Aalto University
UNIVERSITY OF HELSINKI
ARCADA
F-Secure
NOKIA
ssh communications security
TRUSTONIC

CloSer WP4: Infrastructure for and Integration of CloSer

Arseny Kurnikov, Aalto University
Ibbad Hafeez, University of Helsinki

Tekes
cloSer

Topics

- Secure Intermediary
- Trusted Hardware in the Cloud

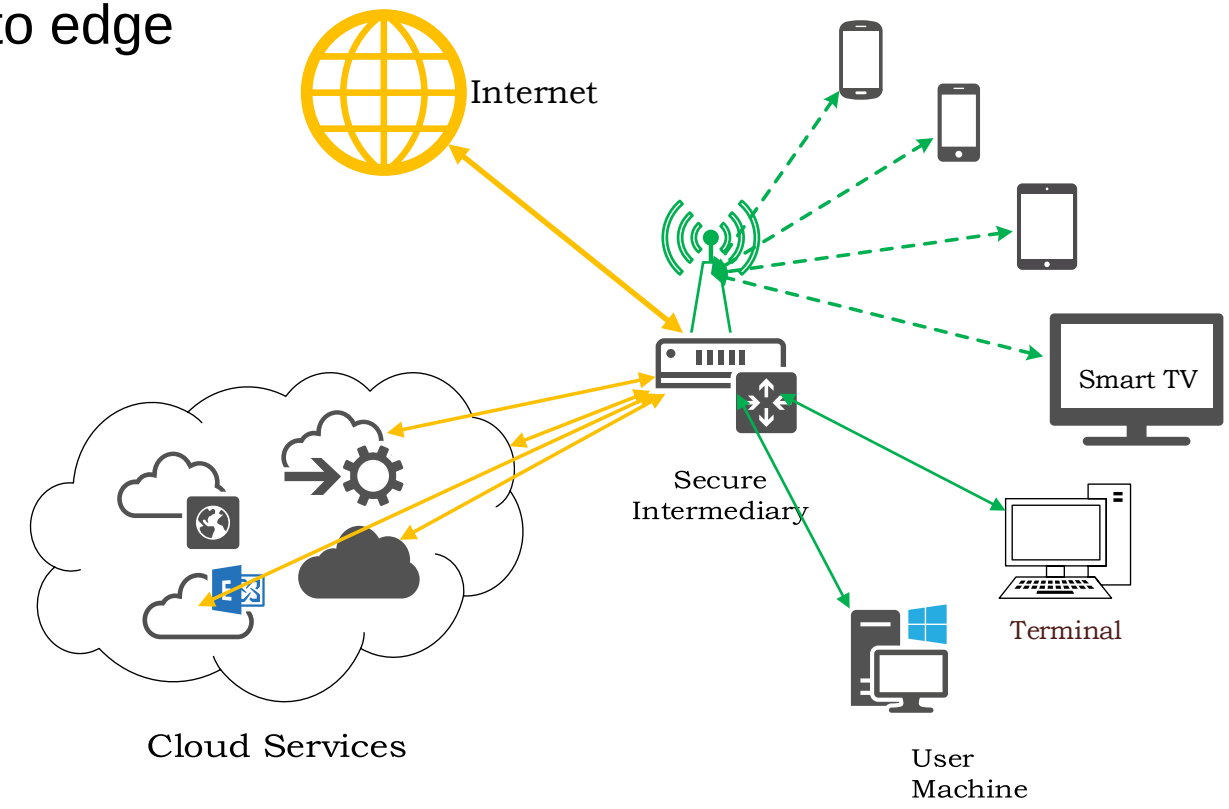
Secure Intermediary

Secure Intermediary

Extension of Securebox (CoNEXT CAN 2016, SEC 2016, Mobicom S3 2015)

Edge network device

- Enabler for bringing cloud services closer to edge
- Improving user privacy, quality of service



4

Secure Intermediary

IoT Scenario

- Scalable management of devices at the edge
- Centralized control of updates from the cloud service

