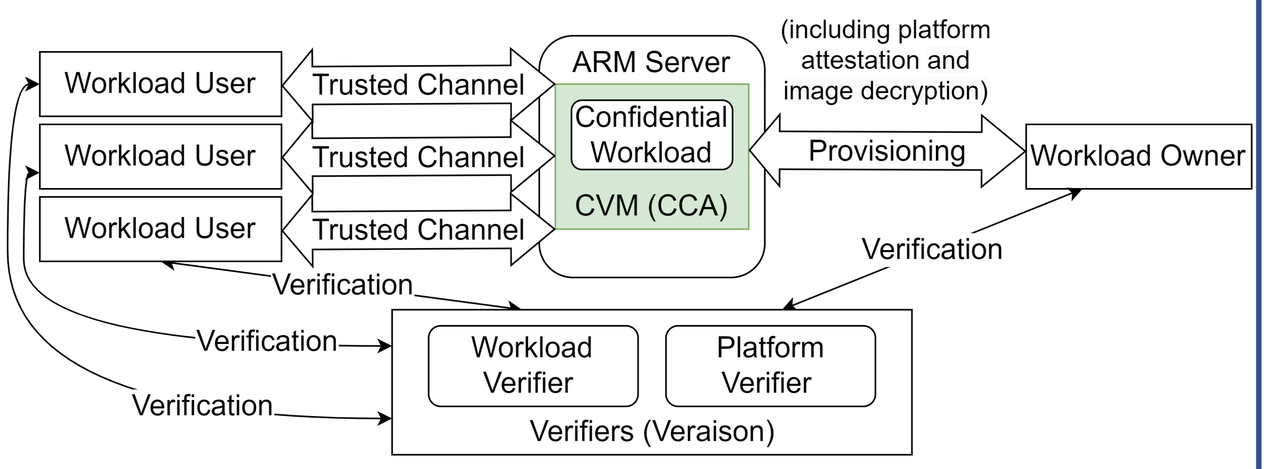
Establishing Trusted Channels for Confidential Workloads

Philipp Giersfeld, Philip Ginzboorg, Valentin Manea, Sampo Sovio

Usage Scenario

- Establish a *Trusted Channel* from client to a confidential workload



- Previous work on creating a secure channel built upon hardware-primitives (TPMs, TEEs)
  - is not tested with CVMs
  - requires modification of the workload
  - uses network protocols, e.g., IPSEC, IKEv2, that are complex to configure

