Advanced System Resiliency Based on Virtualization Techniques for IoT Devices

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

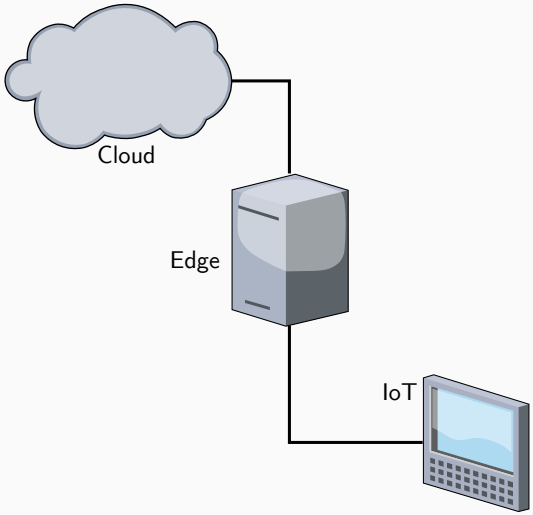
jonas.roeckl@fau.de
https://www.cs1.tf.fau.de/person/jonas-roeckl/

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

9 December 2021

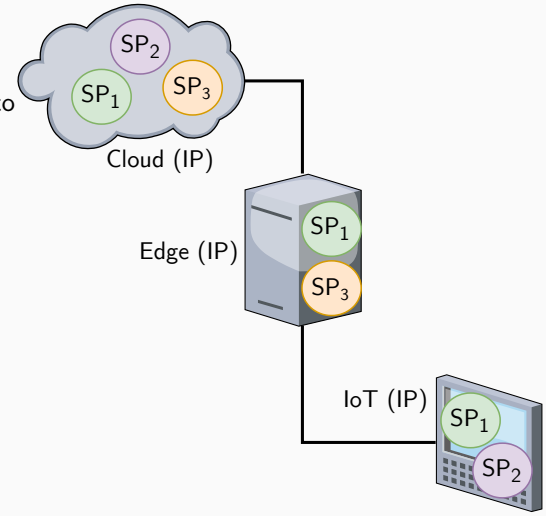
Motivation

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



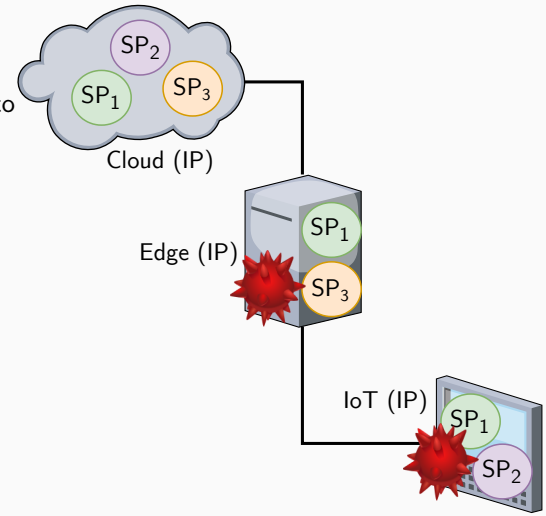
Motivation

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



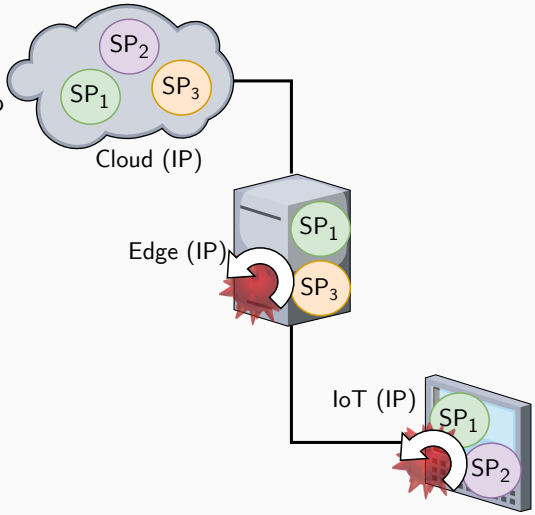
Motivation

- 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



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

Dominance (Xu et al. [8])

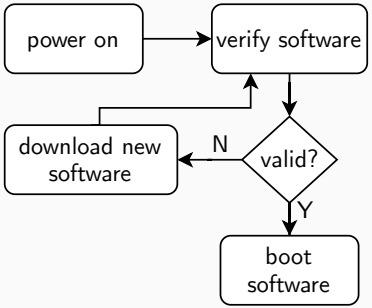
The hub dominates a device if the hub can choose arbitrary code and force the device to run it within a bounded amount of time.

