1 POSTER: An Open-Source Framework for Developing Heterogeneous Distributed Enclave Applications

1.1 Introduction

1.1.1 Enclaves

Trusted Execution Environments (TEEs) allow an application to execute in a hardware-protected environment called enclave. Enclaves are isolated and protected from the rest of the system, ensuring strong confidentiality and integrity guarantees. Cryptographic primitives and cryptographic keys, which are unique per enclave and which can only be used by that enclave, enable secure communication and remote attestation.

1.2 Authentic Execution

1.2.1 Authentic Execution

We developed the concept of authentic execution to address the problem of securely executing distributed applications on a shared infrastructure and to also minimize the application's runtime TCB. Authentic execution provides a notion of security that we summarize as "if the application produces a physical output event, then there must have happened a sequence of physical input events such that that sequence, when processed by the application, produces that output event." which is roughly equivalent to the concept of robust safety. This guarantee relies on standard TEE security properties (i.e., strong software isolation and software attestation) but also on a notion ofsecure I/O where physical I/O channels can be connected to an enclave such that the application enclaves maintain exclusive access over I/O peripherals.

1.2.2 Objectives

We consider an open system as the basis for our framework. In this open system, software is deployed dynamically and multiple stake-holders may run applications on the same infrastructure, including on the light-weight IoT and Edge hardware. Thus, we consider scenarios where arbitrary new code can be loaded at run time and we consider powerful attackers that can manipulate all the software on the infrastructure (unless that software is isolated in enclaves),can manipulate network traffic, but cannot break crypto. Attacks against the hardware are out of scope.