Christof Fetzer, PhD

CONFIDENTIAL COMPUTING WITH SCONÉ & SGX

christof.fetzer@scontain.com
https://sconedocs.github.io/
https://scontain.com/
FOCUS ON APPLICATIONS & SERVICES

- Protect the DATA & CODE
- ATTEST the Platform & Code
- Enable Performance
- Trust
- Resilience
- Transparency

Current Threats: potential vulnerabilities

Hypervisor

BIOS/Firmware

CPU

At rest
In flight
In use
SCONIFY: Native » Confidential Container Image

- Protect the DATA & CODE
- ATTEST the Platform & Code
- Resilience Transparency
- Trust

At rest
In flight
In use

Current Threats
Potential vulnerabilities

Enable Performance

1-Step TLS encrypted

SVC
OS
VM
Hypervisor
BIOS/Firmware
CPU
TRANSPARENT ATTESTATION: Enforcing Cyber Hygiene

attest that genuine SGX, up-to-date firmware & app code
Transparent Secret Provision

- Protect the DATA & CODE
- ATTEST the Platform & Code
- Resilience
- Transparency
- Trust

Generate certs/keys & provisioning of secrets & certs

Potential vulnerabilities

Current Threats

Enable Performance

Protect the DATA & CODE

At rest

In flight

In use

Trust

Resilience

Transparency

Potential vulnerabilities

Current Threats

Enable Performance
SCONE: Transparency of usage & changes

audit log of all attestations, policy changes,...
ledger
log
encrypted

Ledger to enforce transparency

audit log of all attestations, policy changes,... in ledger

Protect the DATA & CODE

ATTEST the Platform & Code

Enable Performance

Protect the DATA & CODE

ATTEST the Platform & Code

Enable Performance

Potential vulnerabilities

Current Threats

LEDGER to enforce transparency

Intel SGX

TLS

Protect the DATA & CODE

ATTEST the Platform & Code

Enable Performance

Current Threats

Potential vulnerabilities

Intel SGX

TLS
Intel Icelake:
close to native performance

TensorFlow Lite
Why Protect Data and Code?

Protect against:

- Malicious insiders with escalated admin privileges
- Hackers exploiting bugs in the hypervisor/OS
- Third parties accessing data without owner’s consent

Data & Computation exposed to...

- Guest OS
- Host OS
- Hypervisor
- Physical hardware access
- Host admin
- VM admin
- Kubernetes admin
- Service admin
- Collaborator

example
USE CASE: Multiple Stakeholder Computation I

- Computations encompassing multiple stakeholders
- Each stakeholder protects its own IP
- Classical RBAC insufficient to protect IP

Managed Kubernetes cluster
USE CASE: Multiple Stakeholder Computation II

- Confidential workflow connects confidential services
- Each stakeholder controls its IP via own policies
- Even operator of workflow cannot look into individual service

---

Managed Kubernetes cluster
A policy can connect a workflow