Occlum Annual Report 2022

CCC TAC meeting, 2022/11

Dr. Hongliang Tian (Tate)

System Architect, Confidential Computing Team, Ant Group

tate.thl@antgroup.com

Occlum is a memory-safe, multi-process LibOS for Intel SGX

Linux Compatibility

- ✓ 150+ Linux system calls
- ✓ Multiple processes
- ✓ Multiple types of file systems
- ✓ Musl and glibc
- ✓ All popular languages, e.g., C/C++, Java, Python, Go, and Rust

Friendly Interface

```
$ occlum new my_occlum_instance
$ cd my_occlum_instance
$ cp ../my_app image/bin/
$ occlum build
$ occlum run /bin/my_app
```

Memory Safety

with Rust

Confidential Computing Consortium

3+ years of development

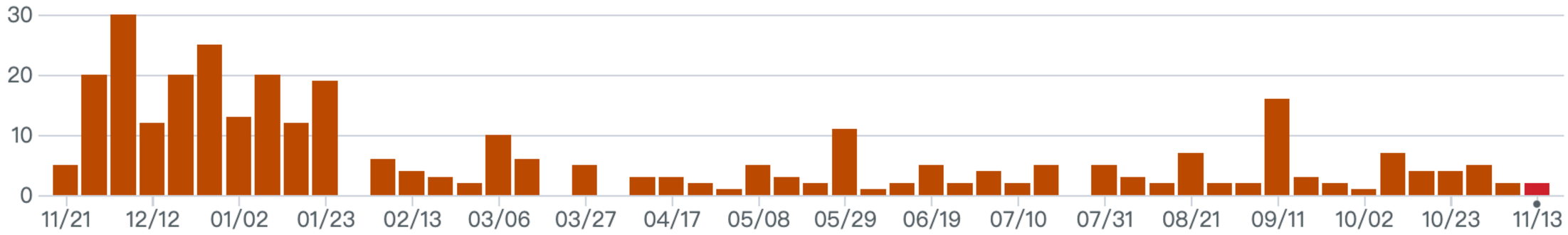
40+ releases

Occlum’s major achievements in 2022

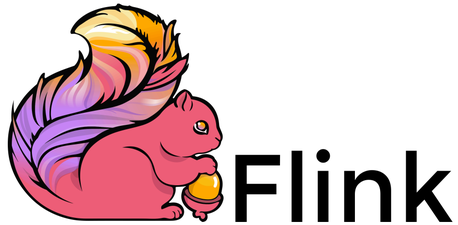
Reaching the milestone of 1K Github stars

https://github.com/occlum/occlum

- **1K+** Github stars
- **100+** forks
- **40+** contributors
- **350+** commits over the last 12 months



Enabling popular and complex applications

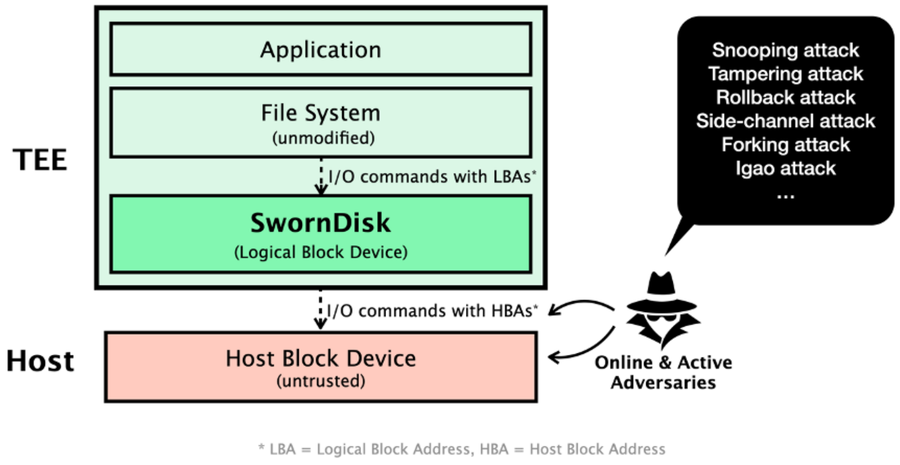


...

