Run Functional Applications in Intel SGX

by - H@ckers0x00 Team

Gaurav Tiwari, Freelancer: Secure Software Dev, gaurav1@tutamail.com

Kushal Ramkumar, Security Researcher at Intel, kushal.ramkumar@gmail.com

Our Goal for Hackathon

- Validation of Fentec libraries CiFEr and GoFE for Intel-SGX readiness
- Run CiFEr/Gofe applications in SGX enclave without any modification in source code
- Provide example, necessary configuration, build scripts, doc., docker etc.

Background

- Why SGX?
  - hardware support for isolated program execution environments
  - enclaves attest to a remote party that it is running a particular program unmodified and isolated
- Why Graphene & Occlum?
  - OSS projects
  - enables to run unmodified applicatios in SGX enclave
  - good for lagacy apps or for teams who don’t have fund to make native SGX app
  - both are LibOSes, so minimal TCB

What We have Done

- Created 2 projects
- simplae_app
  - contains only minimal build scripts and confgration templates
  - downlads CiFEr github project, builds it without modification
  - runs CiFEr project example app in SGX
  - **can be used as an starter project for more complex CiFEr-SGX application**
- pp_analytics_app
  - more multi-party server-client kind of demo
  - C++ client uses CiFEr and runs with graphene-SGX
  - Go Key management server uses uses GoFE and runs with occlum-SGX
    - graphene SGX is not ready with golang, occlum supports go
    - **status: work in progress**

Demo