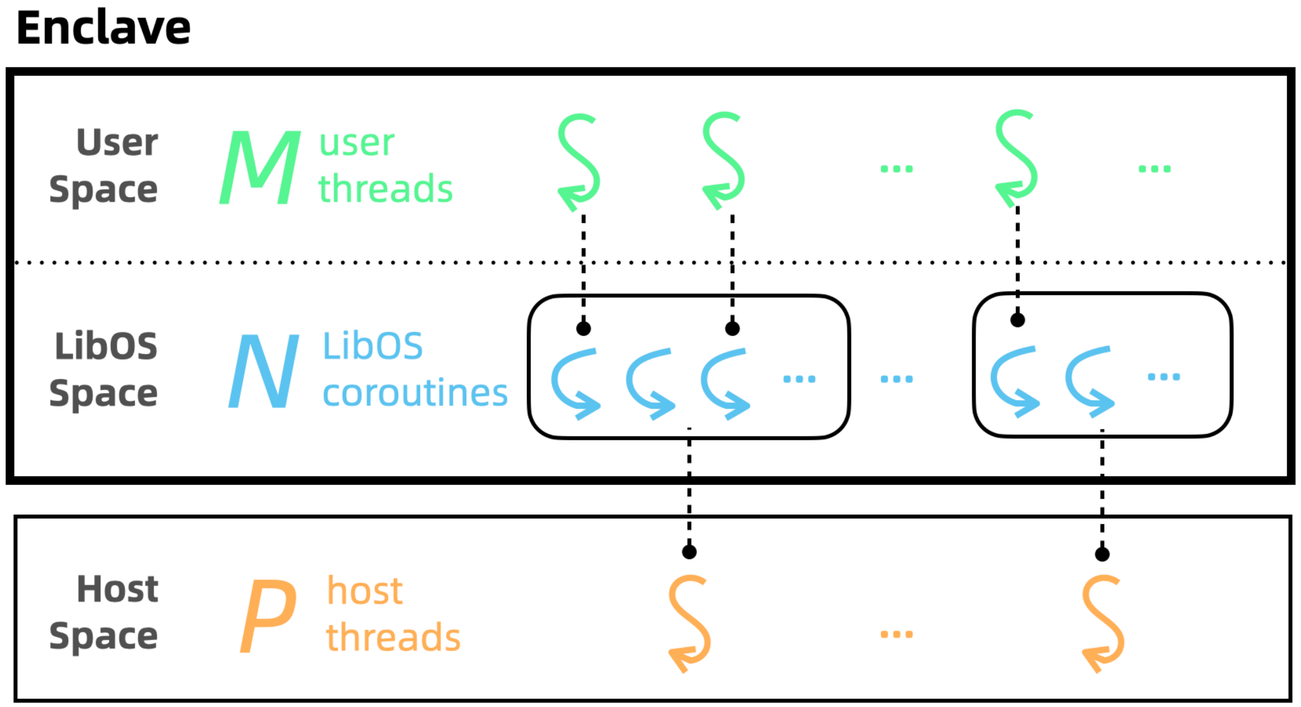


Figure. How tasks are scheduled in NGO

- Coroutines are very light-weight
  - Fast to create or destroy
  - Minimal memory footprint
- Coroutines are scheduled efficiently
  - N coroutines scheduled on P hos threads
  - No enclave switching
- Coroutines run either LibOS or user tasks
  - LibOS tasks are cooperatively scheduled
  - User tasks (i.e. threads) are preemptible

