Towards Management of Chains of Trust for Multi-Clouds with Intel SGX

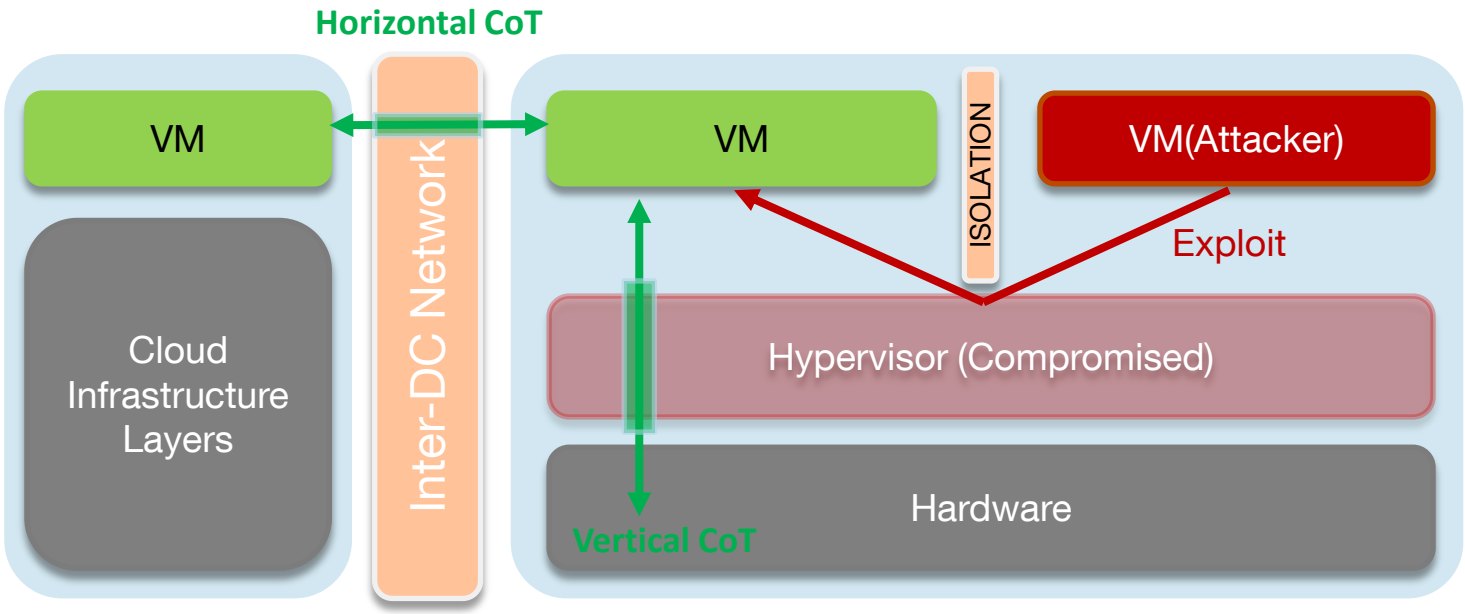
Houssem KANZARI and Marc LACOSTE

Orange Labs

Second Workshop on Security in Clouds (SEC2 2016)

