Occlum

THE LINUX FOUNDATION PROJECTS

CONFIDENTIAL COMPUTING CONSORTIUM

Occlum Annual Review

Chunyang, Hui

Occlum Team
Ant Group

Contents

- Occlum Intro
- Occlum Current Status
- Occlum Updates

Occlum

Empowering everyone to run every app in enclaves

Occlum | THE LINUX FOUNDATION PROJECTS CONFIDENTIAL COMPUTING CONSORTIUM

Empowering Everyone to run every app in TEEs

- A memory-safe, multi-process library OS for TEEs
- Created by Ant Group in 2019 ANT GROUP
- *Occlum: Secure and Efficient Multitasking Inside a Single Enclave of Intel SGX (ASPLOS' 20)*
- Donated to CCC (Confidential Computing Consortium of Linux Foundation) in 2021
- Compatible with multiple TEE platforms including Intel SGX, HyperEnclave (ATC' 22) and Intel TDX (on-going)
- https://occlum.io | https://github.com/occlum/occlum

THE LINUX FOUNDATION PROJECTS

CONFIDENTIAL COMPUTING CONSORTIUM

Key Features

Efficient Multi-tasking

- Single-address-space architecture
- Multiple processes share the same enclave
- Super fast process startup and IPC

Memory Safety

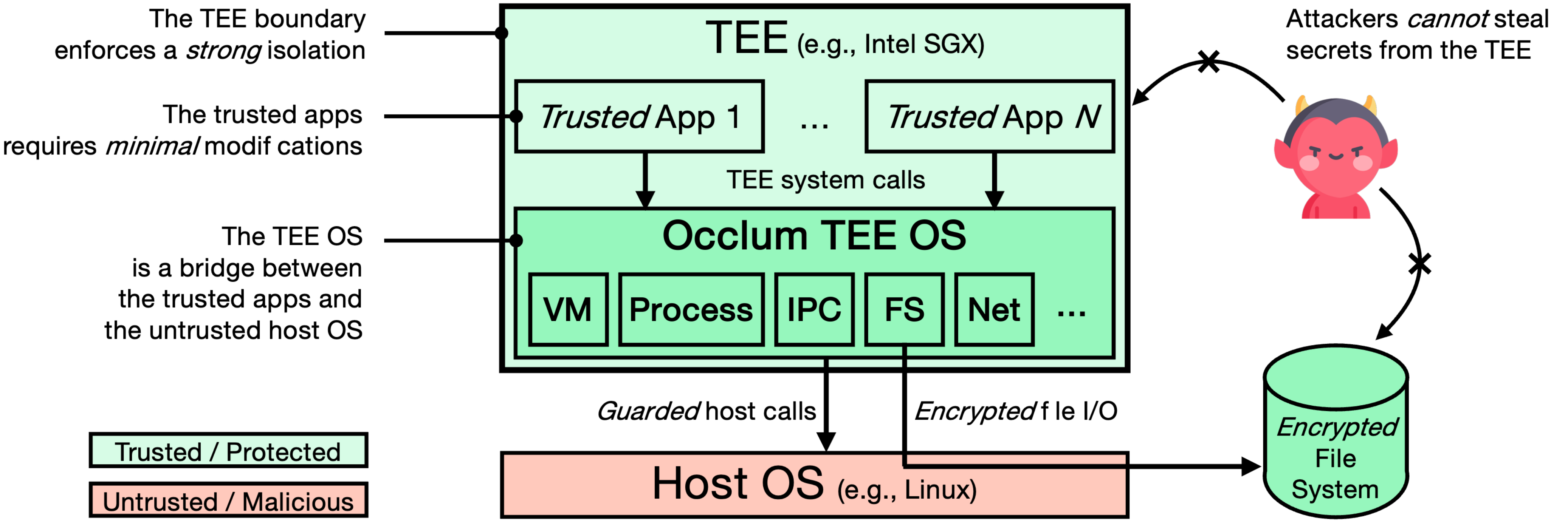
- First SGX LibOS written in Rust
- Rust is designed to be memory safe. It does not permit null pointers, dangling pointers, or data races

Ease of Use

- Empowering everyone to run apps in Enclave
- Similar user commands with Docker

Deeper Inside

Occlum Architecture



The TEE boundary enforces a *strong* isolation

The trusted apps requires *minimal* modifications

The TEE OS is a bridge between the trusted apps and the untrusted host OS

TEE (e.g., Intel SGX)