–> Increase LibOS *parallelism* with *minimal* overhead

Io_uring-based, Switchless Async I/O

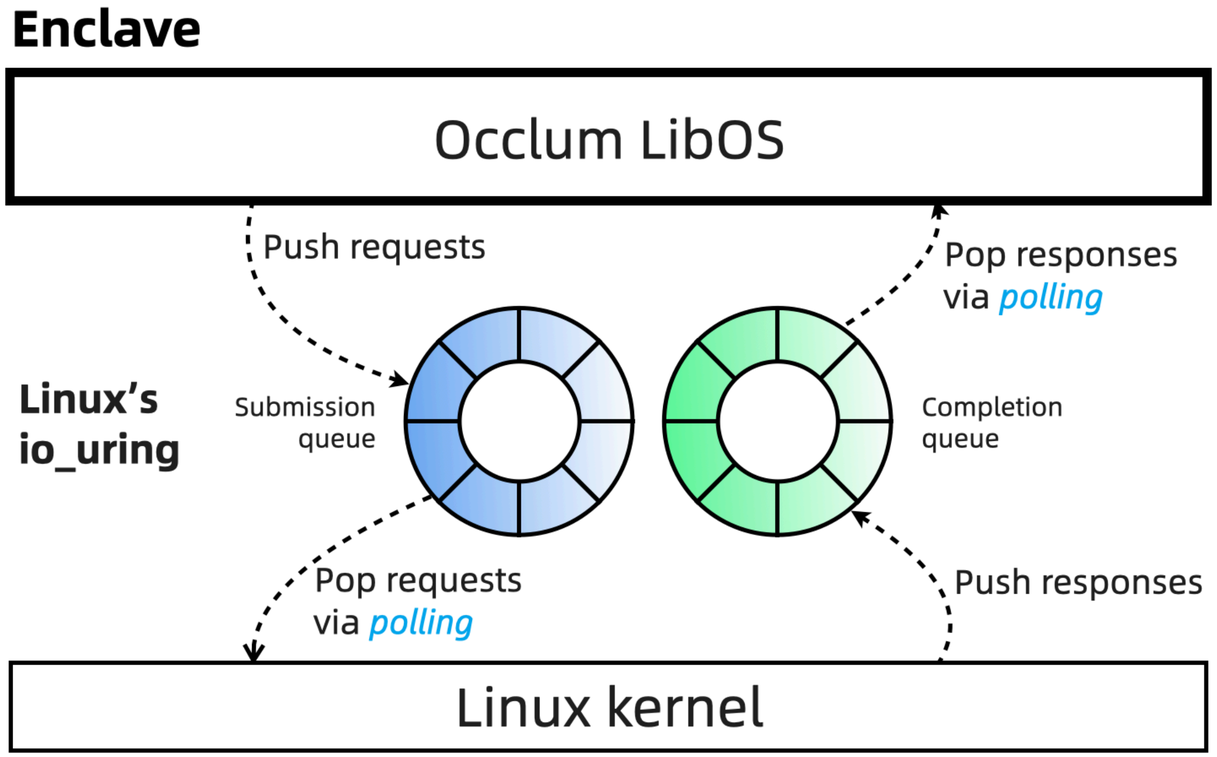


Figure. How NGO performs I/O with io_uring

- A new I/O interface first introduced in Linux kernel 5.1 and still fast growing
- Support most I/O operations
- Very efficient
  - No syscall (i.e., polling)
  - No user page mapping (optional)