orange™

Trust and Isolation Issues in Cloud Environment

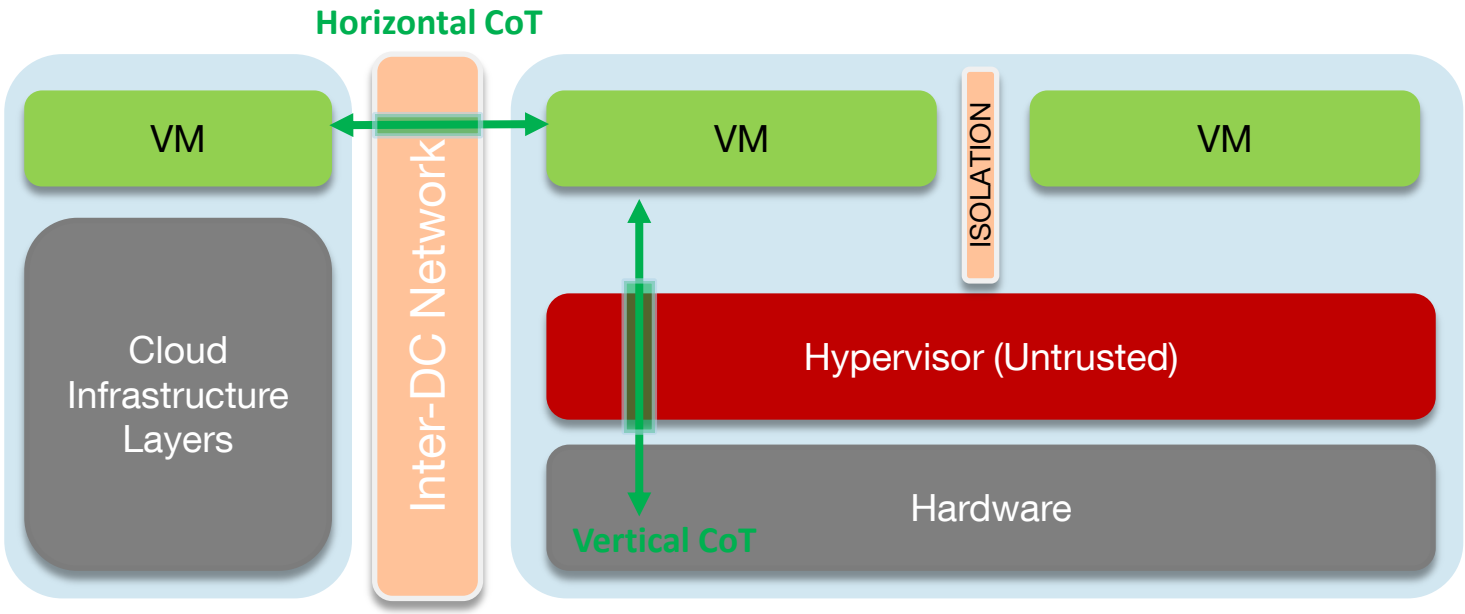


Threats :
VM secure execution compromised due to the vulnerability against insider attack

Approach:
Hardware aided secure isolated execution

➡ Intel SGX enclave

Trust and Isolation Issues in Cloud Environment



Threats :
VM integrity issues due to the vulnerability of virtualized hardware over hypervisor

Approach:
Secure channel who can bypass untrusted layers

⇨ Chain of Trust

Outline

Background: chains of trust and Intel SGX

CoT attestation protocols:

- Intra-SGX Platform
- Remote SGX Platform

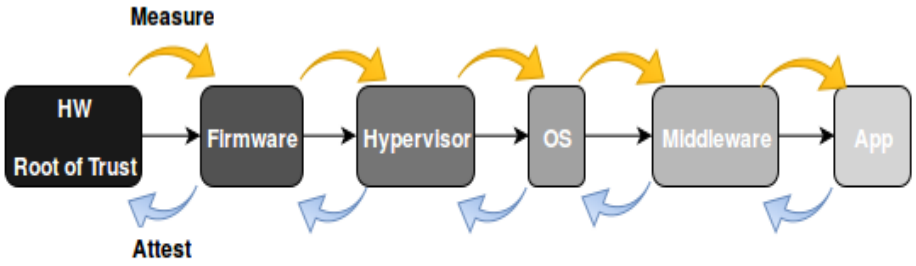
Implementation: CoT API over OpenSGX

Evaluation

Chain of Trust Based Intel SGX

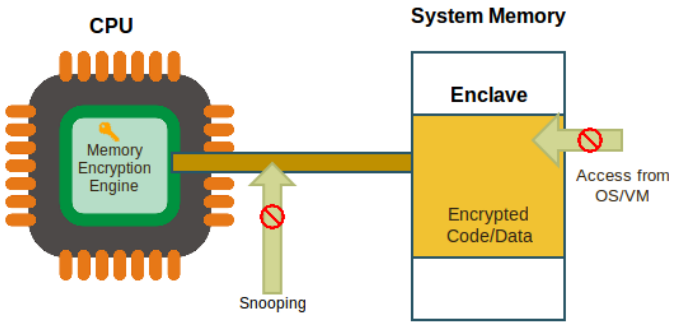
Chain of Trust:

- RoT for measurement and reporting
- Each element reports it's trustworthy in order to be a part of the CoT
- Append element to the CoT by measuring it's trust

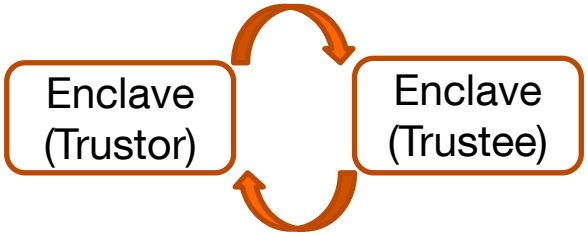


Enclave Intel SGX:

- A secure execution context (code+data) isolated from external access
- On demand report generation for trustworthy attestation
- Built-in report integrity measurement



