TEEProtect: Securing the Interface of Enclaves

Meni Orenbach
Technion

Bar Raveh
Technion

Alon Berkenstadt
Technion

Yan Michalevsky
Anjuna Security

Shachar Itzhaky
Technion

Mark Silberstein
Technion

Introduction

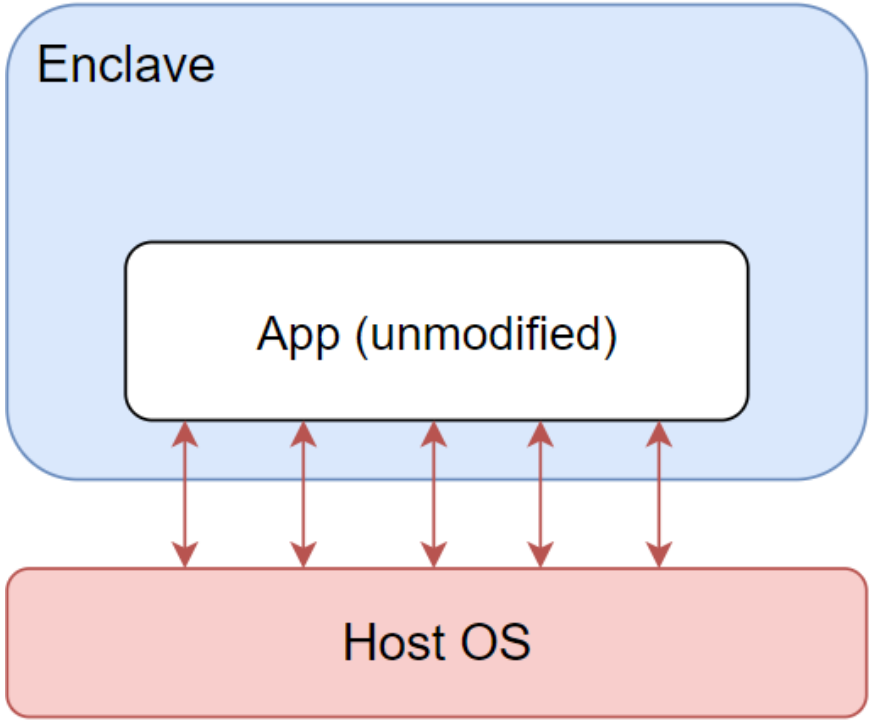
- A **secure enclave** provides CPU hardware-level isolation and memory encryption.

  Applications run in an environment is completely isolated from anything else on the machine, including the OS.

  - But they do rely on OS services to function (filesystem, synchronization etc.)

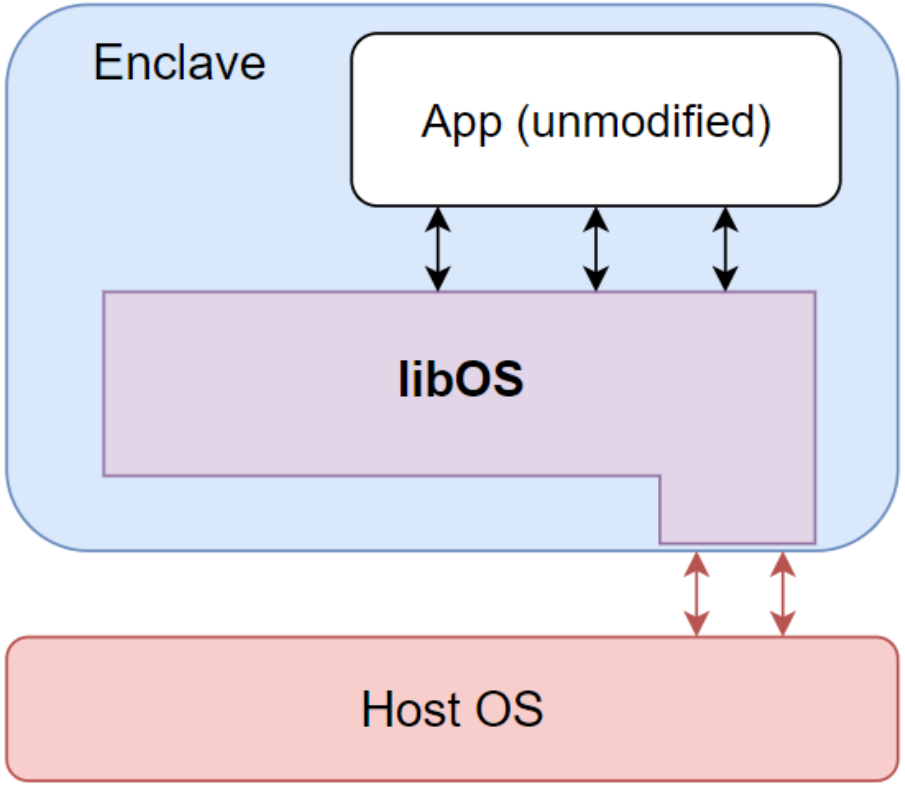
- An untrusted OS can perform **Iago attacks** which may break application's control flow integrity.