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

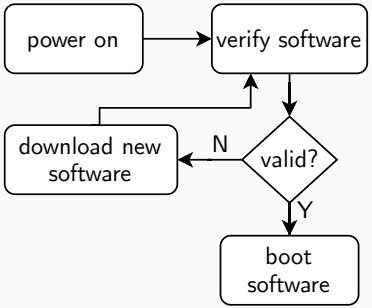


Dominance

Dominance (Xu et al. [8])

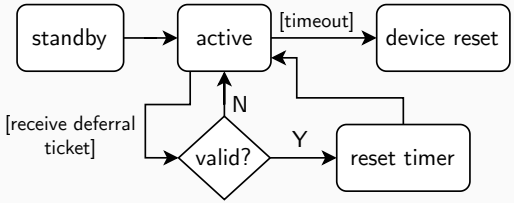
The hub dominates a device if the hub can choose arbitrary code and force the device to run it within a bounded amount of time.

Gated Boot



Reset Trigger

Authenticated Watchdog Timer (AWDT)



Novel Trusted Computing Concepts

Strong Dominance

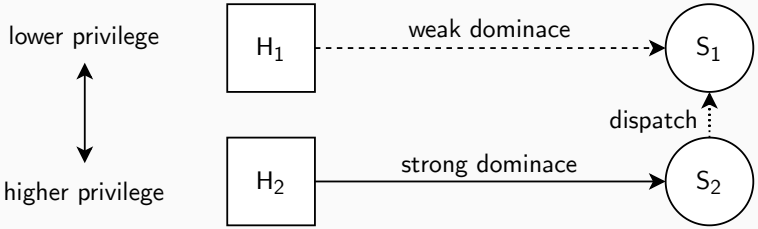
Dominance (Xu et al. [8])

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



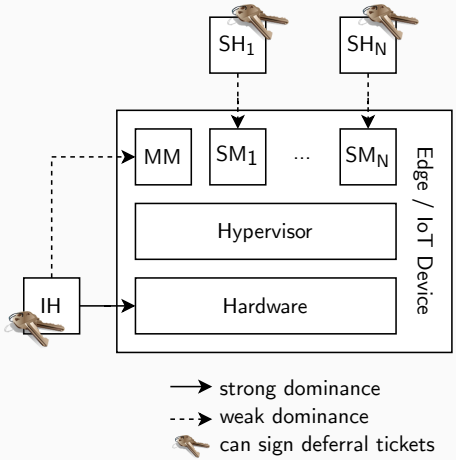
Weak Dominance

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.

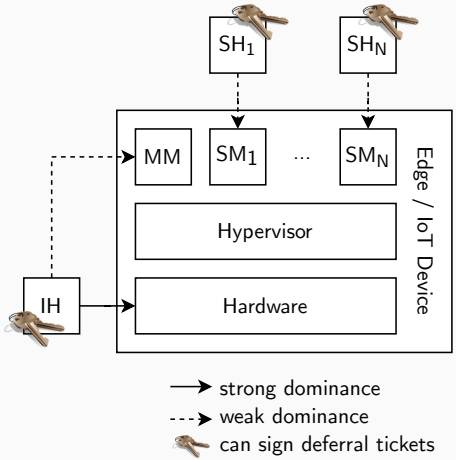
System Architecture

System Architecture



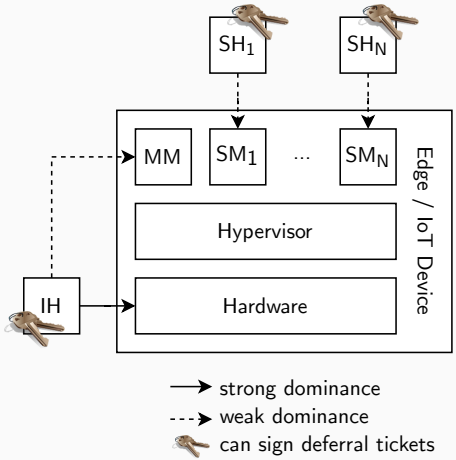
- Service Machines (SMs)
  - Weakly dominated by a Service Hub (SH)
  - Encapsulate services

