蚂蚁集团
ANT GROUP

SOFAEnclave: 机密计算，可信原生

SOFAEnclave Confidential Computing, a Pillar of Trust-Native Computing

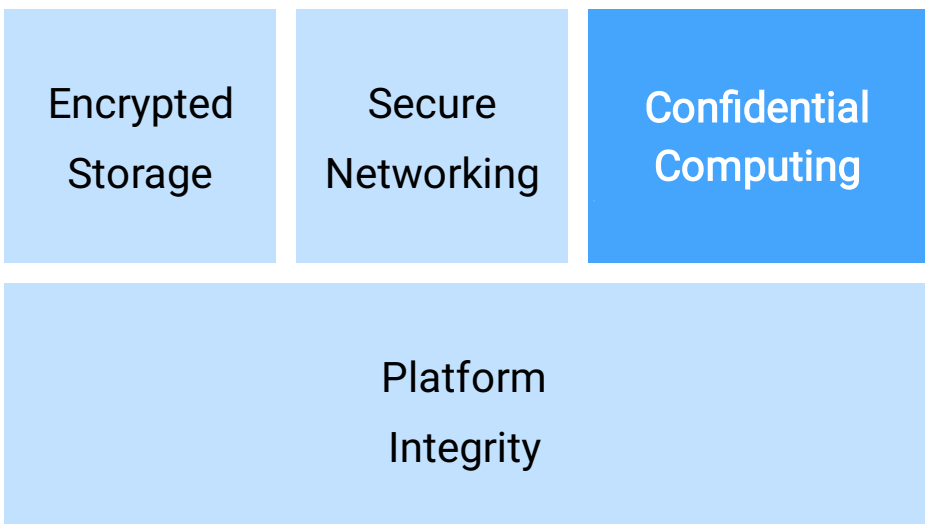
闫守孟

蚂蚁集团

Shoumeng Yan

Director of Ant Confidential Computing

From Cloud-Native to Trust-Native



Confidential Computing

Isolating sensitive data with enclaves, or trusted execution environments (TEEs), such as SGX and TrustZone etc., confidential computing protects applications against threats from other applications, operating systems, or other CSP tenants.