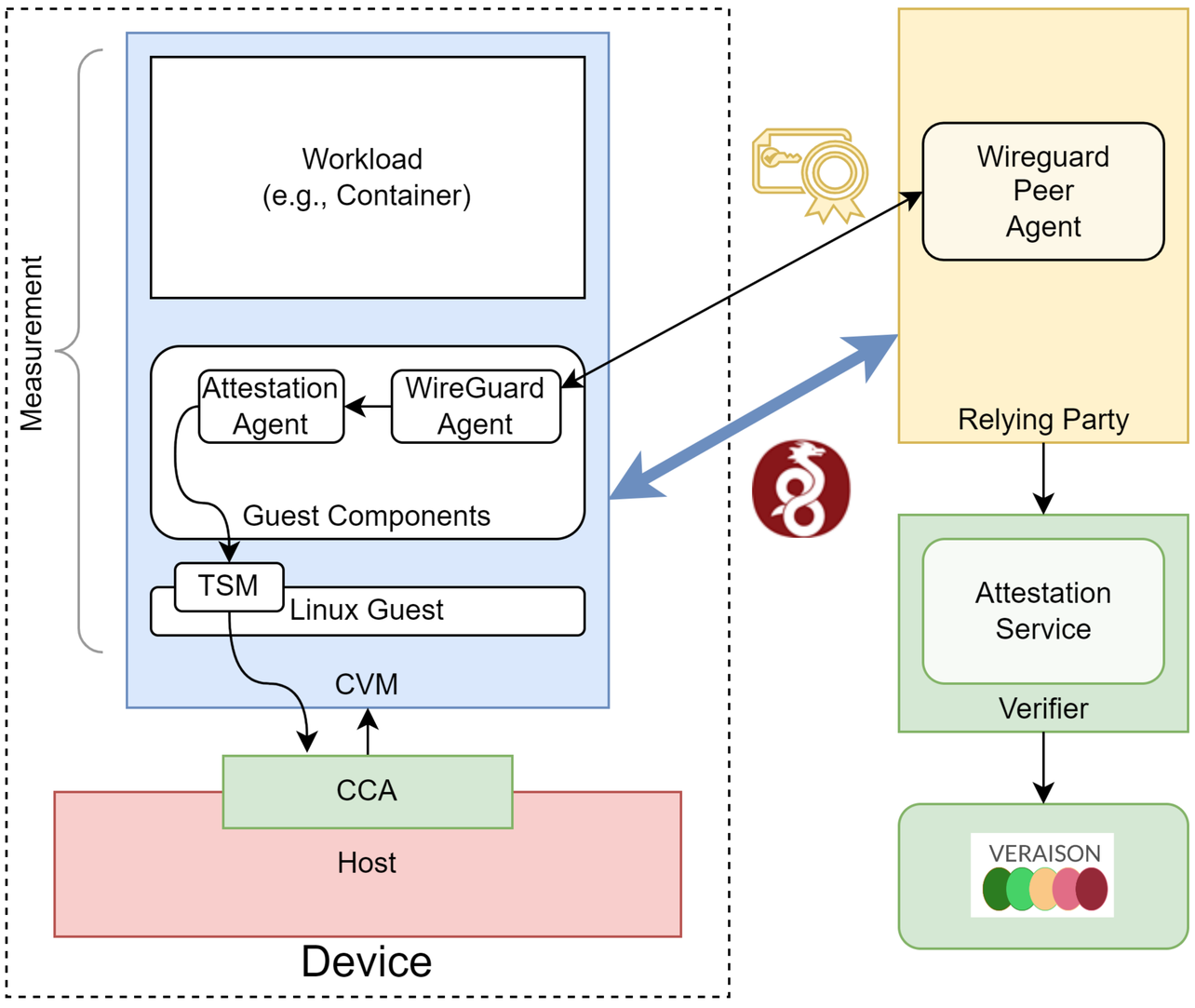
Security Goals

- Platform and Workload Attestation of the CVM
- Security (Confidentiality, Integrity, Replay Protection) of (i) attestation evidence & (ii) the communication channel

Functional Goal

- Minimal changes to the underlying application

Design



Trusted Channel Setup

- Create WireGuardAgent guest component
- Provide confidentiality through HTTPS client authentication
- Workload Attestation
- Bind CCE public key to evidence by embedding it into the nonce
- Initiate WireGuard VPN tunnel

Limitations

- Mostly suitable for applications with long and few sessions
  - ARM RMM specification prohibits concurrent attestations
- PoC based on emulation (QEMU)

CONFIDENTIAL CONTAINERS

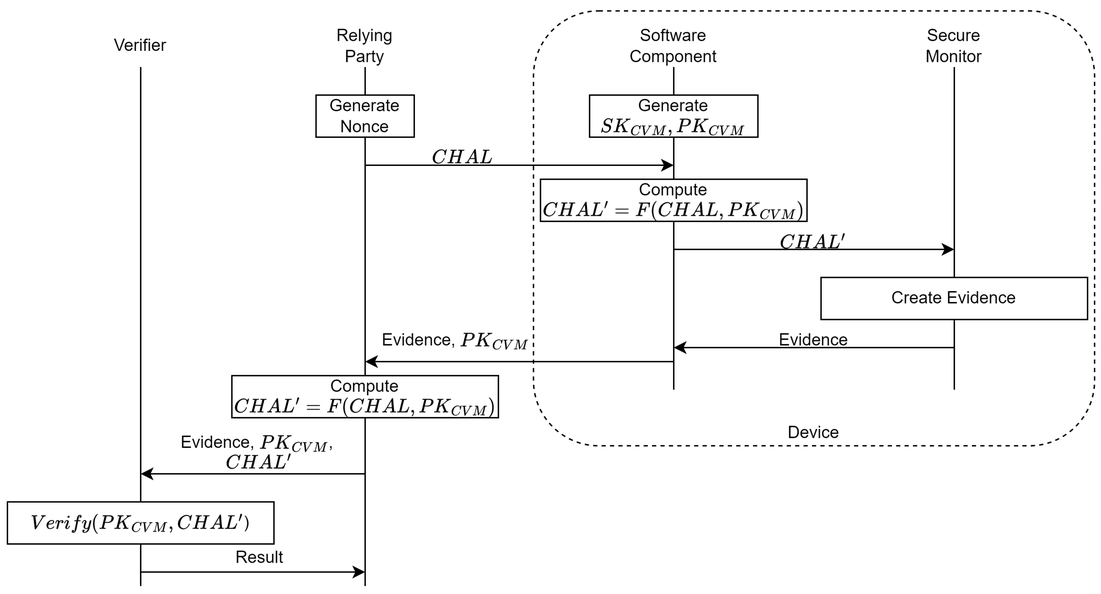
Seamless Deployment of Unmodified Containers inside Confidential Virtual Machines with Confidential Containers