Trusted App 1 … *Trusted* App *N*

TEE system calls

Occlum TEE OS

VM | Process | IPC | FS | Net | …

Guarded host calls

Encrypted file I/O

Host OS (e.g., Linux)

Attackers *cannot* steal secrets from the TEE

Encrypted File System

🟩 Trusted / Protected

🟥 Untrusted / Malicious

https://github.com/occlum/occlum

THE LINUX FOUNDATION PROJECTS

Occlum

CONFIDENTIAL COMPUTING CONSORTIUM

Occlum Current Status

Status

- Technical charter update - No
- Progression status update - Incubation stage, no updates
- License update – No
- Budget allocations – None
- OpenSSF Best Practices Badge – Currently no, but on the TODO list

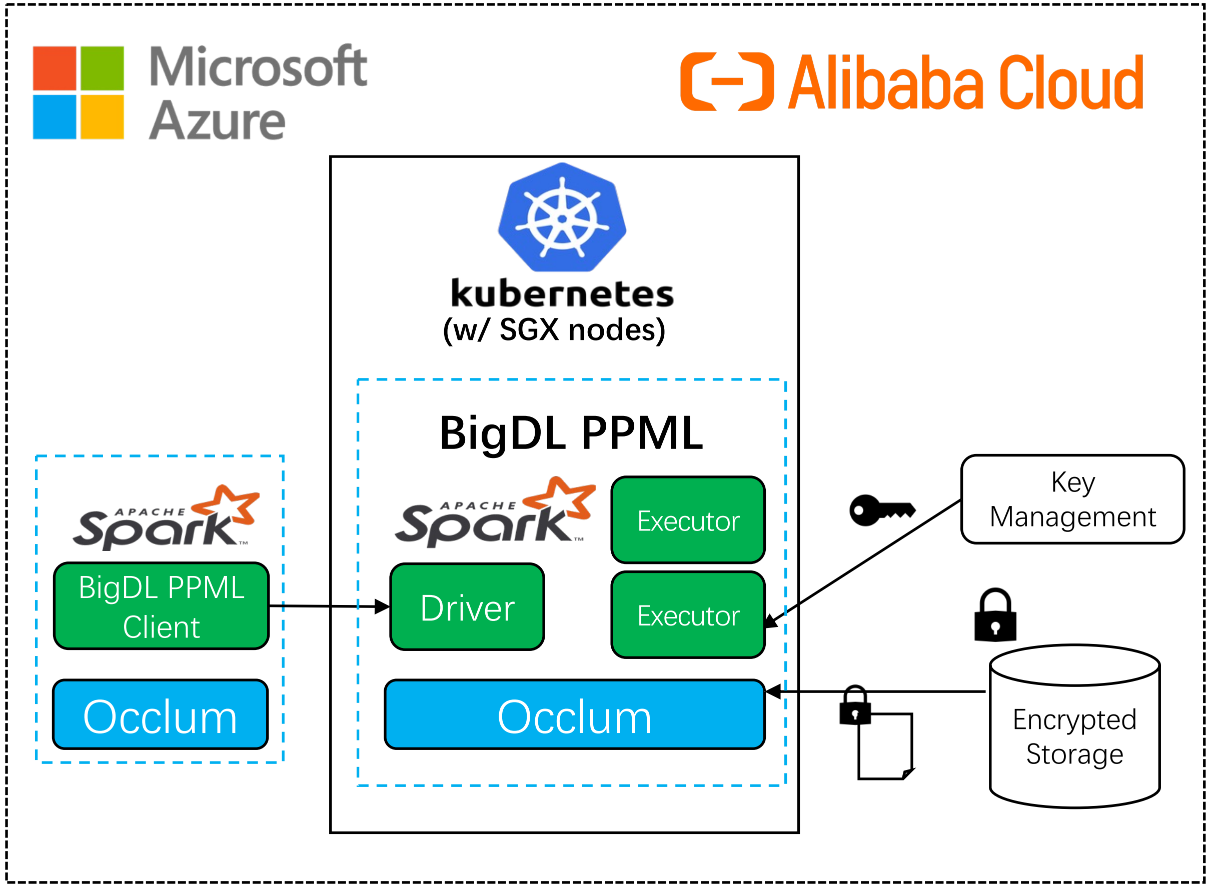
Occlum Update

New Demos

- LLM: ChatGLM2-6B
- MySQL
- Distributed PyTorch
- SWTPM, a software-based Trusted Platform Module (TPM) emulator based on libtpms
- PaddlePaddle, a simple, efficient and extensible deep learning framework
- …

