Developing Apps for Emerging TEEs

Lari Lehtomäki, Thomas Nyman, Brian McGillion, N. Asokan

Aalto University

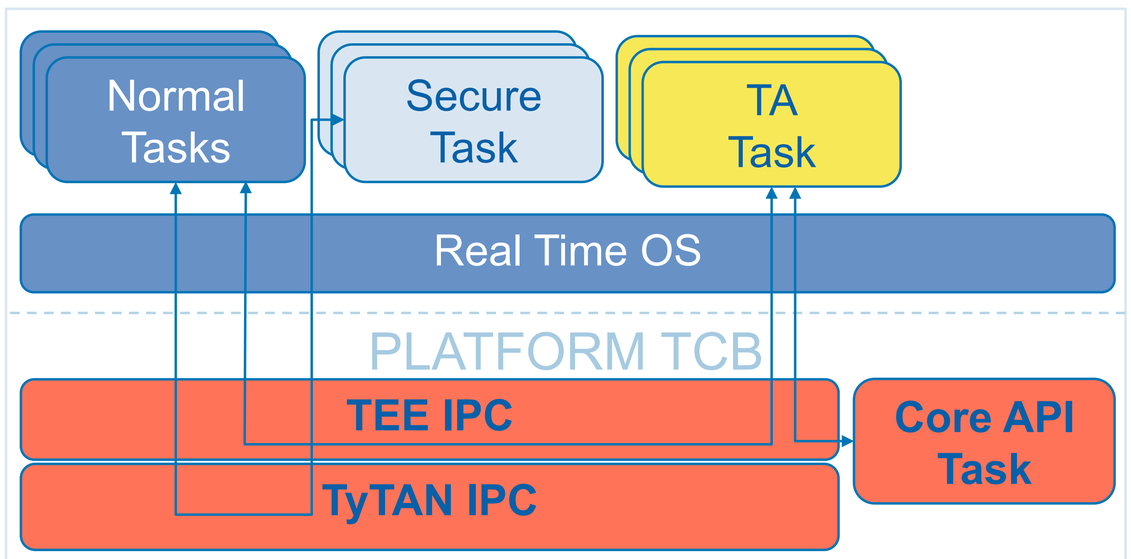
Collaborative Research Institute for Secure Computing

New types of emerging TEEs bring novel features, but come with a high barrier for entry

We highlight challenges in realizing standard TEE interfaces on such TEEs, and show how GlobalPlatform interfaces can be mapped to different TEE environments

TEEs are realized on a wide range of devices, from embedded systems to PC platforms

- New TEEs have new paradigms, interfaces and software development tools, e.g.
  - TrustLite; for tiny embedded devices
  - Intel SGX; for high-end devices
  - Virtualization; for mid-range to high-end
- Standardization efforts, e.g. GlobalPlatform enable TA deployment in compliant TEEs
  - Essential for service providers, who need to support diverse user base
  - Lower barrier to entry for developers who are already familiar with one TEE paradigm
  - No support for novel TEE features



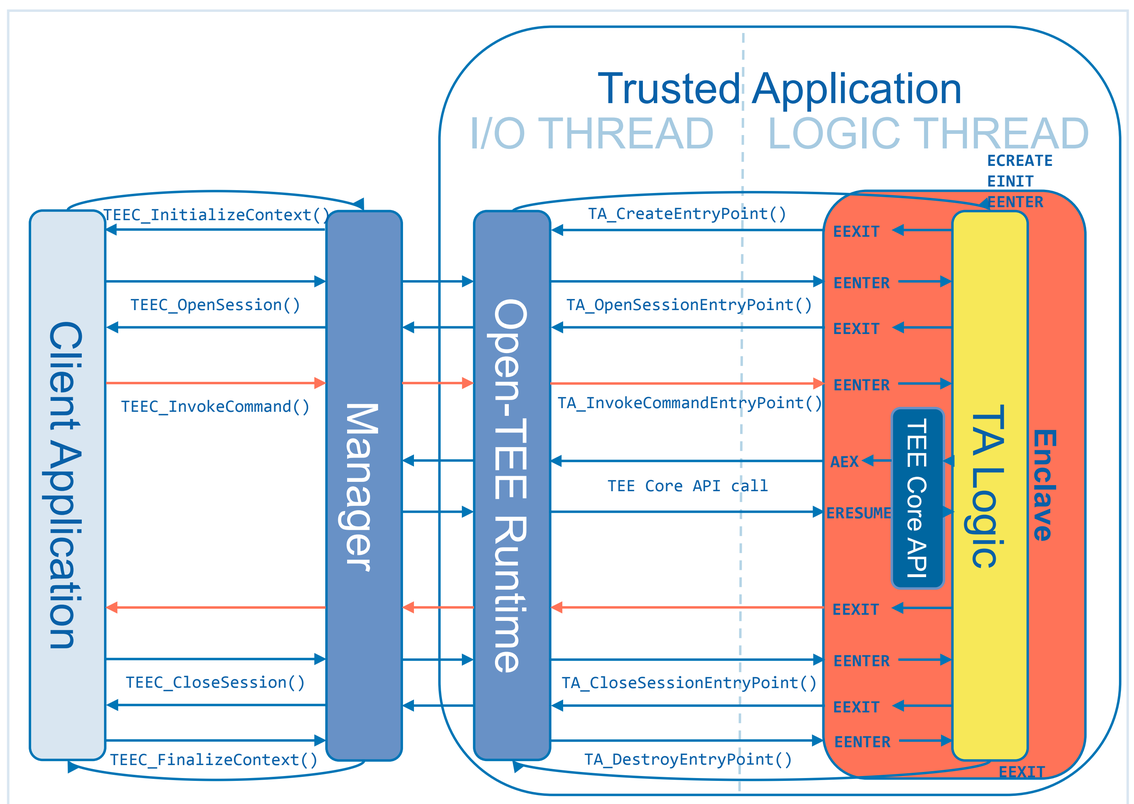
Mapping GlobalPlatform Interfaces to TrustLite

Challenges in realizing GP on TrustLite

- Lacks a split-worlds architecture akin to ARM TrustZone, relies on untrusted OS scheduler
- TyTAN/TrustLite IPC abstraction deviates greatly from GlobalPlatform TEE Client API
- Is subject to prohibitive resource constraints of tiny embedded devices

Challenges in realizing Open-TEE on SGX

- No system calls from enclave
- Marshalling enclave entry and exit at TEE Core API internal TA access points



Mapping Open-TEE to SGX

https://open-tee.github.io

Intel CRI for Secure Computing