–> Enable *true* async I/O in a *switchless* and *speedy* way

Performance Evaluation: Scheduling

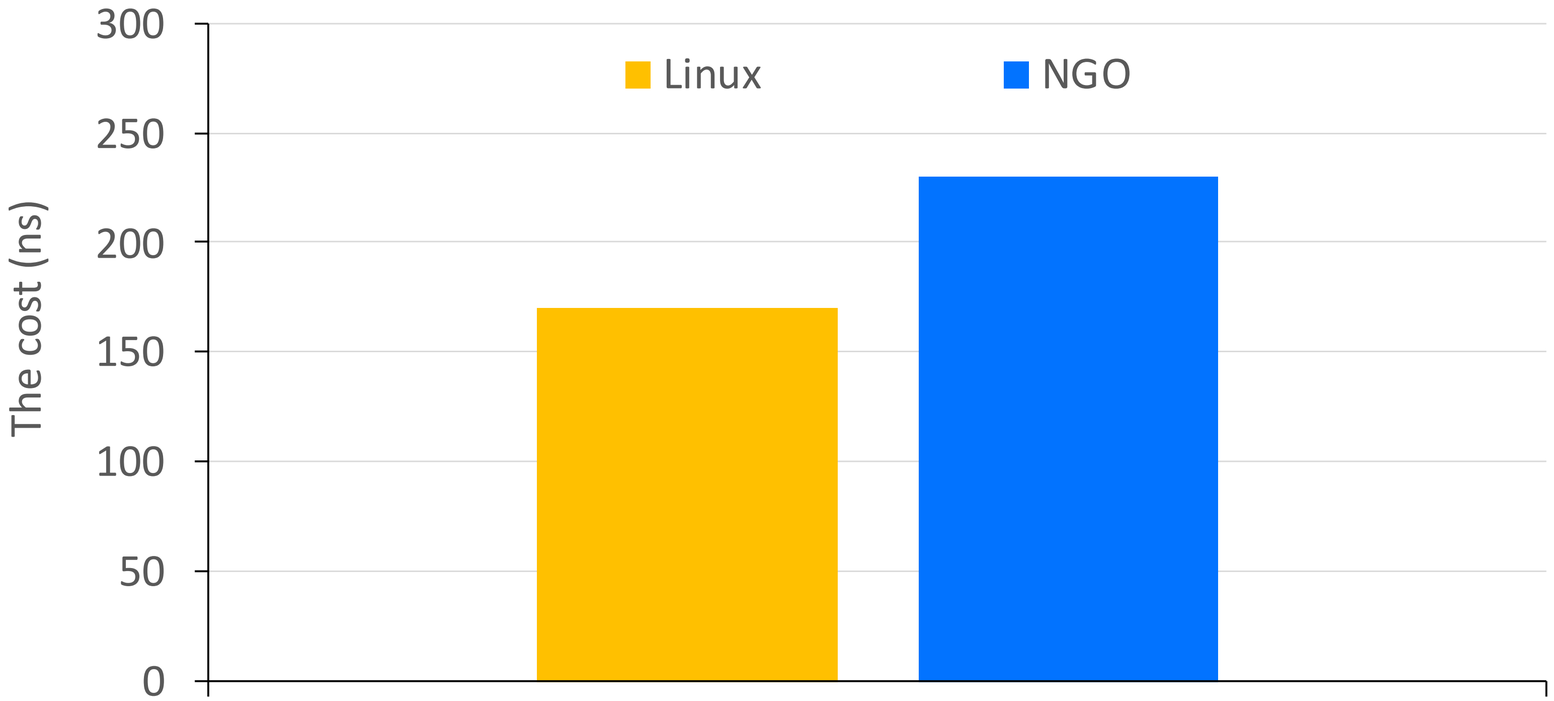


Figure. Thread scheduling (via sched_yield)

