Occlum

THE LINUX FOUNDATION PROJECTS

CONFIDENTIAL COMPUTING CONSORTIUM

Occlum 2025 Annual Review

Chunyang, Hui

GitHub: @jessehui
Occlum Team
Ant Group

Contents

- Occlum Intro
- Occlum Update
- Occlum Current Status

Occlum

Empowering everyone to run every app in enclaves

Empowering Everyone to run every app in TEEs

- A memory-safe, multi-process library OS for TEEs
- Created by Ant Group in 2019
- *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
- https://occlum.io | https://github.com/occlum/occlum

Occlum

THE LINUX FOUNDATION PROJECTS

CONFIDENTIAL COMPUTING CONSORTIUM

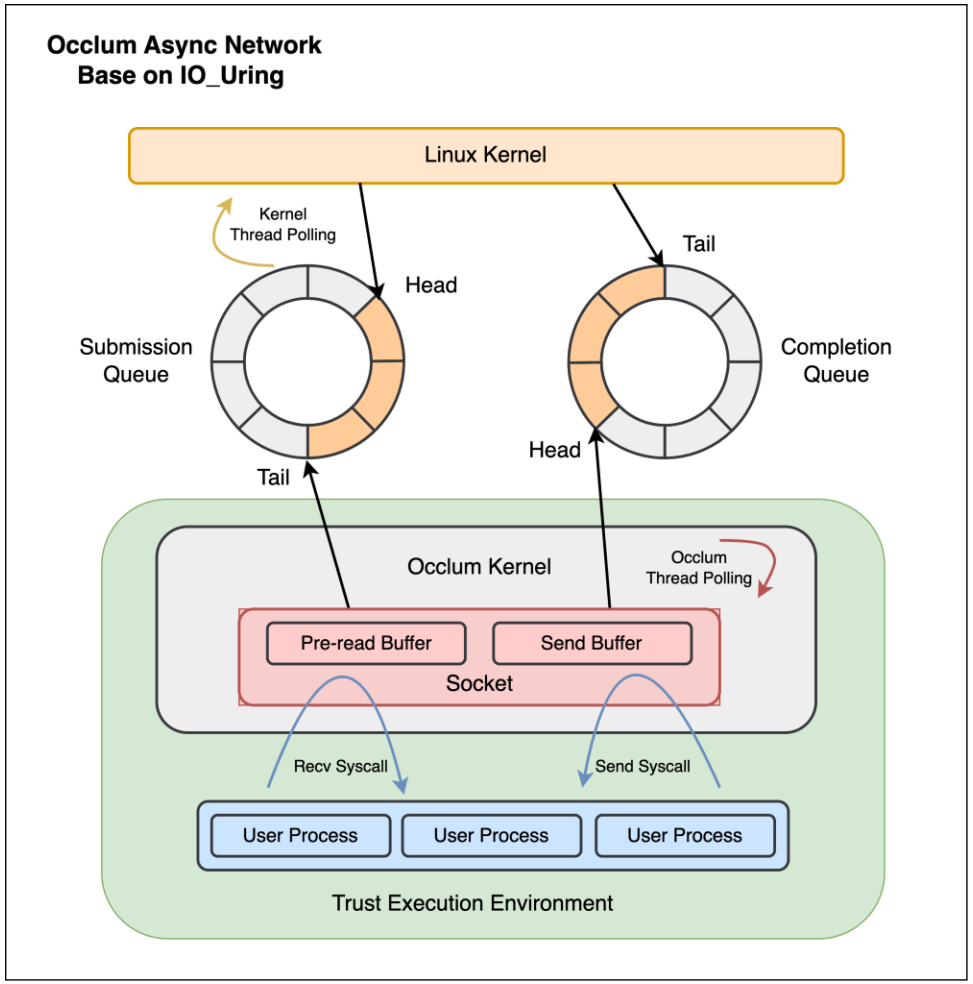
Occlum Update

New Release

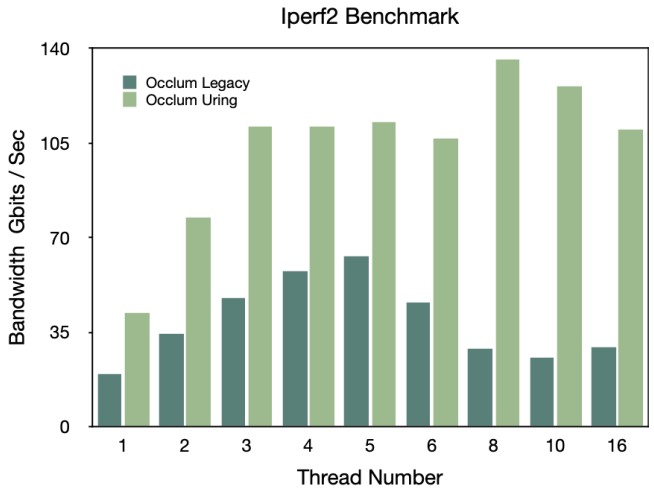
v0.31.0 Release

- IO_Uring based Network IO to improve performance by 40%+
- Support configurable Ext2+MlsDisk