SI development

- Deployment trade-off: edge functionality vs cloud
- User privacy

Integration with CloSer scenarios

- Privacy-preserving malware lookup
- Trust management

IoT Sentinel: Automated Device-Type Identification for Security Enforcement in IoT

Identify the type (make / model / SW version) of a new device when introduced to the network

Assign appropriate enforcement rules for the device based on its type (isolate known vulnerable types)

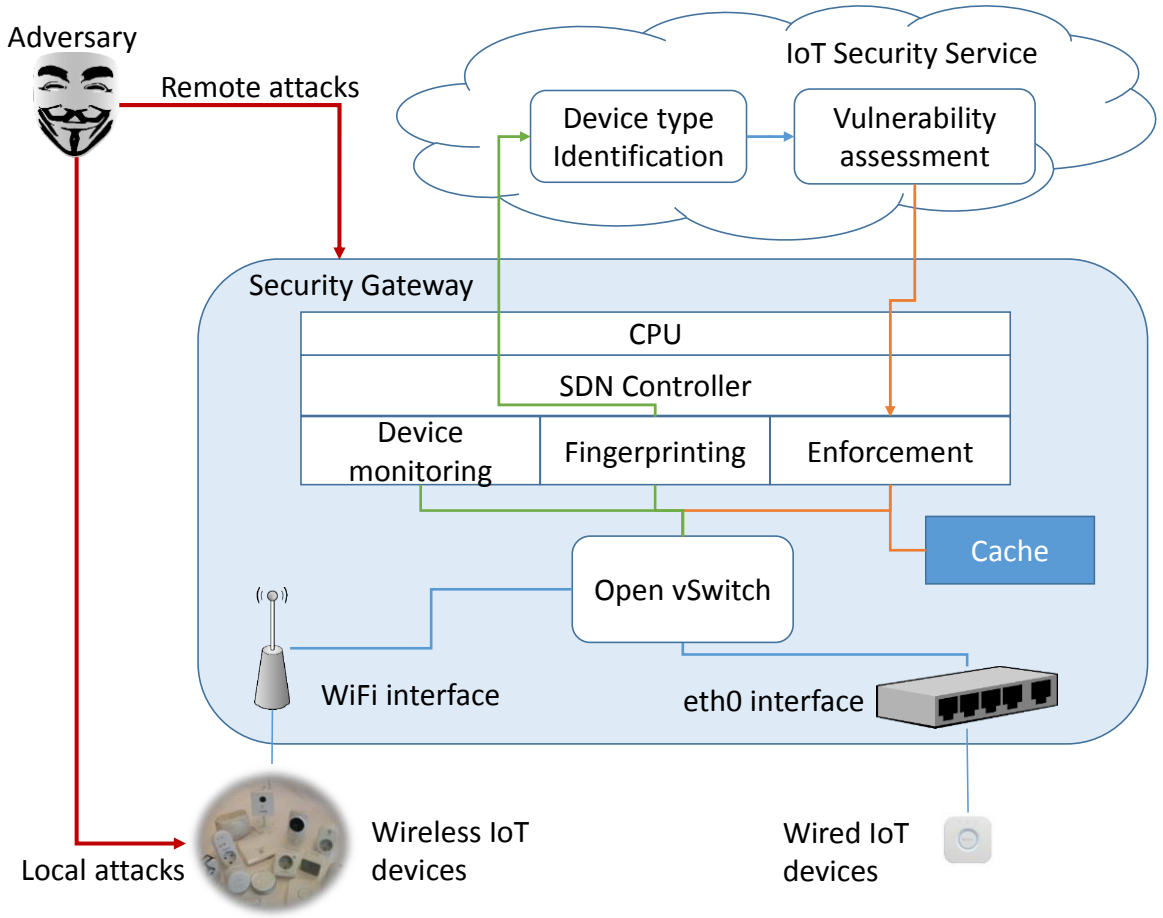
Constrain communications of vulnerable devices trough traffic filtering

- Avoid vulnerable devices to be compromised
- Contain the infection

Paper + Demo accepted in ICDCS 2017 (available on ArXiv)

IoT Sentinel Demo in the poster+demo session this afternoon.