System Architecture



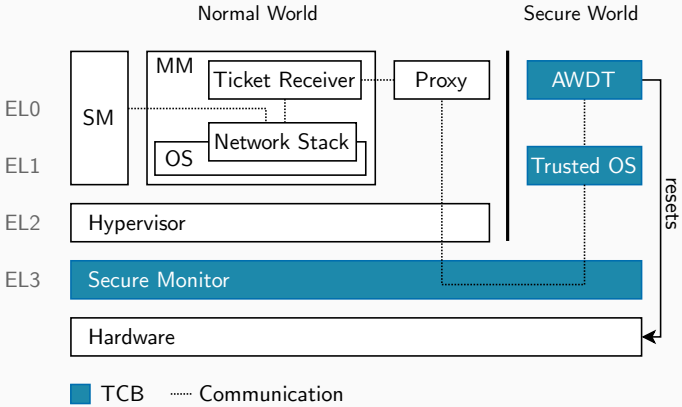
- Service Machines (SMs)
  - Weakly dominated by a Service Hub (SH)
  - Encapsulate services
- Management Machine (MM)
  - Weakly dominated by an Infrastructure Hub (IH)
  - Isolates the network stack during runtime
  - Provides dominance-related functionalities

System Architecture



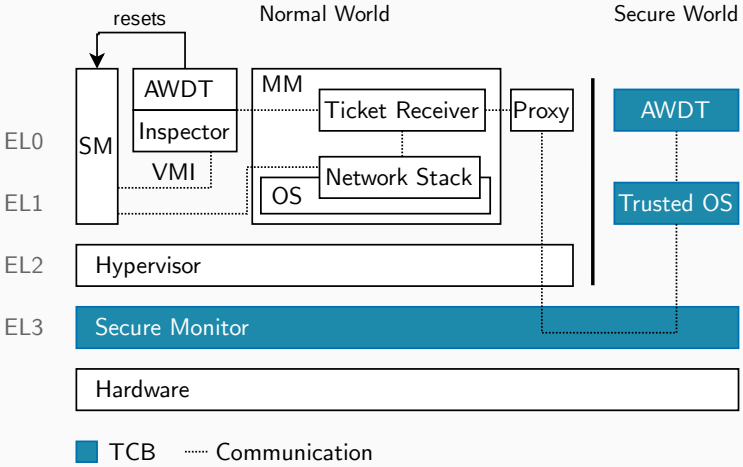
- Service Machines (SMs)
  - Weakly dominated by a Service Hub (SH)
  - Encapsulate services
- Management Machine (MM)
  - Weakly dominated by an Infrastructure Hub (IH)
  - Isolates the network stack during runtime
  - Provides dominance-related functionalities
- An SP can recover a weakly dominated SM even after a severe software compromise
- Even in case of an VM espace: The IH can still recover the device

Achieving Strong Dominance



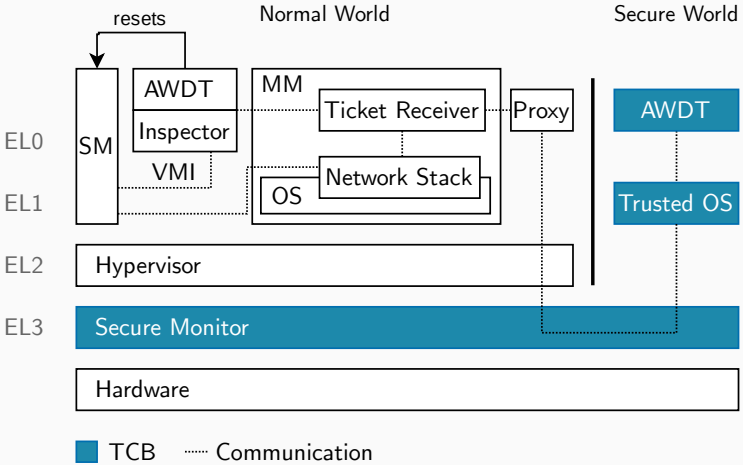
- During boot: Gated Boot
- Ticket Receiver acquires deferral ticket from IH regularly
- TCB compromise: No remote recoverability any longer