Check report integrity



Build then deliver report

Intel SGX capabilities matches CoT model requirements

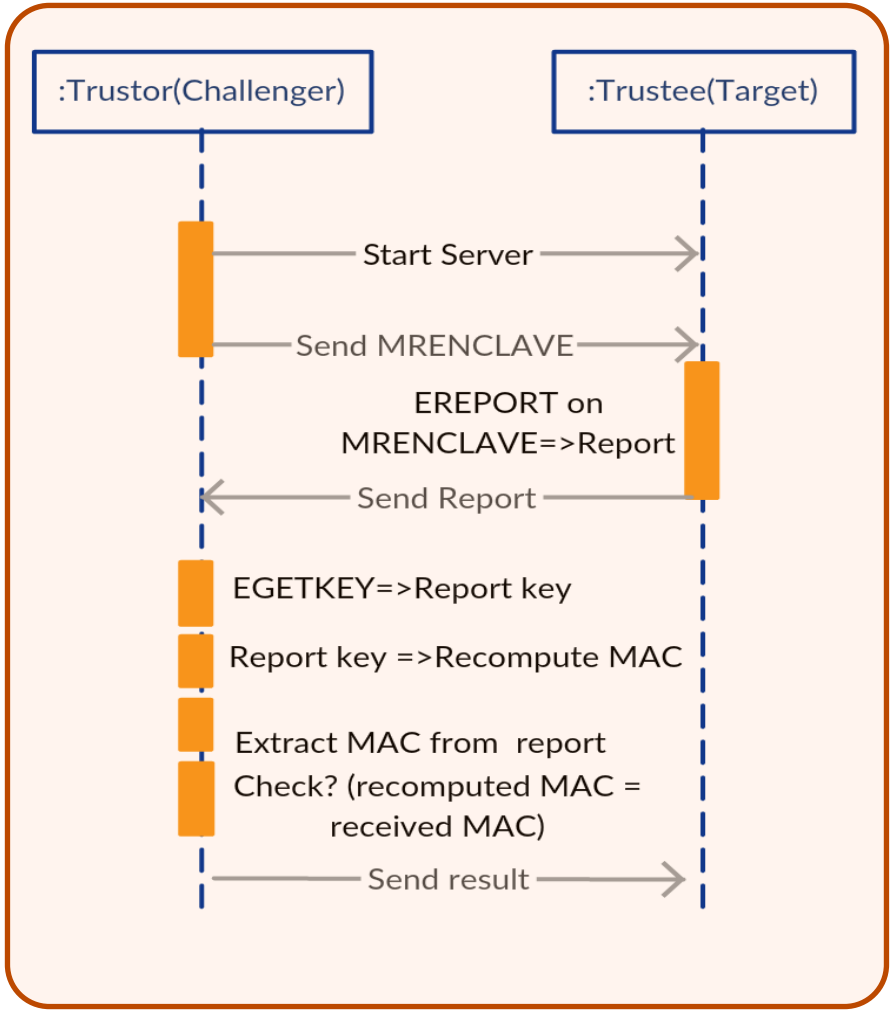
Proposed Attestation Protocols

Intra-SGX Platform enclaves Attestation

Intel SGX platform guarantees the local integrity of its enclaves

Each enclave verify the integrity of the other through a MAC computing challenge allowed by Intel SGX

