Enclave Host Interface for Security

Anmol Sinha, Antti Rusanen
Huawei Technologies Oy Co. Ltd., Finland

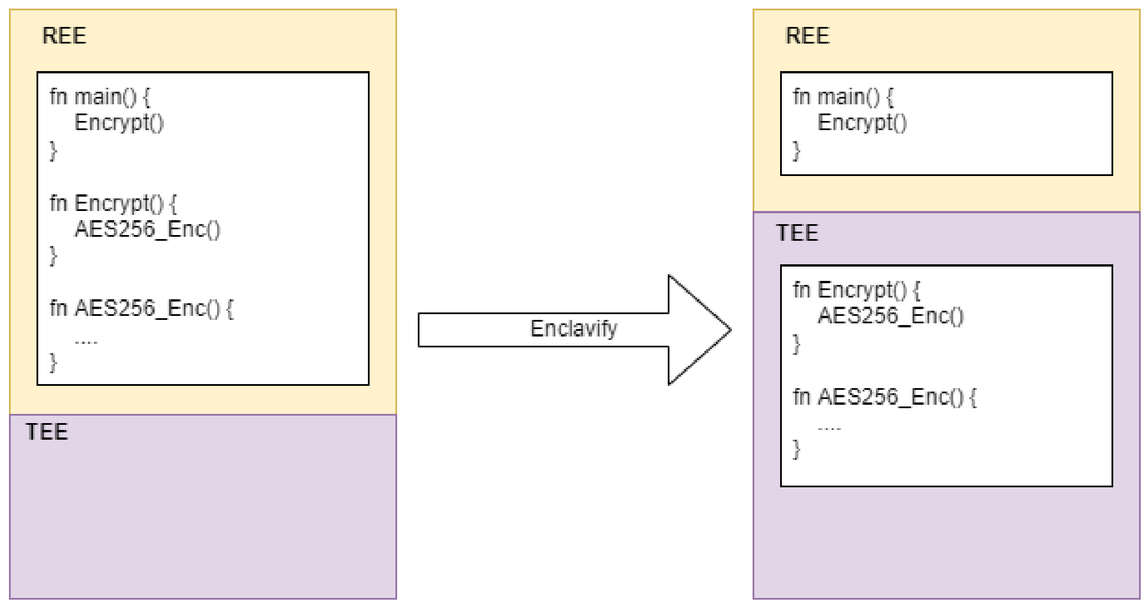
Challenges with Developing Secure Enclaves

A secure enclave is a hardware assisted isolation mechanism where the code is executed in a trusted execution environment and cannot be tampered with.
Creating secure enclave applications can be tedious and error prone. Developer needs to carefully divide the application into host and enclave parts to make the interface as simple as possible and some of the benefits of strongly typed languages are lost.

Our Solution

We created a Visual Studio Code extension that takes an existing Rust program and:

- Automatically creates enclave scaffolding and extracts user selected function and its transitive dependencies into the enclave.
- Generates marshalling code to transparently glue the enclave-host interface.



Implementation

- The parser converts the code into an AST which is used for further analysis of the code.
- AST is used to find the dependencies of the selected function and to create a subset AST.
- The code generator converts the subset AST into enclave Rust code, interface trait and a macro.
- During compilation, macro is expanded into client interface and serializer in the host, and into deserializer and dispatcher in the enclave