CCC TAC Submission: Occlum

Name of Project

Occlum

Project Description

Occlum is a *memory-safe*, *multi-process* library OS (LibOS) for Intel SGX. As a LibOS, it enables *legacy* applications to run on SGX with *little or even no modifications* of source code, thus protecting the confidentiality and integrity of user workloads transparently.

Compared with other SGX LibOSes, Occlum has the following four salient features:

1. Container-inspired interface;
2. Efficient multitasking;
3. Full file system support;
4. Memory safety.

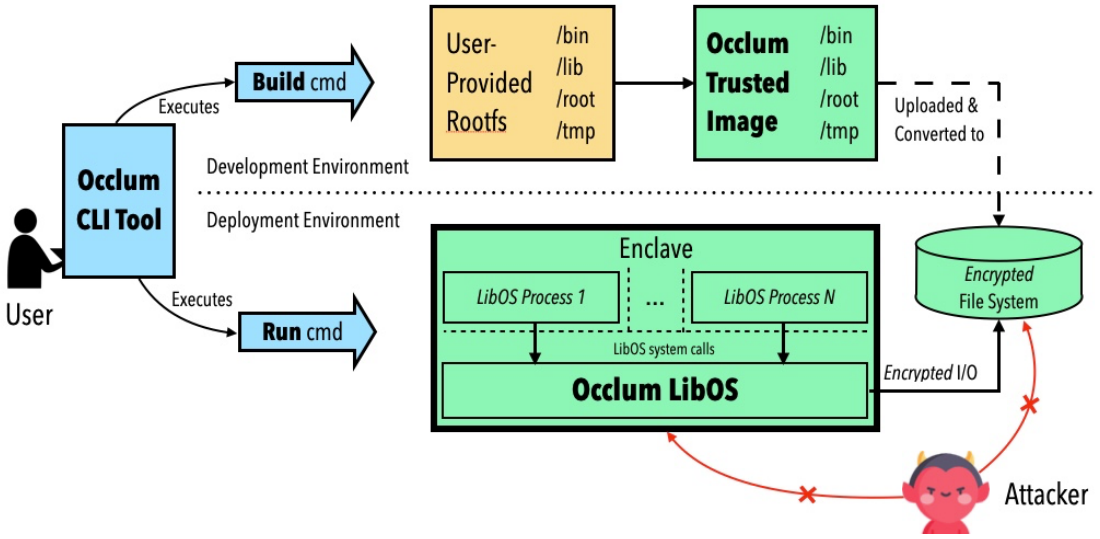

Figure. The architecture of Occlum.

Overall, we believe Occlum presents a unique set of features and tradeoffs that are valuable to the communities of Intel SGX and confidential computing.

Container-Inspired Interface

Occlum offers a user-friendly command-line interface, bringing the familiar Docker-like experience to the users. Running a hello world program on Occlum inside SGX enclaves is as simple as typing several commands:

```
occlum-gcc hello_world.c -o hello_world
```

```
occlum init
cp hello_world image/bin && occlum build
occlum run /bin/hello_world
```

With the user experience demonstrated above, we believe Occlum has greatly lowered the barriers to entry in confidential computing for application developers.

Efficient Multitasking

Occlum offers light-weight LibOS processes: they are light-weight in the sense that all LibOS processes share the same SGX enclave. Compared to the heavy-weight, per-enclave LibOS processes, Occlum's light-weight LibOS processes is up to 1,000X faster on startup and 3X faster on IPC. See our paper published on ASPLOS'20 for details.

Full File System Support

File systems are critical to virtually every application. Occlum supports various types of file systems, e.g., read-only hashed FS (for integrity protection), writable encrypted FS (for confidentiality protection), untrusted host FS (for convenient data exchange between the LibOS and the host OS).

Memory Safety

Occlum is the first SGX LibOS written in a memory-safe programming language (Rust). Thus, Occlum is much less likely to contain low-level, memory-safety bugs and is more trustworthy to host security-critical applications.

How does this project align with the Consortium's Mission Statement

The vision of Occlum is to "empowering everyone to run every app inside enclaves". This goal is well aligned with CCC's mission of "accelerate the adoption of Trusted Execution Environment (TEE) technologies and standards."

Project synergy with existing projects under the CCC

Occlum's relationship with other projects under CCC:

1. Intel SGX SDK. Currently, Occlum is based on Intel SGX SDK.
2. Open Enclave SDK. We are considering migration to Open Enclave SDK for portability on more TEE platforms.
3. Trusted Compute Framework (TCF). Occlum is integrating with TCF as an alternative LibOS backend.

4. Graphene-SGX. Occlum is an alternative to Graphene-SGX that offers a different set of tradeoffs, thus giving the users more choices. As LibOSes, both projects have some common interests, e.g., FSBASE/GSBASE enabling in Linux kernel, preventing/mitigating Iago attacks against host calls.

Currently, Occlum is based on Intel SGX SDK. Occlum would continue using Intel SGX SDK which would bring the latest security update. At the meantime, Occlum would try Open Enclave SDK in the near future, which would bring Occlum to more security platforms.

- Occlum is a secure libOS on the top of security SDKs
- Occlum is a portable libOS. Currently it works on Intel(R) SGX, in the future it would be ported other platforms.
- Occlum provide an open platform for unmodified/limited modified applications. It helps people to use confidential computing easily

Trusted Computing Base (TCB) of the project.

Occlum is a libOS on top of security SDK (Intel SGX SDK or MSFT Open Enclave SDK). Currently Intel SGX SDK is the only used SDK.

Project website URL

https://occlum.io/

Project Code of Conduct URL

https://github.com/occlum/occlum/blob/master/CODE_OF_CONDUCT.md

Source control URL

https://github.com/occlum/occlum

Issue tracker URL

https://github.com/occlum/occlum/issues

Project Logo URL or attachment (Vector Graphic: SVG, EPS)

https://github.com/occlum/occlum/blob/master/docs/images/logo.png

Project license

https://github.com/occlum/occlum/blob/master/LICENSE

External dependencies

N	lib	license
1	Intel SGX SDK	BSD / Intel
2	Rsut SGX SDK	Apache
3	musl	MIT
4	gRPC	Apache
5	Protocol Buffers	BSD
6	rcore-fs	MIT
7	serde-sgx	Apache / MIT
8	ringbuf	Apache / MIT
9	xmas-elf	Apache / MIT
10	itoa-sgx	Apache / MIT
11	serde-json-sgx	Apache / MIT
12	musl-cross-make	MIT
13	grpc-rust	MIT

Release methodology and mechanics

Occlum open sourced the code on GitHub. In each middle of the month, Occlum releases a new version. In each release, Occlum would bring new features and bug fixes.
Users could build Occlum from source code or get the prebuilt version within a docker image.

List of project's official communication channels (slack, irc, mailing lists)

Slack: `occlumworkspace.slack.com`

Social media accounts

N/A

Existing financial sponsorship

Ant Group provides primary financial support with contributions from several other companies

Trademark status

N/A