–> The *scheduling* performance of NGO is on par with that of Linux

Performance Evaluation: Socket I/O

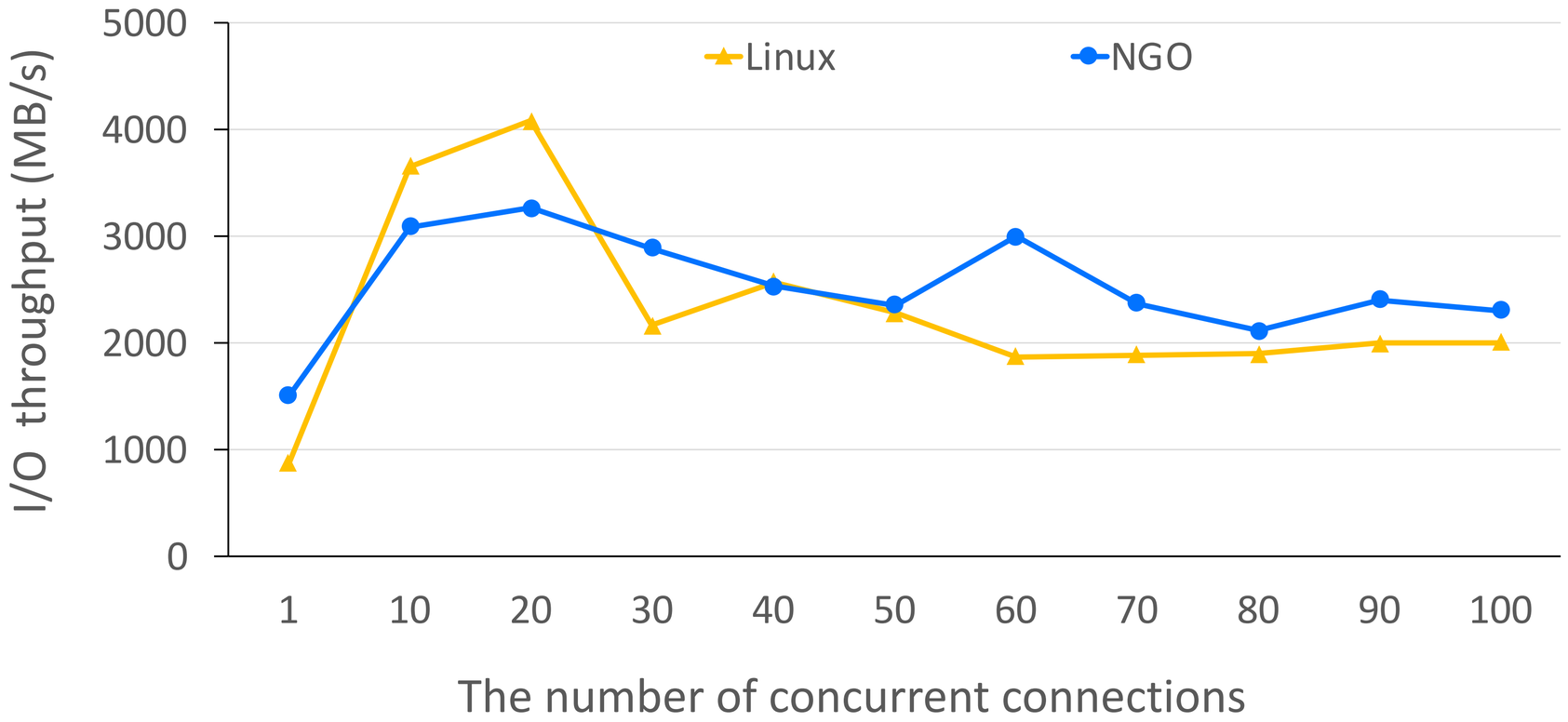


Figure. An event loop-based *echo server* serving local clients

–> The *network* I/O performance of NGO is on par with that of Linux

Performance Evaluation: File I/O

Page cache hit ratio: 0%

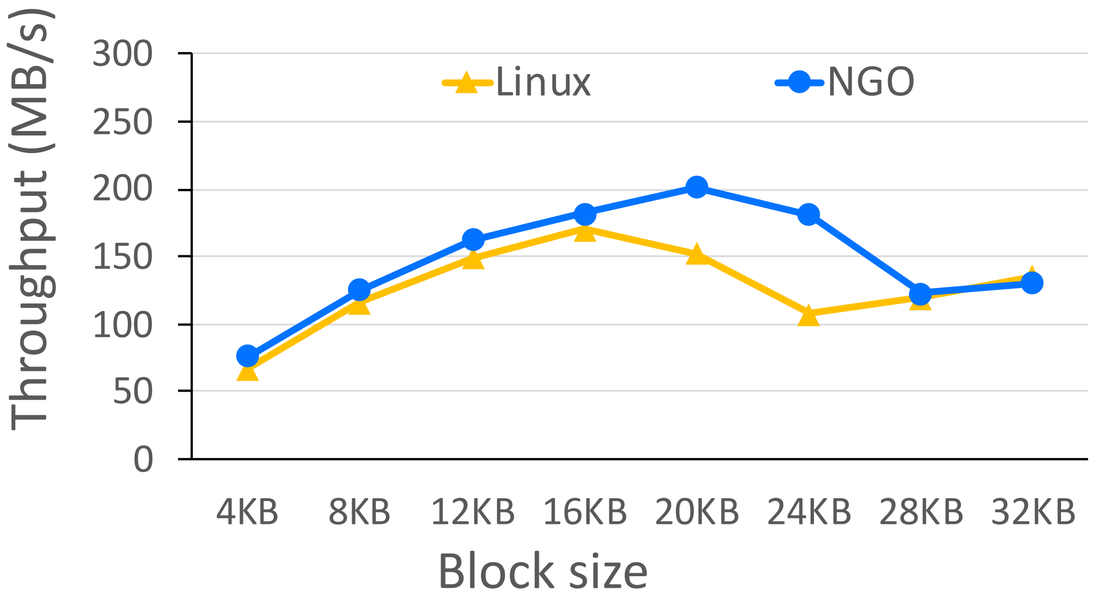


Fig. Sequential reads

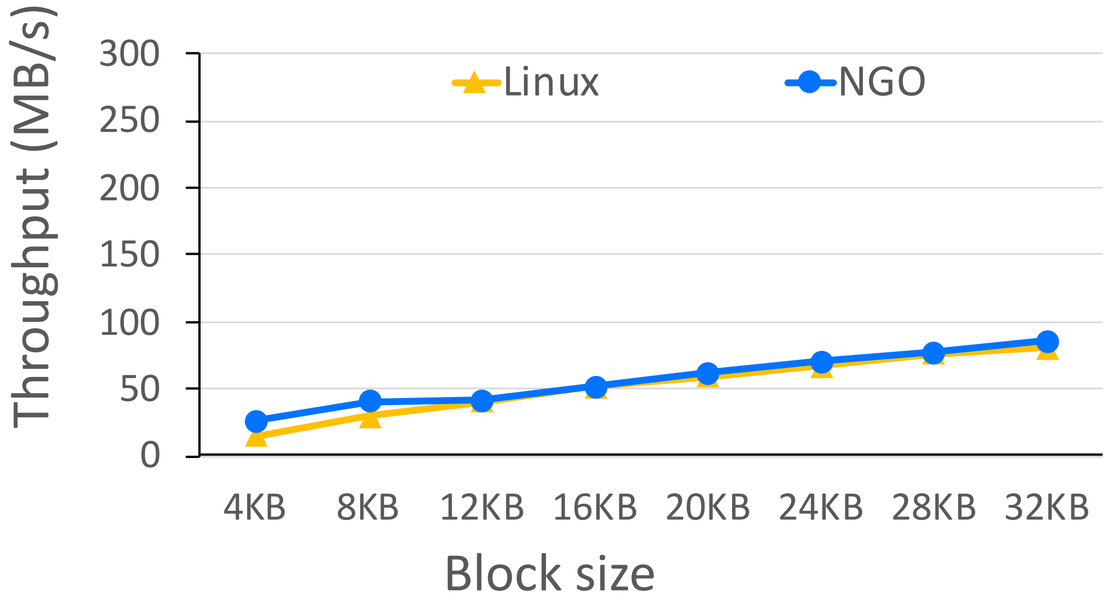