- CoCo creates a Pod inside a micro CVM using Kata Containers
- The encrypted container image is downloaded
- The platform is attested, and upon successful verification the decryption key is obtained
- Decrypt the image and start it

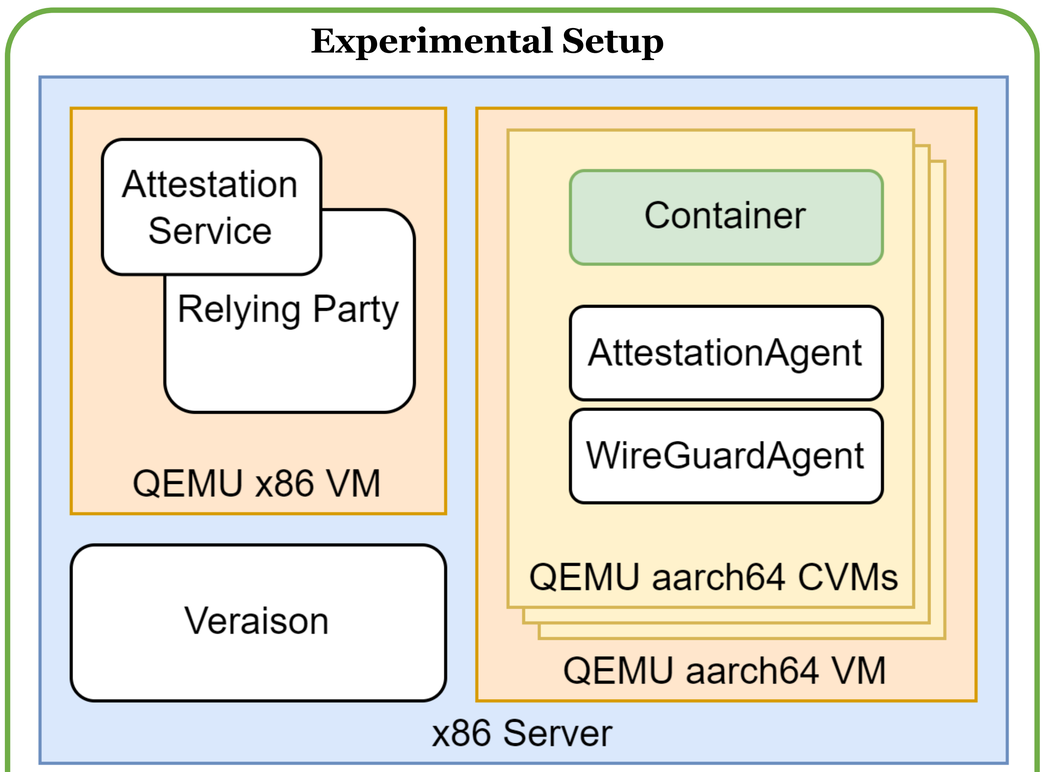
WireGuard

- Simple & Easy-to-use VPN protocol
- Configuration only requires the other peer's public key
- Formally Proven => suitable for TCB

VPN Protocol	1000's LOC
IPSEC	400
OpenVPN	70
WireGuard	4



Experimental Setup



Various implementation challenges due to experimental state of ARM CCA support of dependencies and architecture itself

Future Work

- Test on hardware when it becomes feasible and on other architectures (TDX, SEV-SNP)
- Perform Benchmarking

Helsinki System Security Lab (HSSL)

HSSL drives renewal and mastery in the field of platform and device related security technologies, especially for Huawei consumer devices such as mobile phones, laptops, televisions and automotive. We do research in topics such as hardware-assisted isolation and integrity, as well as in operating system protection (hypervisor, TEE, secure enclaves and kernel hardening). We also carry expertise in cryptography and systems security functionality such as device key management (PKI), device attestation and key-store solutions.

HUAWEI