蚂蚁集团 ANT GROUP

SOFAEncalve: Confidential Computing Made Easy

Constrained programming models, languages, and APIs

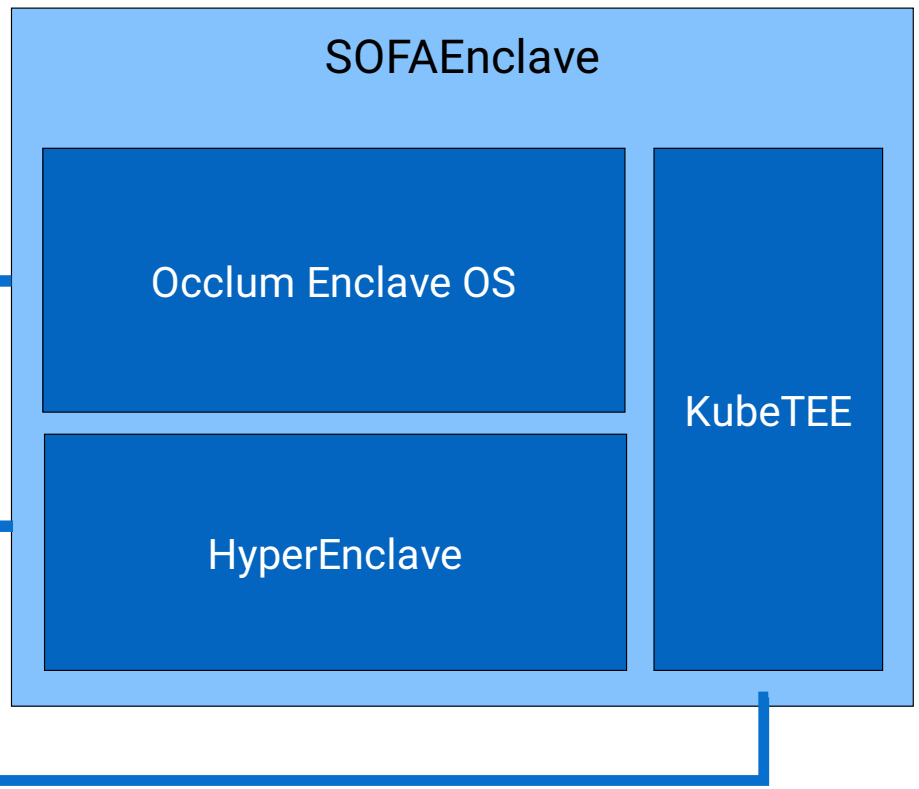
受限的编程模型、编程语言和API

Fragmented enclave platforms

繁多的enclave硬件，适配复杂

Insufficient support from cluster management software

缺乏生产级集群管理软件的支持



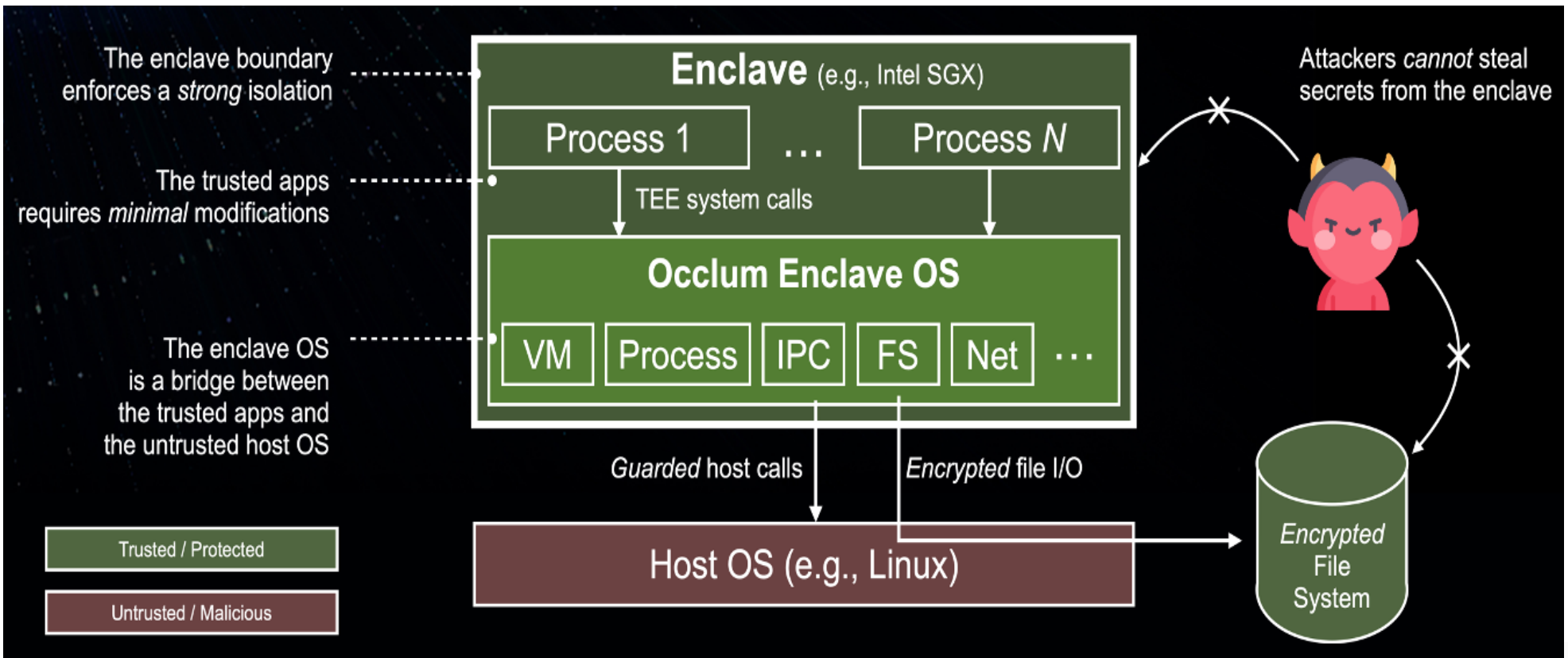
蚂蚁集团 ANT GROUP

Occlum Is The Most User-Friendly Open-Source Enclave OS