IoT Sentinel: Automated Device-Type Identification for Security Enforcement in IoT (ICDCS 2017)



IoTurva: Securing D2D Communications in IoT Ecosystem

Monitor and control device-to-device interactions

Challenges

- Collection of ground truth
- Develop rule base for setting up control

Use machine learning to audit new communications among devices

Trusted Hardware

Trusting cloud

Cloud customers often have to trust the cloud with sensitive data

- Privacy concerns
- Potentially many points for leakage
  - Malicious administrator
  - Bugs in OS
  - Multi-tenancy

Possible mitigation – *trusted hardware*

Applicable technologies and scenarios:

- WP1: IoT scenario
- WP2: Privacy challenges in cloud-assisted (security) services

Hardware-based Trusted Execution Environments

Protect regions of memory/code

- Access enforced by the CPU
- Encrypted if stored in RAM
- OS cannot access

Remote verification of code being executed

Technologies

- Intel Software Guard eXtensions (SGX)
- ARM TrustZone

SGX

***Enclave* – trusted part of an application**

- *Measured* when loaded
- Only enclave can access its memory pages

***Sealing* – storing data outside an enclave**

- Encrypted with a key, only accessible by the enclave

***Monotonic counters*, backed up by hardware (i.e. against rollback attacks)**

***Remote attestation* – verification of the enclave code**

- Enhanced Privacy ID – privacy preserving attestation

Virtualization

Cloud practices:

- **Virtual machines (VMs)**
  - Better resource utilization
  - Elasticity
  - Scalability
- **Migration**
  - When a VM has to be moved from one physical host to another
  - Live migration
  - Offline migration

Virtualization and SGX

Sealing, attestation – depend on a CPU provided secret

When a VM with an enclave is live migrated:

- Sealed data will not be available
- Counter values will be lost
- Communication sessions with other parties should be re-established

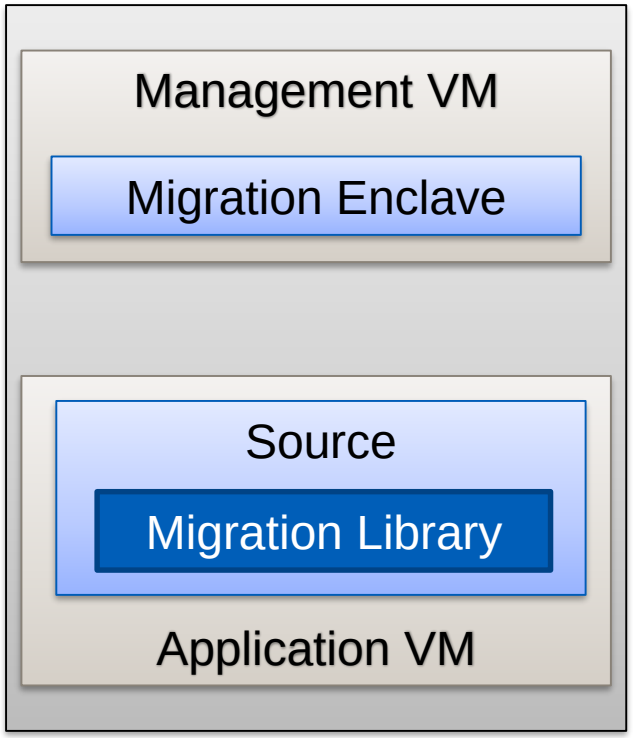
Proposed solution

Cloud provider VM with a migration enclave

- Establish secure channel between source and destination
- Mutual attestation: migration only possible to trusted nodes

Library for migratable operations

- When migration notification arrives
  - re-encrypts sealed data with a key from migration enclave
- When starting an enclave on the destination host
  - obtains key and decrypts sealed data



SGX VM migration poster in the poster/demo session this afternoon.