Establish trust between two enclaves



Proposed Attestation Protocols

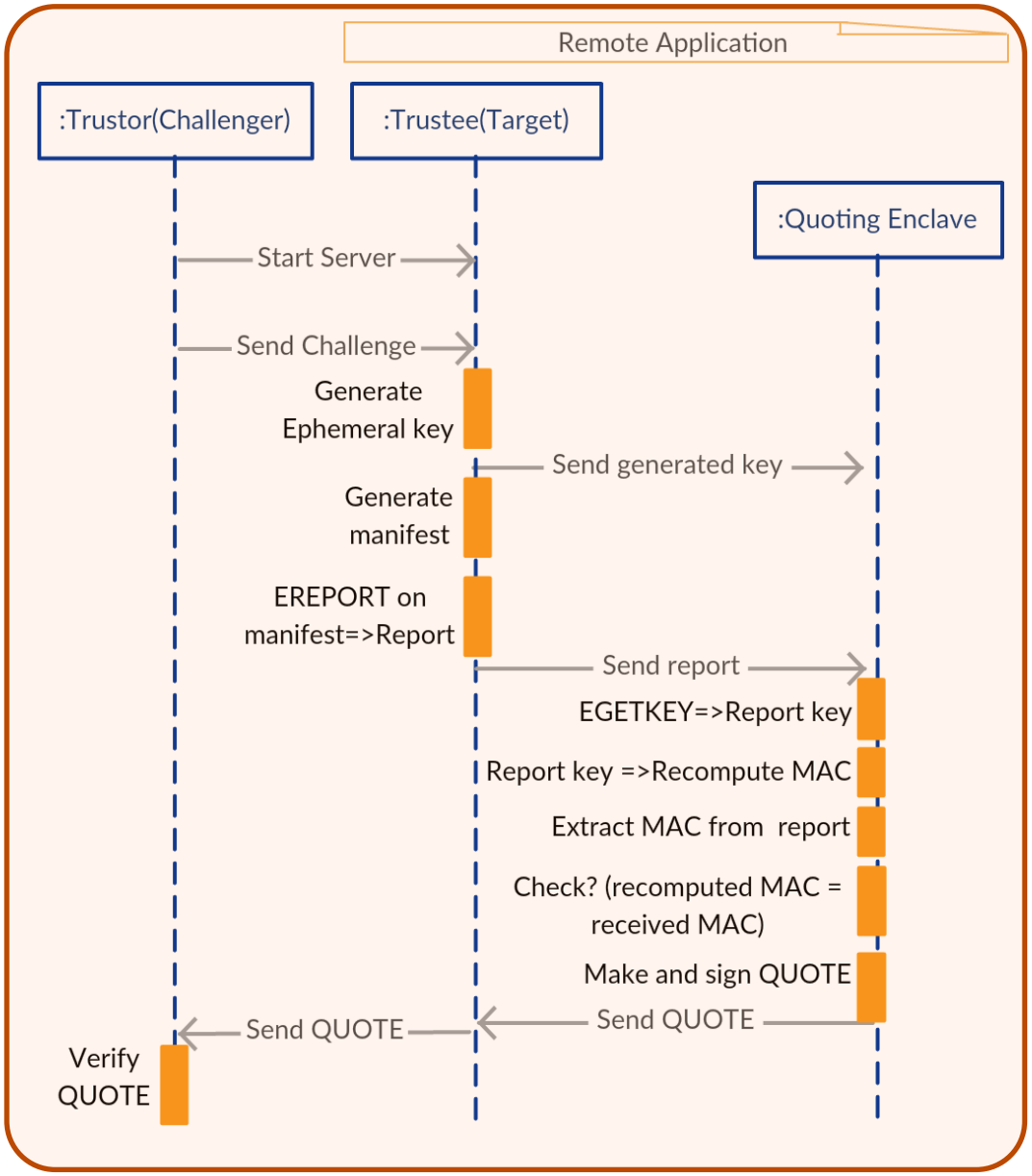
Inter-SGX Platform

Quoting enclave is responsible of reporting enclave integrity outside the platform

The target attest about its integrity to quoting enclave

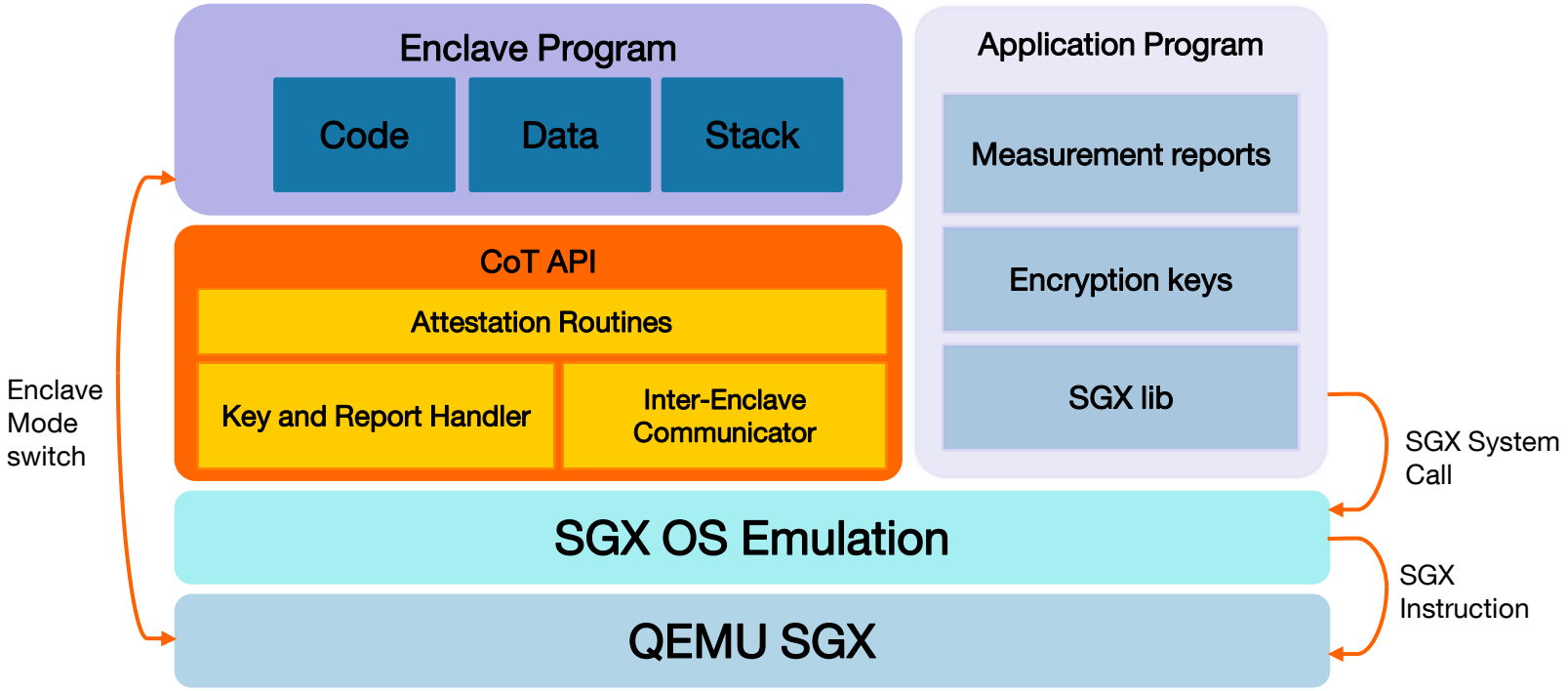
The quoting enclave deliver to the target a formatted proof able to be verified outside the platform