Performing fast file I/O with SwornDisk

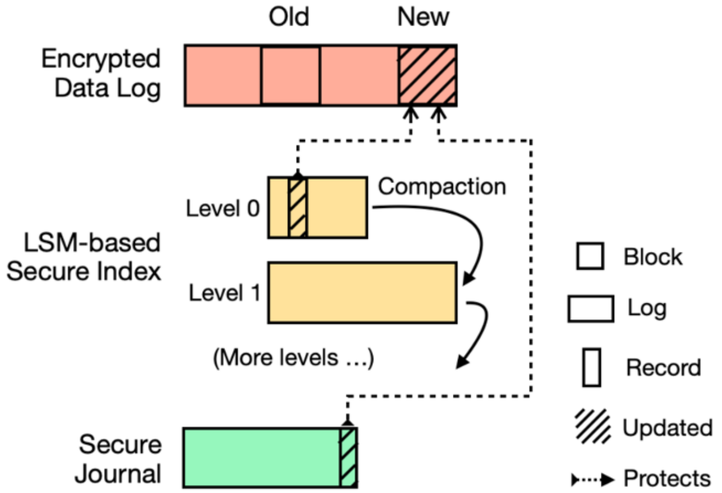
- SwornDisk is a log-structured secure block device
- Our insight is that *logging is not only more friendly to storage medium, but also to security protection*.

The threat model



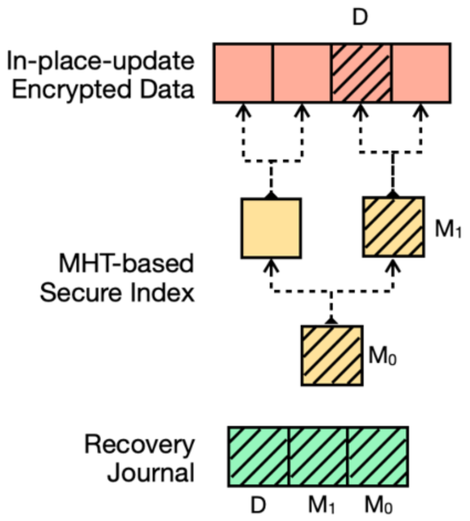
The log-structured approach

(SwornDisk)



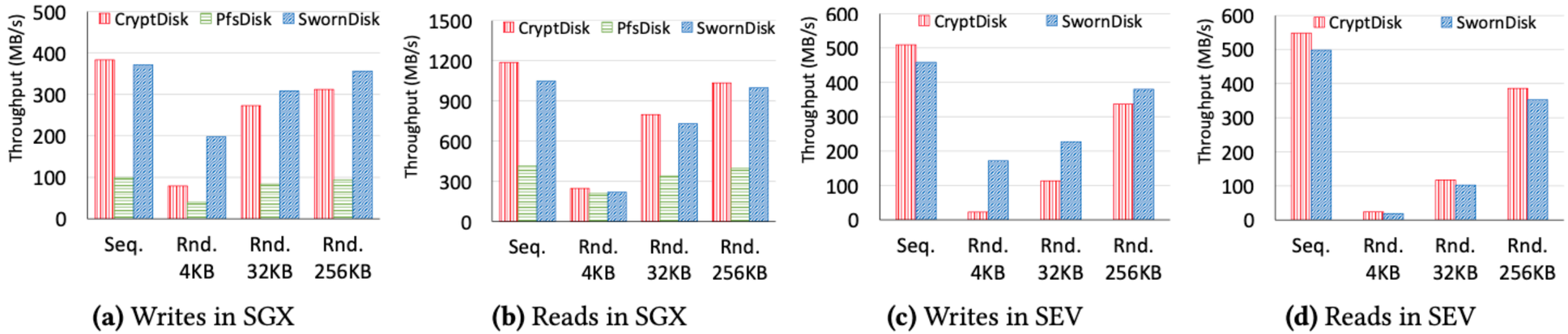
The traditional approach

(In-place updates + MHT)