  - In a nutshell, Iago attacks return malicious values instead of valid results.

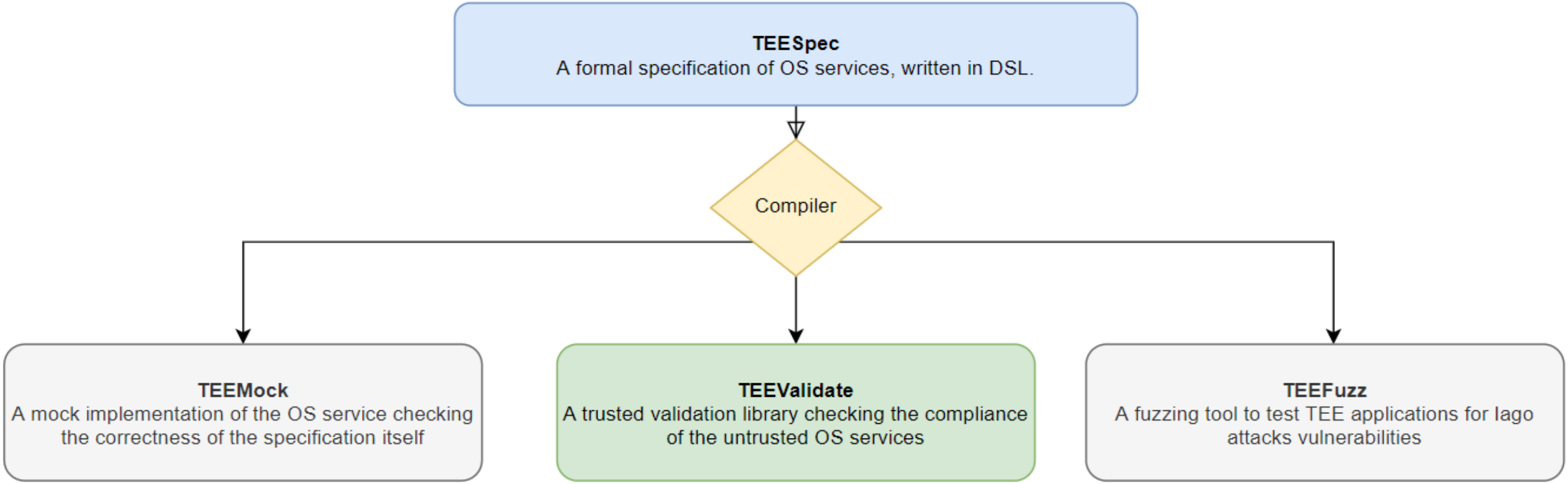


Introduction

- Existing solutions rely on partial re-implementation of OS services, in the form of a **library OS** within the enclave.
- This does reduce the untrusted OS services to a minimum, but:
  - Dramatically increases the **Trusted Code Base (TCB)**
  - Lacks many features available in a regular OS
  - No Iago attack protection guarantees



TEEProtect


TEESpec
A formal specification of OS services, written in DSL.
Compiler
TEEMock
A mock implementation of the OS service checking the correctness of the specification itself
TEEValidate
A trusted validation library checking the compliance of the untrusted OS services
TEEFuzz
A fuzzing tool to test TEE applications for Iago attacks vulnerabilities

TEESpec

TEESpec models the OS services as a Labeled Transition System

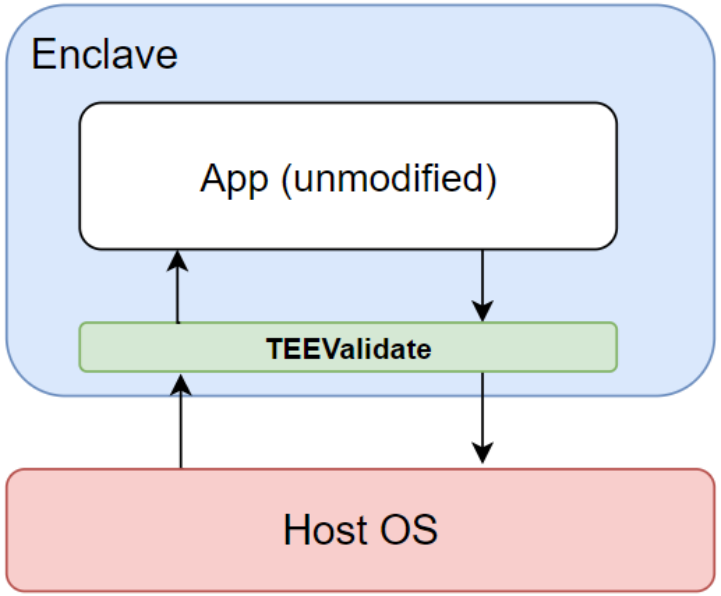
- Relations
  - Mapping of abstract keys to an abstract values
  - Allows capturing any number of real-world states
- Transitions
  - Used to describe system call semantics

