Variations in TEEs

David M. Wheeler

28 March 2017

TEE Variations

- Protections
  - Size of TCB
  - Confidentiality of Code & Data
  - Integrity of Code & Data
  - Confidentiality of Execution
  - Coverage of Attestation
- Type & Capability of Root of Trust
  - Verifying code
  - Attesting to TEE
  - Attesting to loaded code
  - Deriving application key materials
- Anonymity

Intel Trusted Execution Environments

- Intel® Software Guard Extensions
  - Intel® Software Guard Extensions (Intel® SGX) is an Intel technology for application developers who are seeking to protect select code and data from disclosure or modification. Intel SGX makes such protections possible through the use of enclaves, which are protected areas of execution.
  - EPID 2.0 root of trust
  - https://software.intel.com/sgx
- Intel® Dynamic Application Loader
  - The Intel® Dynamic Application Loader (DAL) is a unique feature of Intel platforms that enables you to directly access and run small portions of code on part of the system's root of trust.
  - EPID 1.1 Root of Trust
  - http://developers.txe.iil.intel.com/
- Intel Innovation Engine
  - A co-processor withinIntel SOC that provides an are for OEM/ODM to run trusted firmware, including cryptographic operations and protocols
  - https://ami.com/en/products/remote-management/intel-innovation-engine-firmware/

Intel® SGX Creates TEE on Load

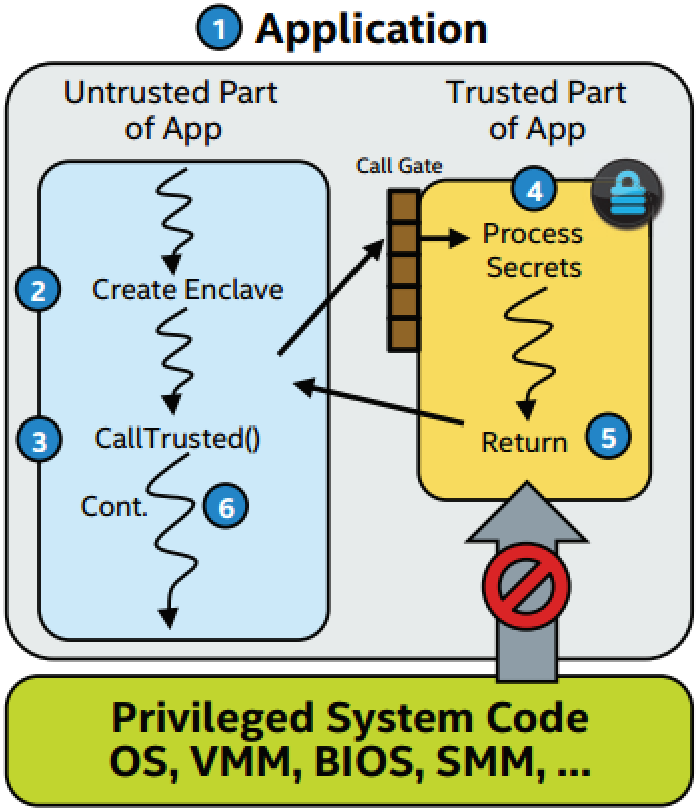

Figure 3:
Runtime Execution

1. App built with trusted and untrusted parts
2. App runs & creates the enclave which is placed in trusted memory
3. Trusted function is called, execution transitioned to the enclave
4. Enclave sees all process data in clear; external acess to enclave data is denied
5. Trusted function returns; enclave data remains in trusted memory
6. Application continues normal execution

See https://software.intel.com/sites/default/files/managed/50/8c/Intel-SGX-Product-Brief.pdf

Interesting SGX Attributes

- Enclave (TEE) is constructed on demand
- SGX Launcher verifies trusted code is authorized on the platform
- Enclaves get their own derived key material unique to them and their version
  - Strong cryptographic binding of secrets to platform and trusted applet
- Attestation (Quoting) performed by trusted service on the platform using the platform’s RoT providing anonymous attestation

Intel SGX Explained https://eprint.iacr.org/2016/086.pdf

Management of TEEs

- Must support different types of TEEs
  - TEEs without RTOS/Manager, like SGX
  - TEEs with dynamic loading of applets (DAL & SGX)
- Must support platforms with multiple simultaneous TEEs
  - Cooperating
  - Non-Cooperating
- Must support validation of TEE trust by cryptographic means
  - Not merely by an identifier in a certificate
- Must support privacy of applets, service providers, devices and users
- EPID is very important for Intel to support existing TEEs