Spark-with-Occlum Solution

Running Unchanged Spark Applications with End-to-End Protections



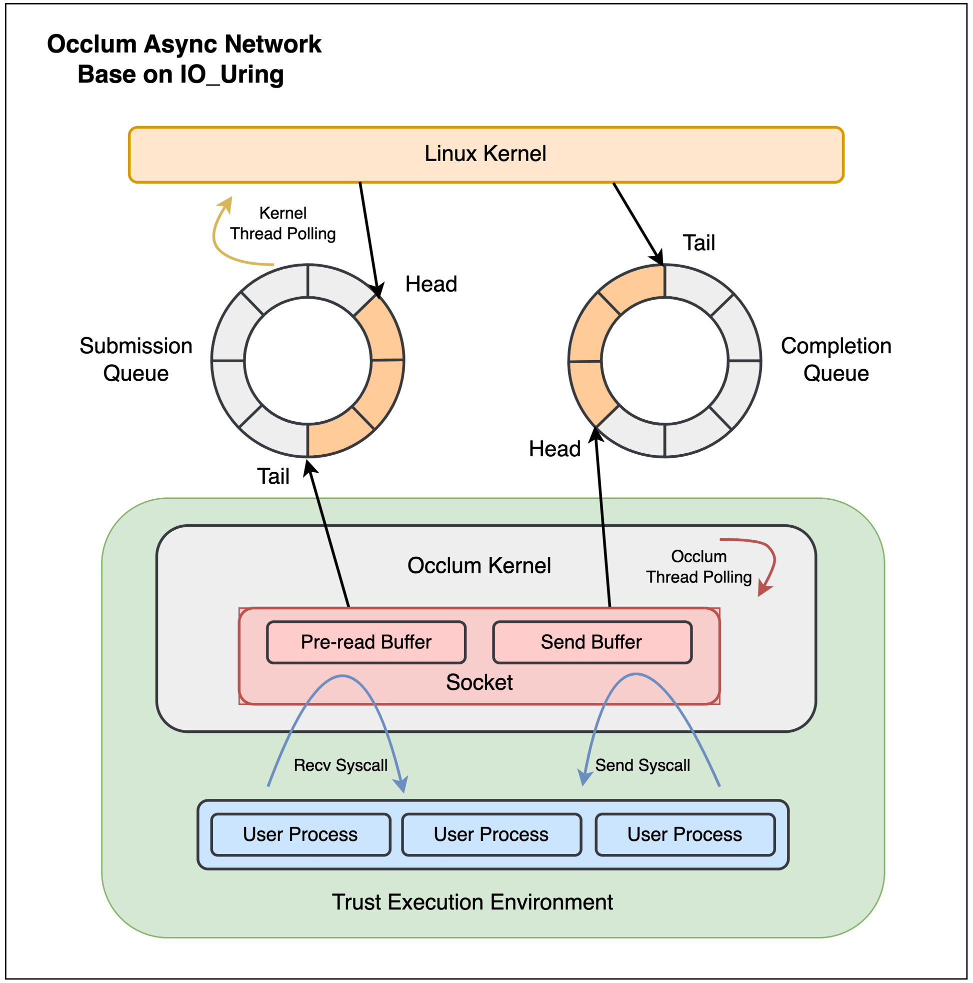
Running in SGX

- Joint work with Intel BigDL team
- Helps users migrate existing big data /distributed applications to end-to-end secure environments
- Applied in the real-world business of Ant Group, including the AntChain MOSS Privacy Computing Platform