Establish trust between two enclaves remotely located



Implementation over OpenSGX

Architecture



CoT API features:

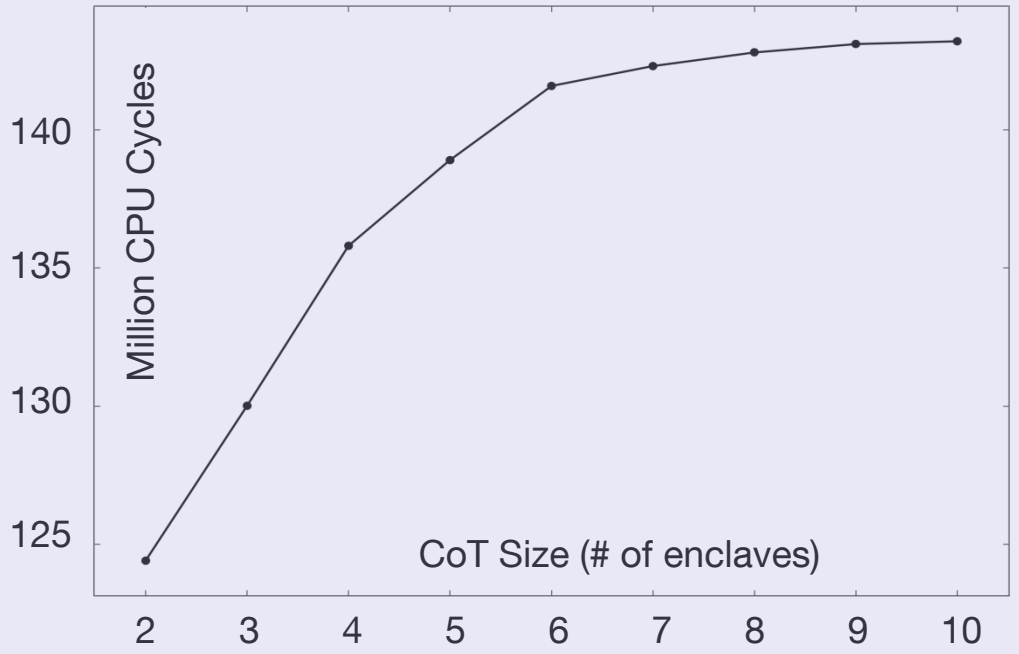
- Built-in key creation, report signing and checking procedure.
- Dedicated secure socket interface
- Ready to use attestation routines

Preliminary Scalability Results

CPU cycle consumption during CoT building vs CoT size

- Start-up offset (~120 Mcycles)
- CoT establishment overhead appears sub-linear w.r.t size

➡ Our protocols could scale to large CoT sizes



Next steps:

- Translate our approach from emulated to real Intel SGX hardware
- Verify scalability on very large CoT size
- Extend and enhance CoT API to capture richer CoT model (cross-layer)
- Integrate with self management security framework

Thank you