Performing fast file I/O with SwornDisk

- SwornDisk is a log-structured secure block device
- Our insight is that *logging is not only more friendly to storage medium, but also to security protection*.
- Microbenchmark results with fio (3.6X-5.0X speedups for writes compared to Intel SGX PFS)



(a) Writes in SGX (b) Reads in SGX (c) Writes in SEV (d) Reads in SEV

- Will be merged into Occlum v1.0

Launching v1.0 by the end of 2022

- The version 1.0 will be based on Next-Gen Occlum (NGO) project, which has been developed in parallel to the mainline Occlum.
- NGO has major performance improvements over the mainline Occlum

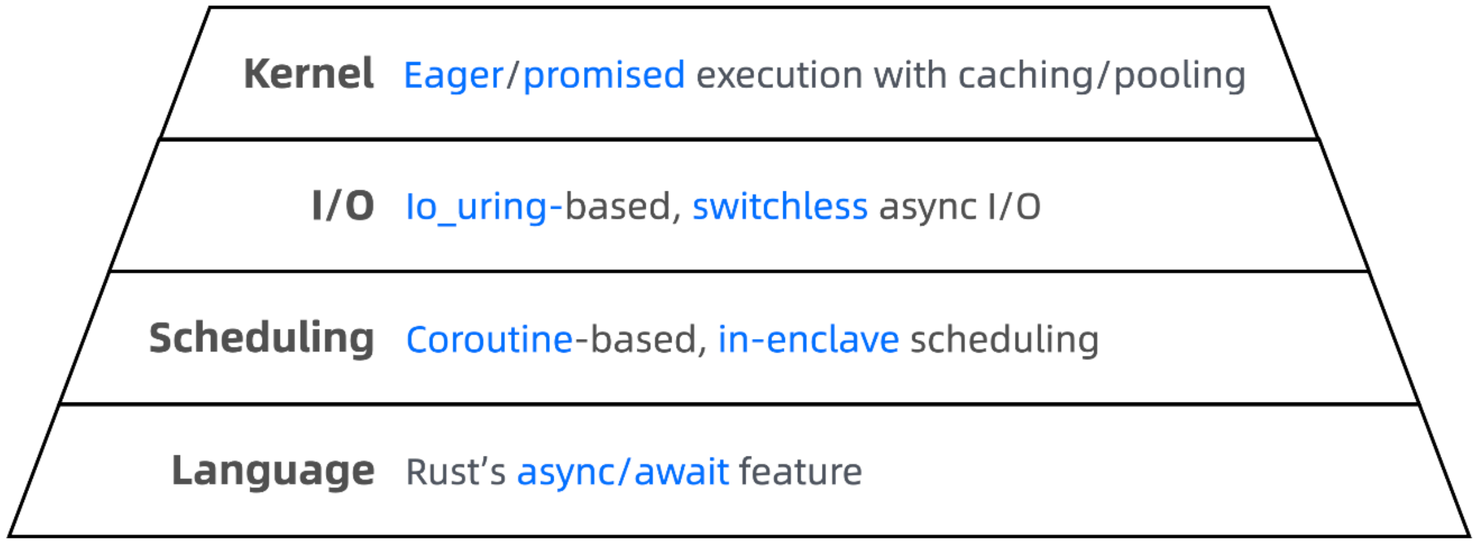


FIG. NGO adopts an *asynchrony*-centric design to boost performance

Items required by Annual Review Process

- Review any changes Project Charter
  - No
- Review the project's progression status
  - Still in the Sandbox Stage
  - May apply for the Incubation Stage next year
- Review any budget allocation
  - I am not aware of any budget assigned to Occlum...
- Review license scans provided by the Linux Foundation
  - N/A

- By the way, Occlum needs a new mentor...

Occlum

https://github.com/occlum/occlum