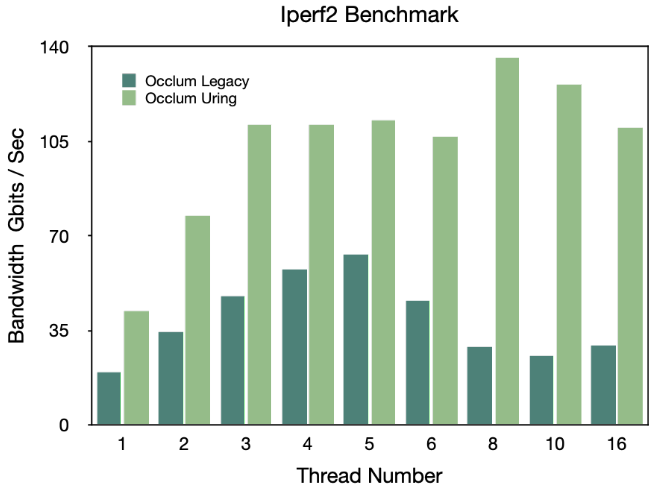
EDMM

- With the newly added instructions in SGX 2, dynamically increase, reduce, or modify the permissions of the enclave‘s EPC pages during runtime
- #PF based on-demand commit, Page level management, New user space memory layout
- Higher security, Faster startup time, Better user experience
- With Spark GBT demo, total time decrease 11.3%, startup time decrease over 90%
- Under evaluation by several internal customer of Ant Group

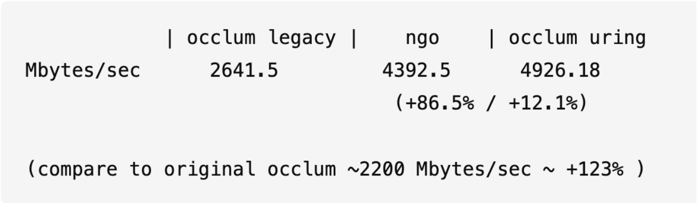
IO URING



Asynchronous Network Arch



Iperf2



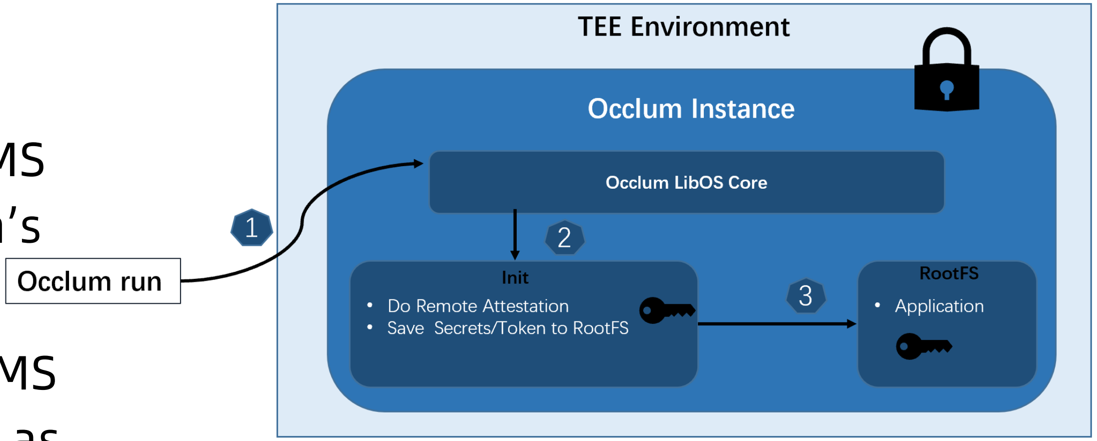
```
             | occlum legacy |    ngo    | occlum uring
Mbytes/sec       2641.5           4392.5       4926.18
                                   (+86.5% / +12.1%)

(compare to original occlum ~2200 Mbytes/sec ~ +123% )
```

Iperf3

- Significantly reduces context switching overhead
- Support for Asynchronous & Synchronous Syscalls
- Seamless user experience and optimized resource utilization
- TEE High performance I /O

Init-RA Solution

- Designed an unique “Occlum -> init ->application” boot flow
- The Init-RA solution puts remote attestation based KMS client into the init stage without involving application’s change
- Template config file is provided to users to define: KMS server, keys required and verifying components such as mrsigner, mrenclave, etc.
- Two Init-RA solutions provided, GRPC-RATLS and AECS



https://occlum.readthedocs.io/en/latest/remote_attestation.html#init-ra-solution

Others

- Security: PKU (Protection Keys for User space)
- Functionality
  - AMX (Advanced Matrix Extensions)
  - System-V and POSIX Shared memory
- Stability: Fully-automated CI/CD based on GitHub Actions
- Document: Official website https://occlum.readthedocs.io/en/latest/

Community

- Occlum GitHub community - 1.3K + stars, 200 + forks
- Occlum WeChat community – 130+ members
- 2023 Occlum Beijing Meetup – 20+ developers on site, 700+ viewers on line

Thank you !