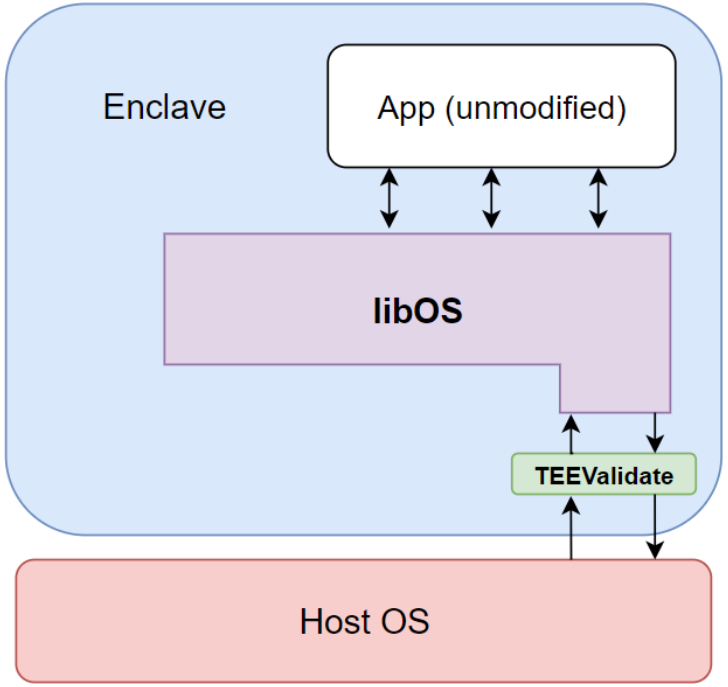
```
relation mutex_state(id:int) returns(val:bool);

action mutex_lock(id: int) returns (res: void) := {
  extern call untrusted_toyos_lock(id);
  atomic (mutex_state(id)) {
    await requires (mutex_state(id).val == UNLOCKED);
    mutex_state(id).val := LOCKED;
  };
};
```

TEEValidate

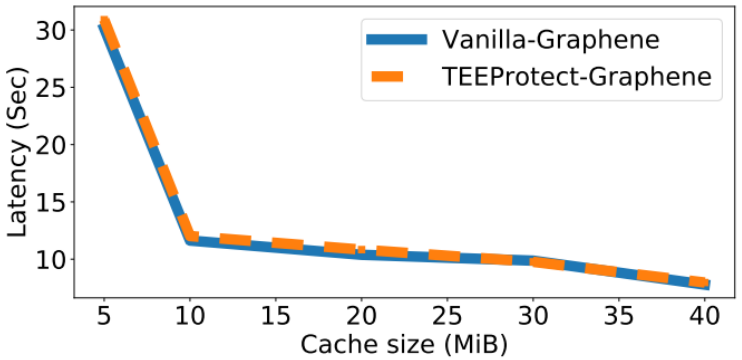
- A linkable library. Validates each system call according to TEESpec's specification.



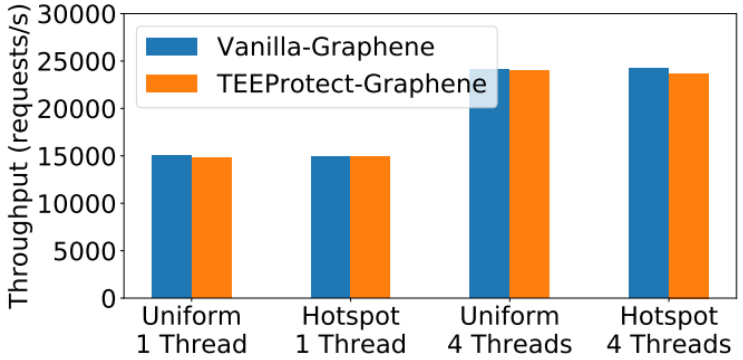


Results

- TEESpec:
  - Formal specification of POSIX Filesystem and synchronization API
- TEEValidate:
  - A linkable library that protects TEE apps and library OSes from Iago attacks
  - Negligible overhead



(b) FS overheads with SQLite



(c) Futex overheads with Memcached

Thank you!