- Upgrade Intel SGX SDK v2.21 and get performance improvement from Intel PFS (50%+ in FIO benchmark)
- Support ubuntu 22.04 and Glibc 2.35
- Support Flink K8s deployment demo

Network IO with 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%)

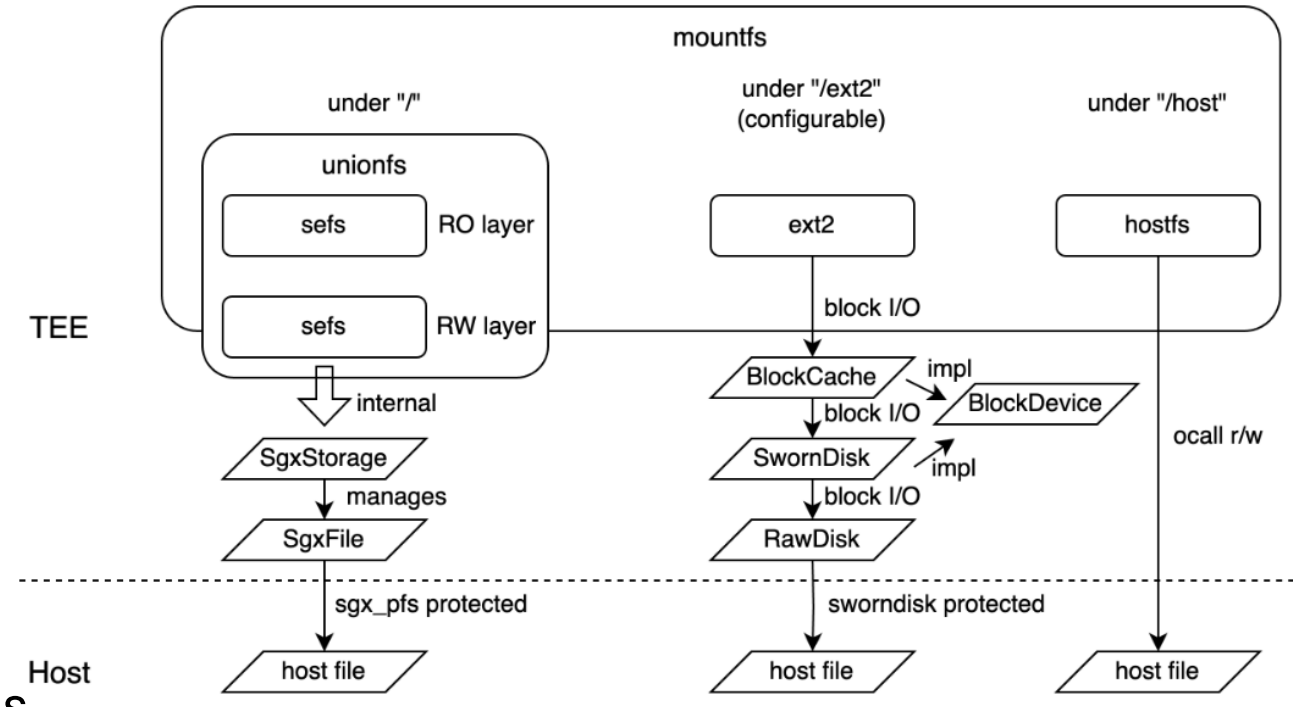
Iperf3

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

Ext2-rs and MlsDisk

- Occlum SEFS (Simple Encrypted File System) built on Intel PFS (Protected File System) has some limitations in terms of performance (especially in writing) and security
- Developed by Ant Group, an option to replace Intel PFS and Occlum SEFS
- Achieve better performance with multilayered log-structured design
- Provide better security in atomicity (AtomicDisk: A Secure Virtual Disk for TEEs against Eviction Attacks – FAST'25)