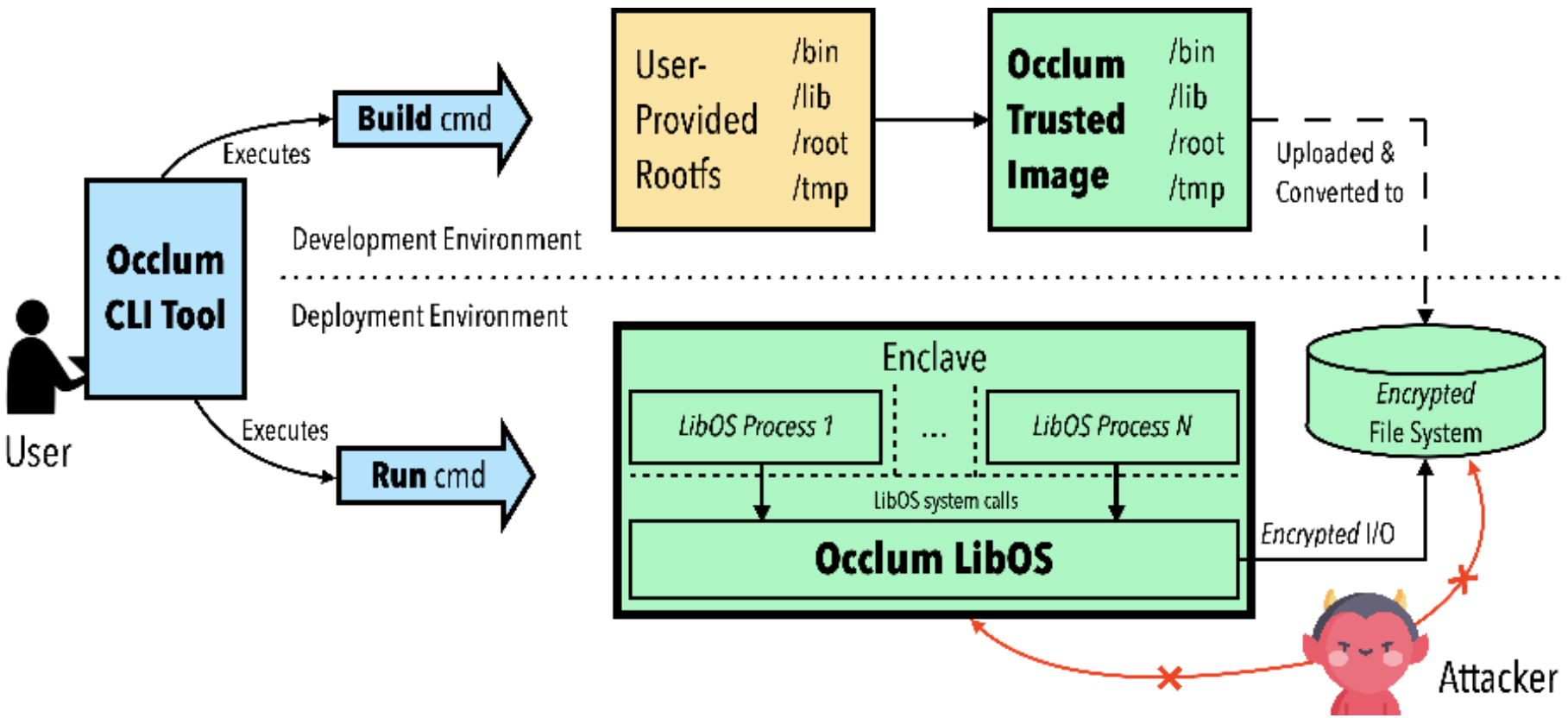
https://github.com/occlum/occlum

蚂蚁集团
ANT GROUP

Occlum Enclave OS: An Overview



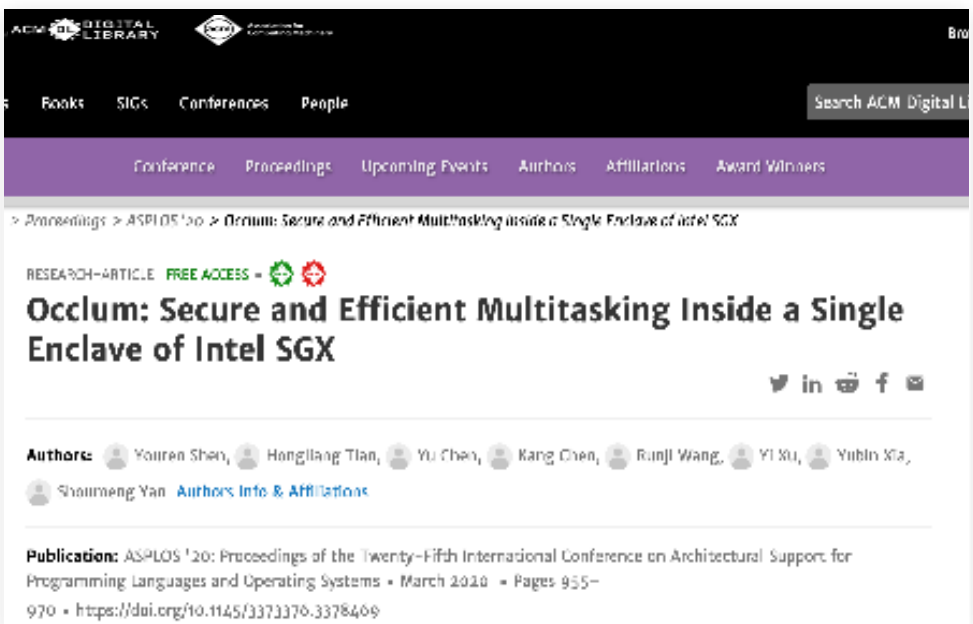
蚂蚁集团 ANT GROUP



蚂蚁集团
ANT GROUP

Occlum Features

- POSIX APIs
- Container-like UX
- Mainstream languages
- Full-fledged file systems
- Memory safety



蚂蚁集团
ANT GROUP

Community

SGX 2.0 Performance Evaluation & Optimization