Fig. Random reads

Performance Evaluation: File I/O

Page cache hit ratio: 0%

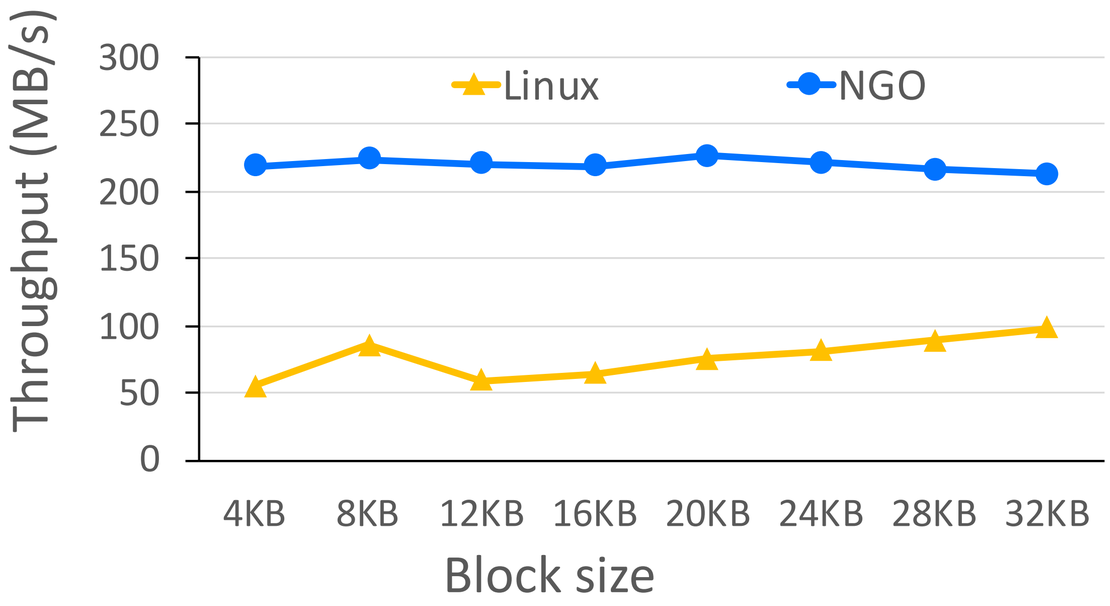


Fig. Sequential writes

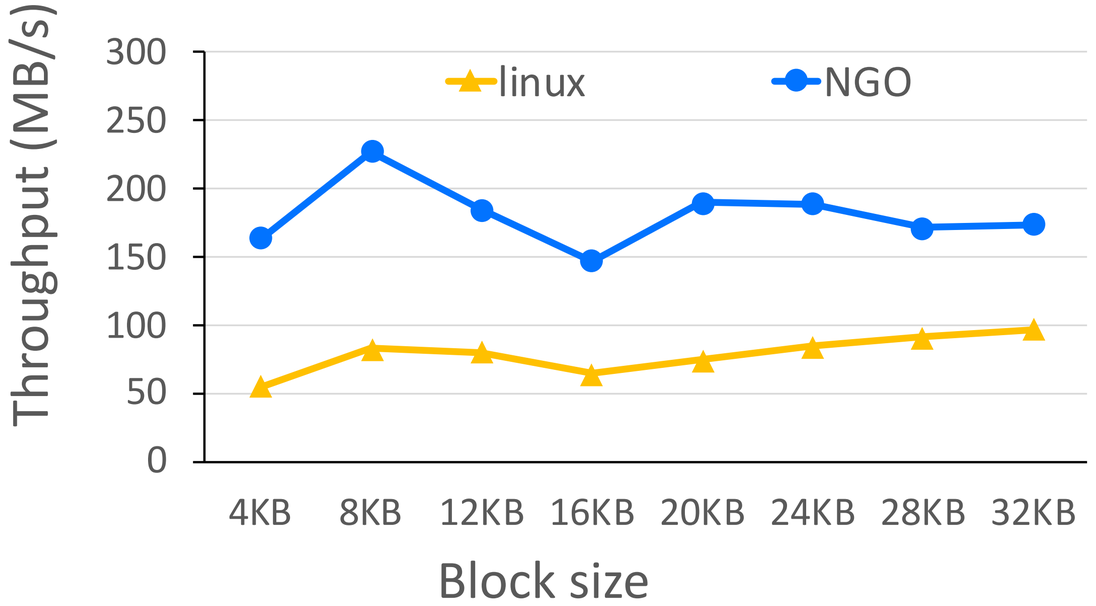


Fig. Random writes

–> The (unencrypted) *file* I/O performance of NGO is on par with that of Linux

1 Confidential Computing & Intel SGX

2 Ant Group & the Occlum Project

3 Re-architect Occlum with Async-Centric Design

Key Takeaways

- Confidential computing is an emerging technology that enables the trust-based business model of Ant Group.
- Porting applications to Intel SGX is made simple with Occlum.
- Intel SGX may incur a significant performance overhead due to enclave switching.
- The latest version of Occlum introduces the async-centric design to deliver a close-to-native performance.

Thank you

Occlum

https://github.com/occlum/occlum

ANT GROUP | Alipay