Advanced System Resiliency Based on Virtualization Techniques for IoT Devices

Jonas Röckl, Mykolai Protsenko, Monika Huber, Tilo Müller, and Felix C. Freiling

jonas.roeckl@fau.de
https://www.cs1.tf.fau.de/person/jonas-roeckl/

IT Security Infrastructures Lab
Department of Computer Science
Friedrich-Alexander University Erlangen-Nürnberg (FAU)

9 December 2021
Motivation

- IoT and edge is on the rise [4, 2]
Motivation

- IoT and edge is on the rise [4, 2]
- Paradigm shift [7]: One infrastructure provider (IP) offers computing resources to multiple service providers (SP)

Jonas Röckl, Friedrich-Alexander University Erlangen-Nürnberg (FAU)
- IoT and edge is on the rise [4, 2]
- Paradigm shift [7]: One infrastructure provider (IP) offers computing resources to multiple service providers (SP)
- Critical vulnerabilities (Ripple20 [5], Amnesia:33 [6]) and botnets [1, 3] targeting IoT deployments
- Manual recovery impossible
Motivation

- IoT and edge is on the rise [4, 2]
- Paradigm shift [7]: One infrastructure provider (IP) offers computing resources to multiple service providers (SP)
- Critical vulnerabilities (Ripple20 [5], Amnesia:33 [6]) and botnets [1, 3] targeting IoT deployments
- Manual recovery impossible

How can we link strong remote recoverability for service providers and intrusion and anomaly detection?
Background
Dominance (Xu et al. [8])

The hub dominates a device if the hub can choose arbitrary code and force the device to run it within a bounded amount of time.
Dominance

**Dominance (Xu et al. [8])**

The hub dominates a device if the hub can choose arbitrary code and force the device to run it within a bounded amount of time.

**Gated Boot**

```
power on -> verify software

download new software

valid?

N

valid?

Y

boot software
```
**Dominance (Xu et al. [8])**

The hub dominates a device if the hub can choose arbitrary code and force the device to run it within a bounded amount of time.

---

**Gated Boot**

1. **power on**
2. **verify software**
3. **download new software**
   - **valid?**
     - **N**
     - **Y**
       - **boot software**

---

**Reset Trigger**

Authenticated Watchdog Timer (AWDT)

1. **standby**
2. **active**
   - **[timeout]**
   - **device reset**
   - **[receive deferral ticket]**
     - **valid?**
       - **N**
       - **Y**
         - **reset timer**

---
Novel Trusted Computing Concepts
Strong Dominance

**Dominance (Xu et al. [8])**

The hub dominates a device if the hub can choose arbitrary code and force the device to run it within a bounded amount of time.

**Strong Dominance**

A hub *strongly dominates* a scheduler if the hub can choose arbitrary code and force the execution of the code as an activity of the scheduler in a bounded amount of time.
Weak Dominance

A hub $H_1$ weakly dominates a scheduler $S_1$ if the following conditions are fulfilled:

1. There is a hub $H_2$ that strongly dominates a scheduler $S_2$.
2. The scheduler $S_2$ dispatches the scheduler $S_1$.
3. Given that $H_2$ behaves cooperatively, $H_1$ can choose arbitrary code and force its execution in an activity of the scheduler $S_1$ in a bounded amount of time.
System Architecture
Service Machines (SMs)

- Weakly dominated by a Service Hub (SH)
- Encapsulate services

- Service Machines (SMs)
- Weakly dominated by a Service Hub (SH)
- Encapsulate services

- Management Machine (MM)
- Weakly dominated by an Infrastructure Hub (IH)
- Provides dominance-related functionalities
- An SP can recover a weakly dominated SM even after a severe software compromise
- Even in case of an VM escape: The IH can still recover the device
**System Architecture**

- **Service Machines (SMs)**
  - Weakly dominated by a Service Hub (SH)
  - Encapsulate services