与Intel合作研究在SGX 2上的性能优化

Alicloud Inclavare Containers Powered by Occlum

与阿里云合作基于Occlum在Enclave上实现OCI兼容

Confidential Computing for Blockchains

与Hyperledger旗下项目合作赋能区块链的机密性计算

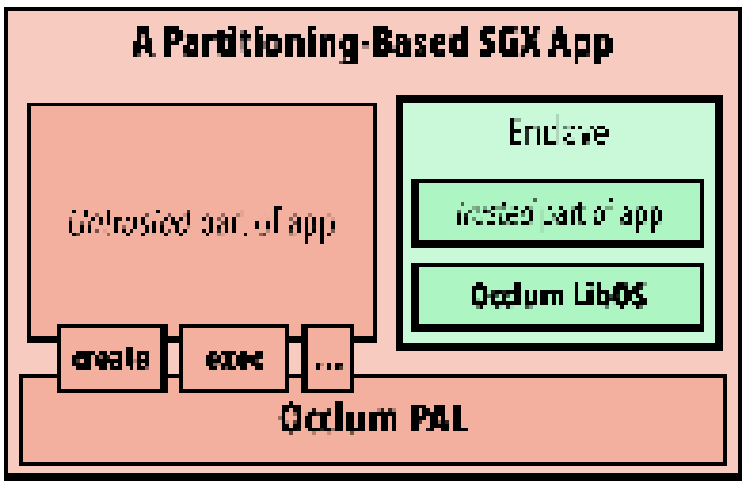
蚂蚁集团
ANT GROUP

The *First* Open-Source Project from China

+=

A Linux Foundation project
that aims at accelerating
the adoption of confidential computing