Occlum rootfs arch



Ext2-rs and MlsDisk

- Occlum SEFS (Simple Encrypted File System) built on Intel PFS (Protected File System) has some limitations in terms of performance (especially in writing) and security
- Developed by Ant Group, an option to replace Intel PFS and Occlum SEFS
- Achieve better performance with multilayered log-structured design
- Provide better security in atomicity (AtomicDisk: A Secure Virtual Disk for TEEs against Eviction Attacks – FAST'25)

fio (mb/s) 10gb	seq-write	rnd-write-4k	seq-read	rnd-read-4k
sefs	103	22.7	324	67.2
sefs-opt	156	45.5	771	150
ext2+sworndisk	575	390	737	164

filebench (mb/s)	varmail	fileserver	oltp	videoserver
sefs	7.1	116.1	98.1	31.6
sefs-opt	10.1	173.8		
ext2+sworndisk	52.2	197.4	160.7	42.8

Occlum

THE LINUX FOUNDATION PROJECTS

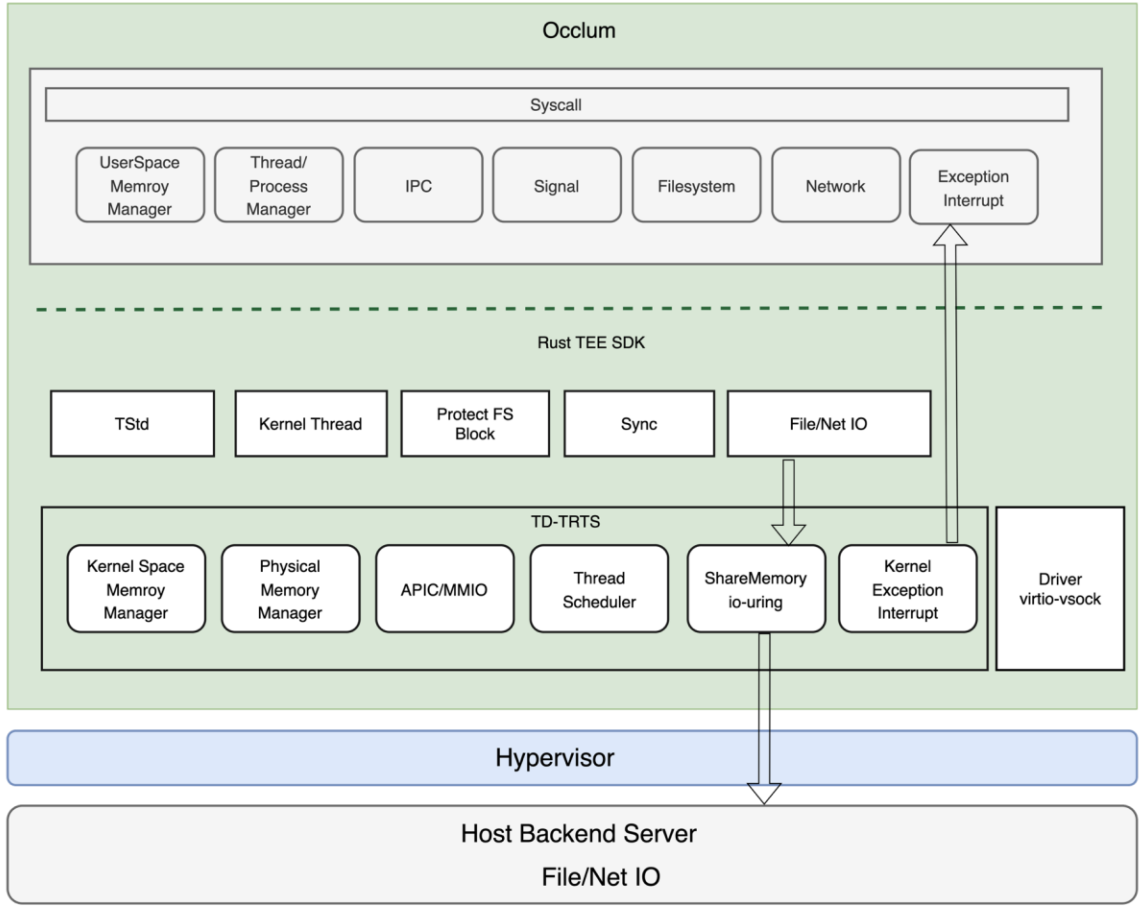
CONFIDENTIAL COMPUTING CONSORTIUM

Occlum for TDX

Overview

- Background:
  - VM-Based TEE emerging
  - Linux is an option for CVM but not the final answer
- Target
  - Support more functionalities as a general OS
  - Smaller TCB than Linux
  - Multiple-TEE platforms support with single code base
- Challenge
  - Reuse Occlum code (Ring 3 -> Ring 0)