- **Management Machine (MM)**
  - Weakly dominated by an Infrastructure Hub (IH)
  - Isolates the network stack during runtime
  - Provides dominance-related functionalities

> • Service Machines (SMs)
  - Weakly dominated by a Service Hub (SH)
  - Encapsulate services

> • Management Machine (MM)
  - Weakly dominated by an Infrastructure Hub (IH)
  - Isolates the network stack during runtime
  - Provides dominance-related functionalities
System Architecture

- **Service Machines (SMs)**
  - Weakly dominated by a Service Hub (SH)
  - Encapsulate services

- **Management Machine (MM)**
  - Weakly dominated by an Infrastructure Hub (IH)
  - Isolates the network stack during runtime
  - Provides dominance-related functionalities

- An SP can recover a weakly dominated SM even after a severe software compromise
- Even in case of an VM espace: The IH can still recover the device

---

Jonas Röckl, Friedrich-Alexander University Erlangen-Nürnberg (FAU)
During boot: Gated Boot
- Ticket Receiver acquires deferral ticket from IH regularly
- TCB compromise: No remote recoverability any longer
During VM boot: Virtual Gated Boot

- Ticket Receiver acquires deferral ticket from SH regularly
- Requests for deferral tickets contain dynamic runtime state (VMI)
- Granular resets of SMs
Achieving Weak Dominance

- During VM boot: *Virtual Gated Boot*
  - Ticket Receiver acquires deferral ticket from SH regularly
  - Requests for deferral tickets contain dynamic runtime state (VMI)
  - Granular resets of SMs

- During VM boot:
  - Virtual Gated Boot

- Ticket Receiver acquires deferral ticket from SH regularly

- Requests for deferral tickets contain dynamic runtime state (VMI)

- Granular resets of SMs
Implementation and Evaluation
Implementation and Evaluation

- Boundary Devices
  - Nitrogen8M, Cortex A-53, 2GB RAM

Jonas Röckl, Friedrich-Alexander University Erlangen-Nürnberg (FAU)
Implementation and Evaluation

- Boundary Devices
  Nitrogen8M, Cortex A-53, 2GB RAM
- TCB: ARM Trusted
  Firmware, OP-TEE, AWDT, Gated Boot:
  600 kLoC (no hypervisor)
Implementation and Evaluation

- Boundary Devices
  - Nitrogen8M, Cortex A-53, 2GB RAM
- TCB: ARM Trusted Firmware, OP-TEE, AWDT, Gated Boot: 600 kLoC (no hypervisor)
- Dominance components do not add overhead, virtualization does

Jonas Röckl, Friedrich-Alexander University Erlangen-Nürnberg (FAU)
Summary

- Trusted computing concepts: Strong dominance and weak dominance for future resilient IoT and edge deployments
- Application-level protocol that binds the runtime state to strong recoverability guarantees
- System architecture for the proposed concepts, assuming shared edge and IoT infrastructure
- Proof of concept implementation, showing feasibility
Thank you for your attention!
Feel free to ask questions!

jonas.roeckl@fau.de
https://www.cs1.tf.fau.de/person/jonas-roeckl/

IT Security Infrastructures Lab
Department of Computer Science
Friedrich-Alexander University Erlangen-Nürnberg (FAU)

Icon Author Contribution:
Some icons used in this presentation are provided by JGraph and their useful tool diagrams.net (https://github.com/jgraph/drawio). They are licensed under the Attribution 4.0 International (CC BY 4.0).
References


[4] **INSIDER, B.**  
*Internet of Things Report 2020.*  

[5] NIST.  
**CVE-2020-11901 Details.**  

[6] NIST.  
**CVE-2020-24338 Details.**  

*A secure iot service architecture with an efficient balance dynamics based on cloud and edge computing.*  
*IEEE Internet of Things Journal* 6, 3 (2018), 4831–4843.

Dominance as a New Trusted Computing Primitive for the Internet of Things.