Occlum Embedded Mode



- **The embedded mode** allows users to build partitioning-based SGX app with Occlum
  - Occlum is embedded as a shared library in the user app
  - Cross-enclave communication through shared memory or host unix domain sockets
  - Achieving the same level of TCB and flexibility as the SDK-based approach

蚂蚁集团 ANT GROUP

Abstracting Enclaves

HW Enclaves are great, although users still want to:

- Have a uniform enclave abstraction
- Run confidential apps on existing hardware in their data centers
- Have more control over enclave launch & attestation
- Mitigate side channel attacks, to some extent

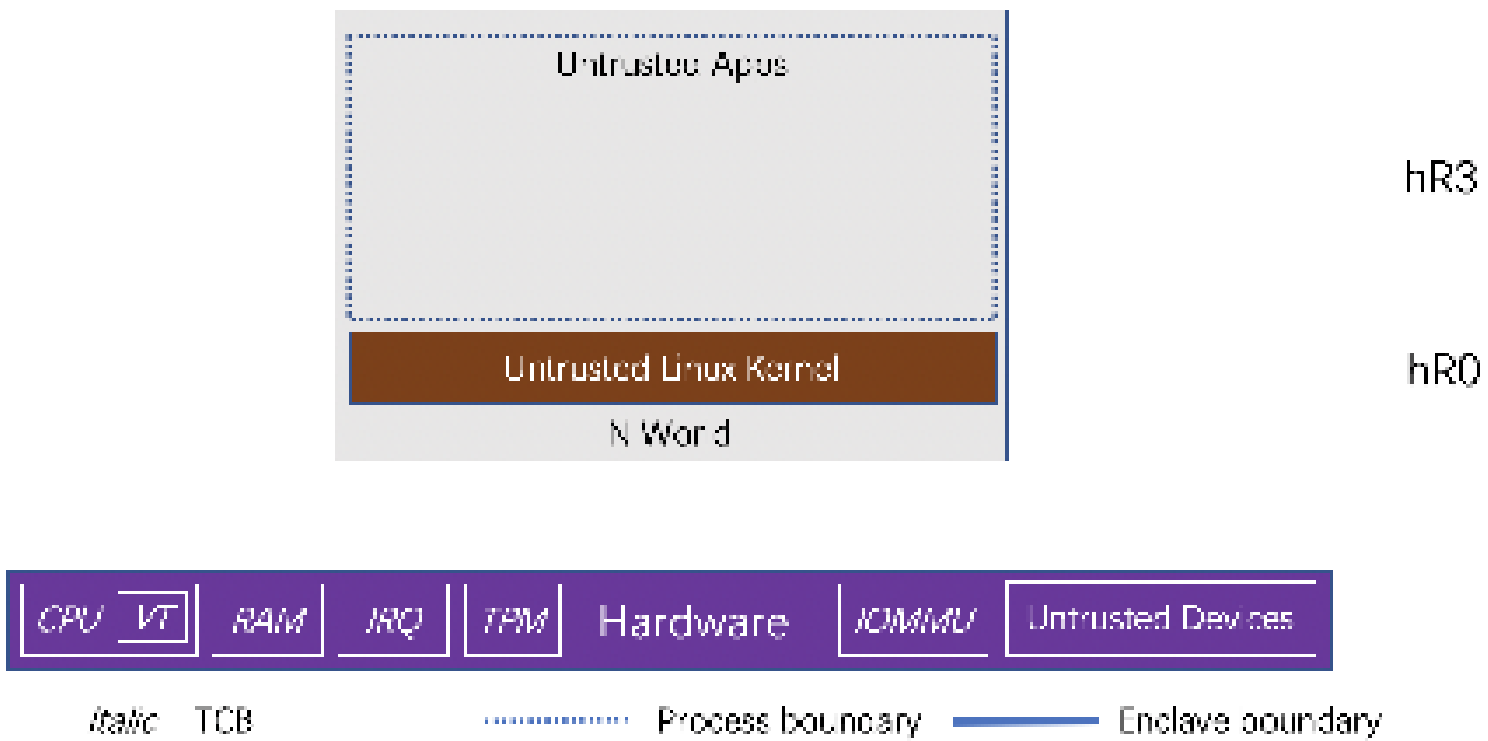
蚂蚁集团
ANT GROUP

HyperEnclave

HyperEnclave is a uniform enclave platform

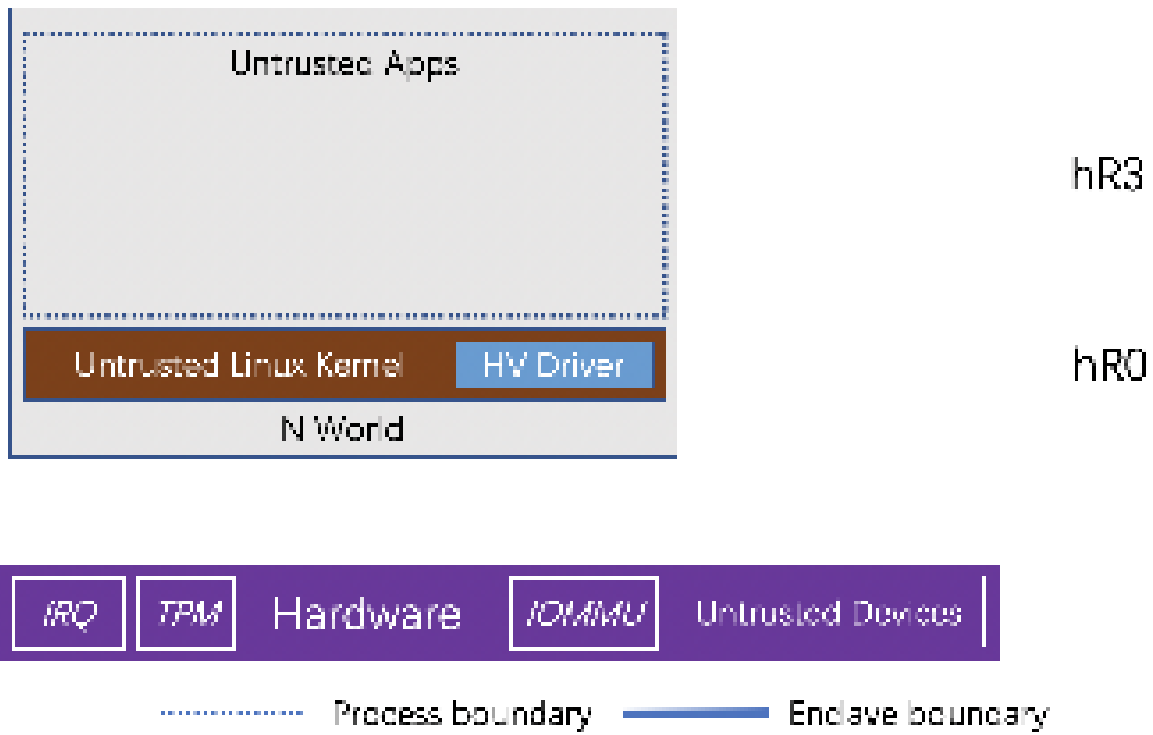
- Support programming models of de-facto Enclave SDKs
- Easily map to existing HW Enclaves and take advantage of future HW capabilities
- *Also support legacy platforms w/o HW Enclave extensions*

Architecture: Type-1.5 Hypervisor(Before Loading)