  - Address all previous constraints due to unikernel architecture
  - find way to handle ocall

Architecture

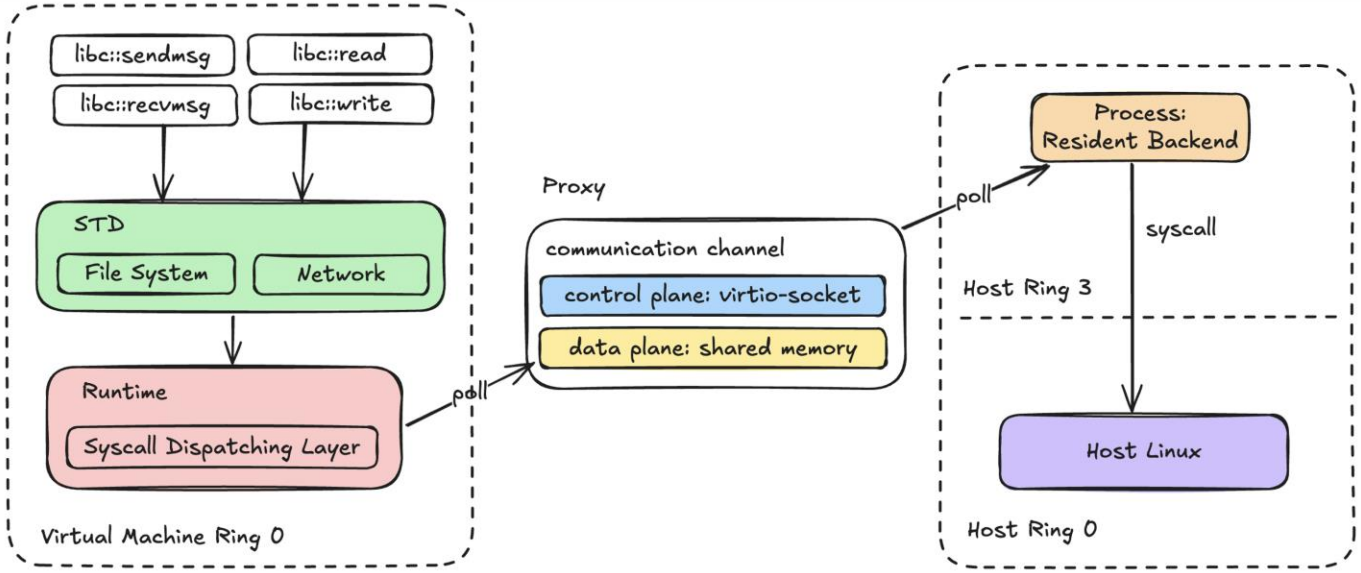


Kernel services	The kernel services module forms the foundational layer of the system, implementing critical kernel functionalities
SDK	The kernel SDK layer provides a Rust STD-like library that enables developers to build custom applications or kernel services running directly in ring 0 (kernel mode).
Runtime	The kernel runtime operates at the lowest level, interfacing directly with hardware and platform-specific features.

- The layered design abstracts platform and services for decoupling and code reuse.

First Step

- Layered arch: TEE-trts, TEE-std, occlum
- Page table management, fork
- Support page-cache and shared memory
- Ocall to Virtio request



Current Status

- Bootable on normal VM and TDX CVM
- Support most of the syscalls and capabilities Occlum-legacy support
- Support unmodified bash, redis, nginx
- Open source in progress

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 – Still in progress. Update needed.

Occlum

THE LINUX FOUNDATION PROJECTS

CONFIDENTIAL COMPUTING CONSORTIUM

Thank you !