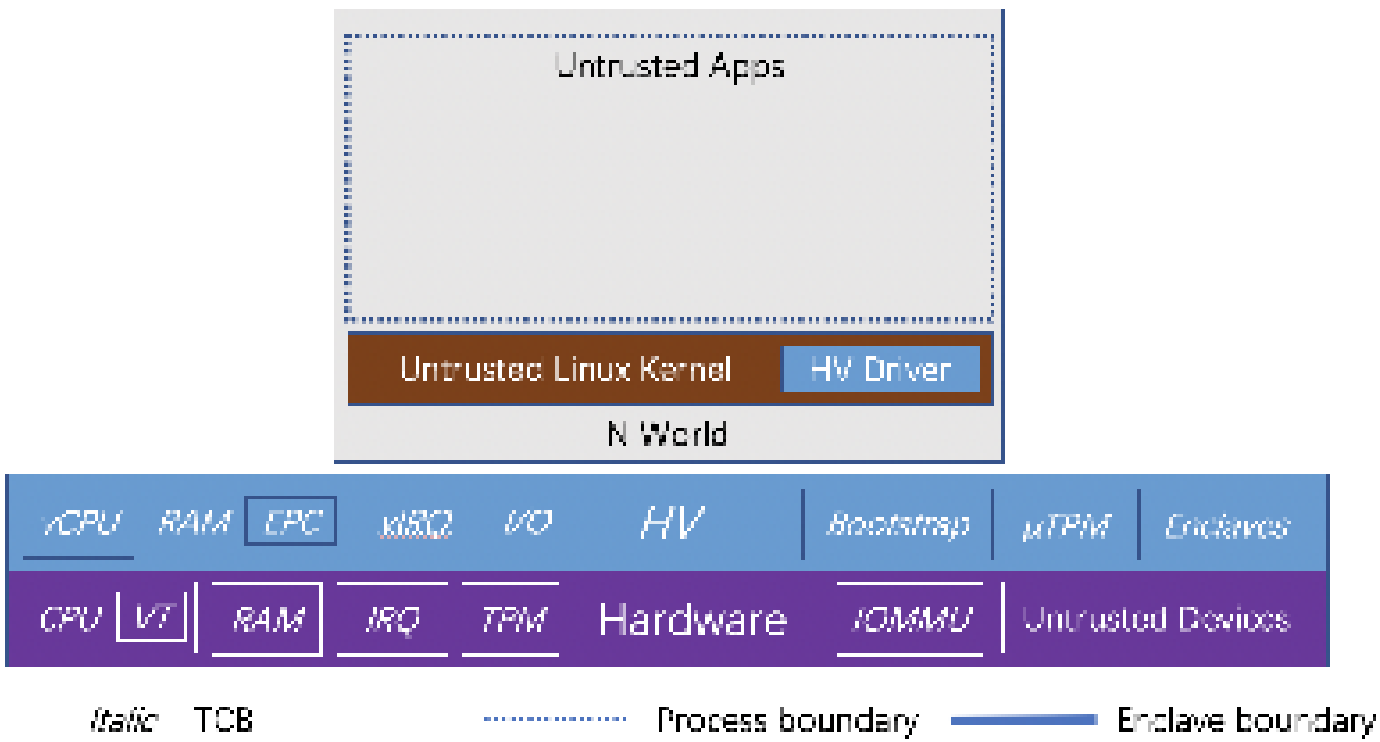
蚂蚁集团
ANT GROUP

Architecture: Type-1.5 Hypervisor (Loading)



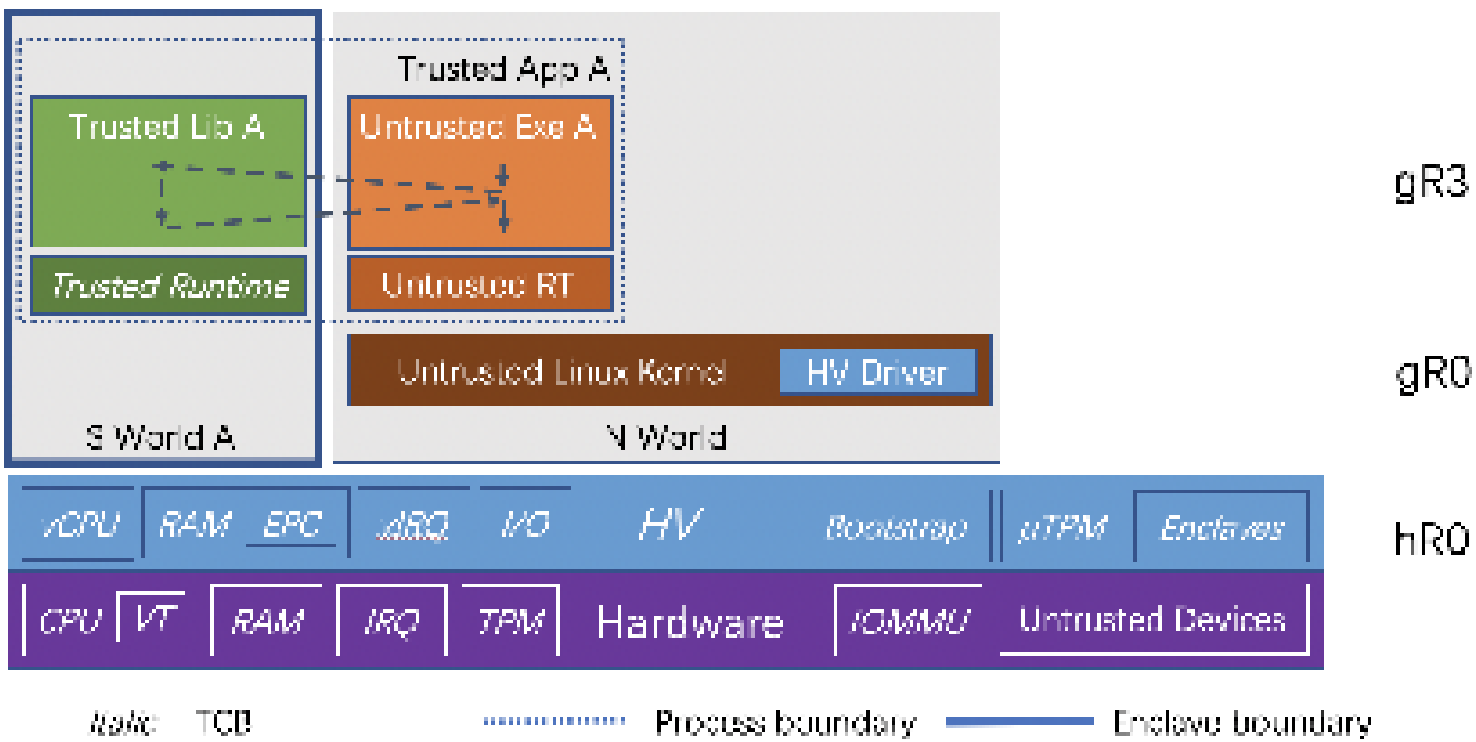
蚂蚁集团
ANT GROUP

Architecture: Type-1.5 Hypervisor(After Loading)



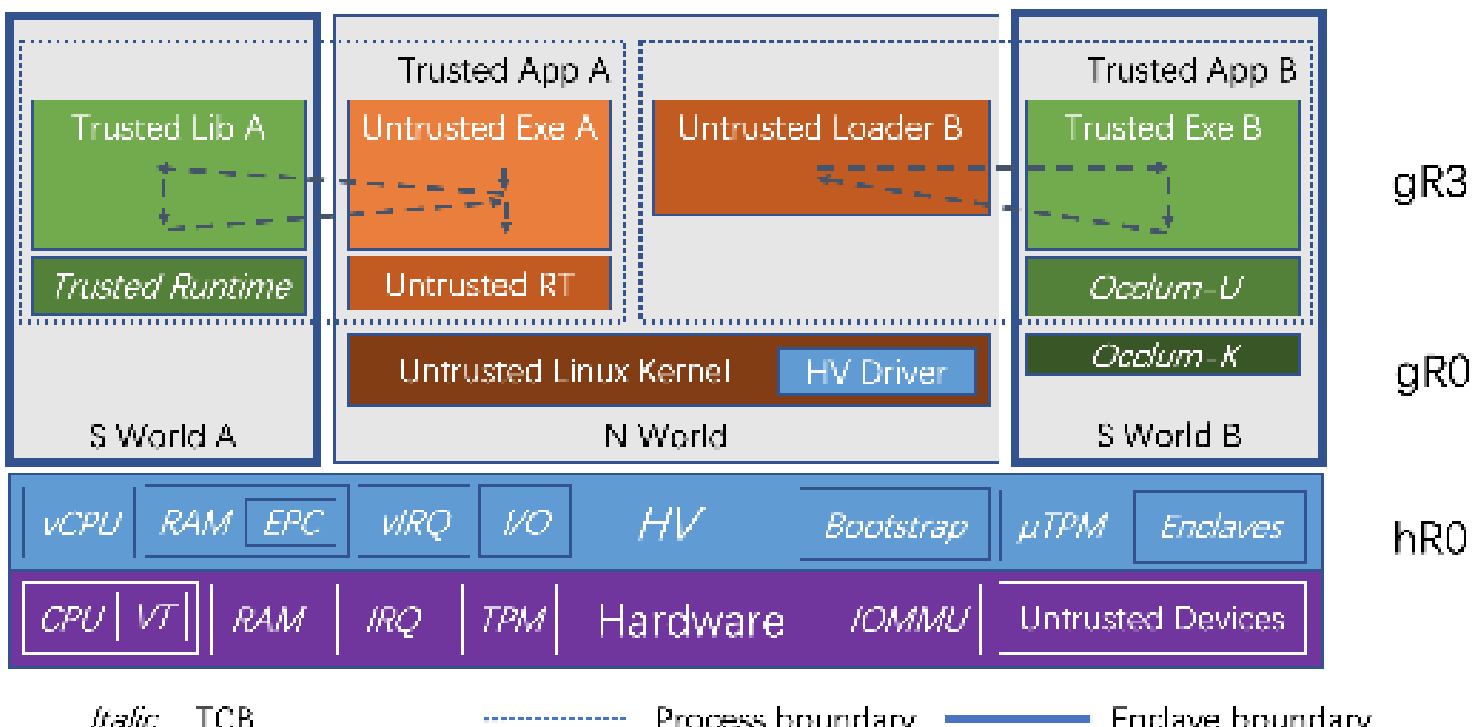
蚂蚁集团
ANT GROUP

Architecture: Programming Model (1)



蚂蚁集团
ANT GROUP

Architecture: Programming Model (2)



蚂蚁集团 ANT GROUP

Characteristics Recap

Trusted launch and attestation with TPM/TXT

Security first design principle

- Minimal TCB hypervisor → eventually formally verified
- Memory safety from rust
- Side channel mitigations

Ecosystem friendly

- Type 1.5
- In concert with KVM (which runs along with the demoted Linux host)

Take advantage of future HW memory encryption capabilities such as Intel MKTME

Scaling Enclaves, in Cloud-Native Manners

Kubernetes Cluster

- Maintain and deploy the TEE hardware in a cloud native manner
- Benefit from Kubernetes auto-scaler
- Benefit from Kubernetes monitor and services

Kubernetes + TEE = ?

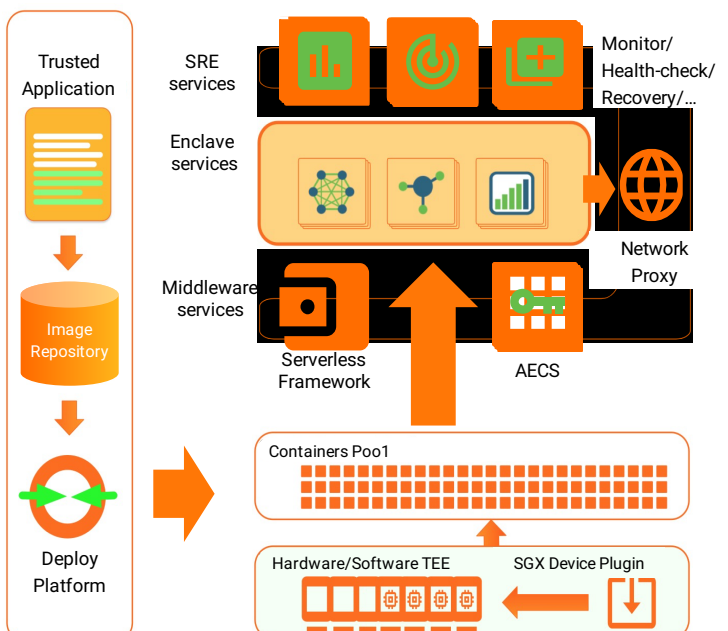
- Differentiate HW with and without enclaves
- Expose TEE device to containers
- Monitor and manage TEE resources
- Handle TEE specific logistics like remote attestation

蚂蚁集团
ANT GROUP

KubeTEE = Kubernetes + TEE

Simplify the DevOps workflow of confidential computing clusters

- Don’t worry about any hardware things
- Easily deploy the Enclave services
- Enclave specific middleware services
- Offer SRE services to simplify runtime maintenance

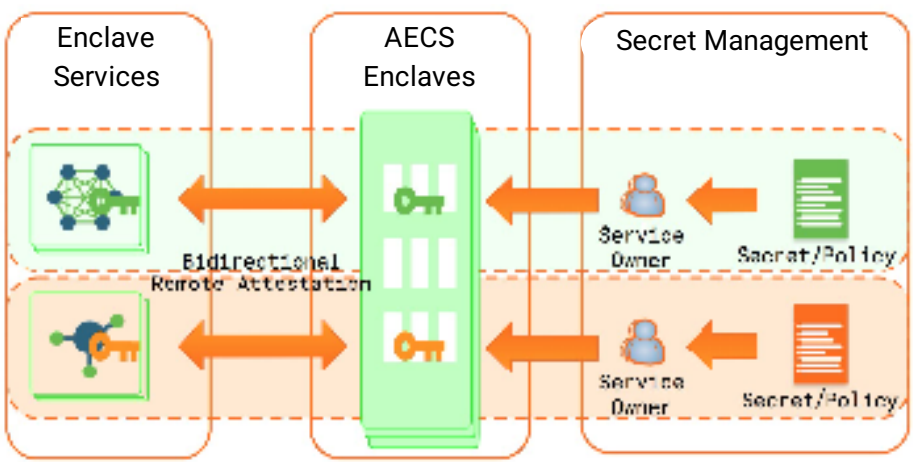


蚂蚁集团 ANT GROUP

AECS - Attestation Based Enclave Configuration Service

Bring your own secrets and policies for Enclave Services

- Create/protect/dispatch secrets *for* Enclaves and *with* Enclaves
- RA-based enclave service authentication (without the need of access keys)

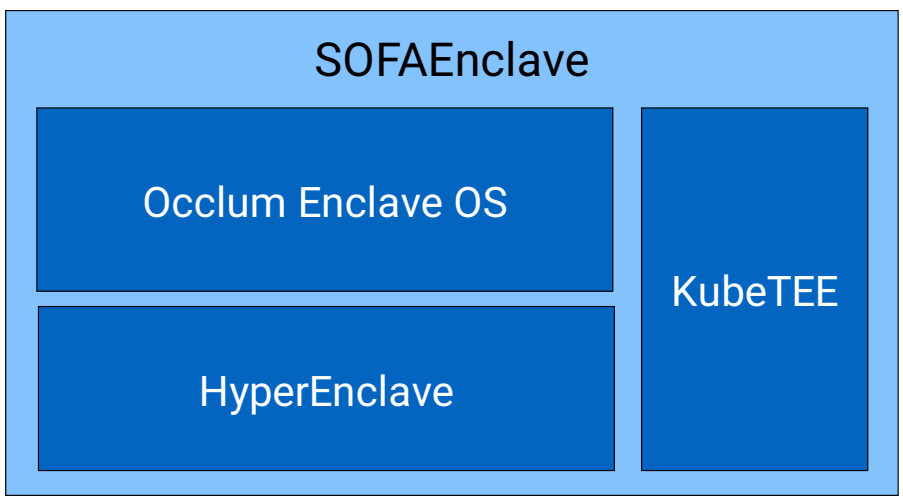


蚂蚁集团 ANT GROUP

Confidential Computing Made Easy

Open source projects

Call for collaboration



蚂蚁集团
ANT GROUP

蚂蚁安全计算校招&社招&合作

- **我们的使命** 研发独创性的安全底层技术，打造金融级可信基础设施，为亿万客户和海量数据保驾护航
- **我们的团队**
  - 有战斗力的集体，均毕业于国内外顶尖高校
  - 原创技术的摇篮，曾多次在顶级学术会议上发表论文
  - 业务快速发展，成长空间巨大
- **我们希望你**
  - 大学本科或以上学历，计算机或相关专业
  - 熟悉如下编程语言语言中的至少一种：C/C++、Rust和Go
  - 熟悉如下技术中至少一种：操作系统、虚拟化、TEE、编译器、体系结构、安全攻防、可信计算、程序验证等
  - 现有研究成果优秀者优先
- **工作地点** 北京、上海、杭州
- **联系方式**

shoumeng.ysm@antfin.com

微信 32713933