Achieving Weak Dominance



- During VM boot: *Virtual Gated Boot*

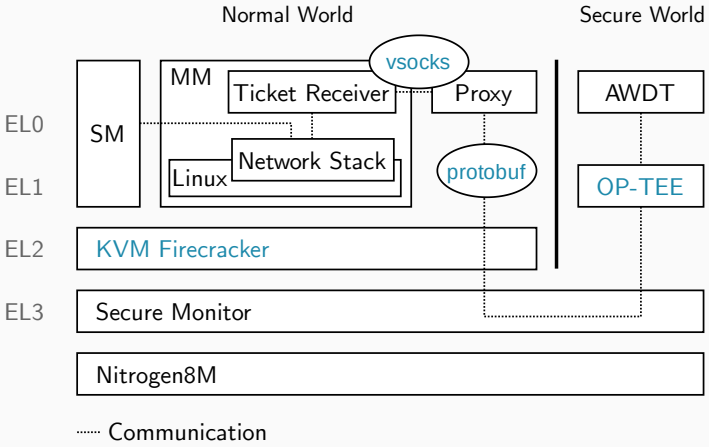
Achieving Weak Dominance



- 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

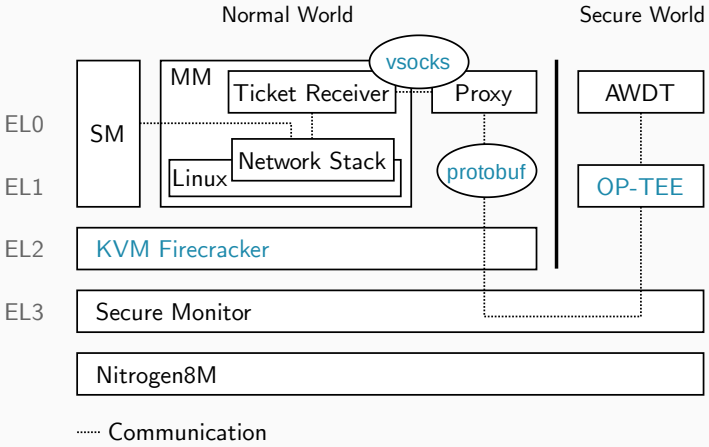
Implementation and Evaluation

Implementation and Evaluation



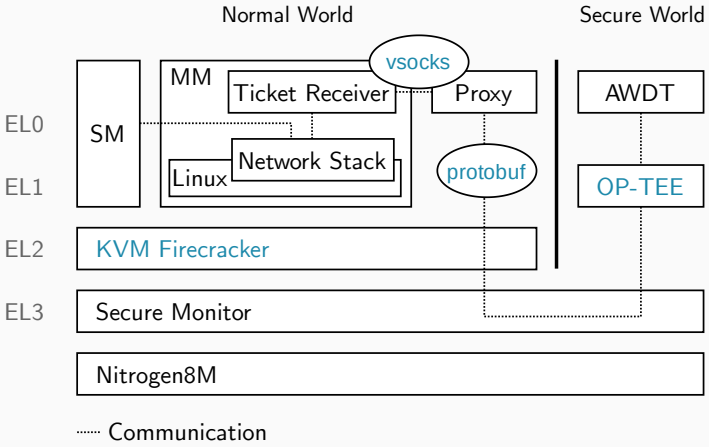
- Boundary Devices Nitrogen8M, Cortex A-53, 2GB RAM

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

Summary

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)

References

[1] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., and Zhou, Y.
Understanding the Mirai Botnet.
In *26th USENIX Security Symposium (USENIX Security 17)* (Vancouver, BC, Aug. 2017), USENIX Association, pp. 1093–1110.

[2] Gartner.
Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016.
`https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016`, 2017.
Accessed 2021-04-25.

[3] Herwig, S., Harvey, K., Hughey, G., Roberts, R., and Levin, D.
Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet.
In *NDSS* (2019).

References (cont.)

[4] Insider, B.
Internet of Things Report 2020.
`https://www.businessinsider.com/internet-of-things-report`, 2020.
Accessed 2021-04-25.

[5] NIST.
CVE-2020-11901 Details.
`https://nvd.nist.gov/vuln/detail/CVE-2020-11901`, 2020.
Accessed 2021-04-25.

[6] NIST.
CVE-2020-24338 Details.
`https://nvd.nist.gov/vuln/detail/CVE-2020-24338`, 2020.
Accessed 2021-04-25.

[7] Wang, T., Zhang, G., Liu, A., Bhuiyan, M. Z. A., and Jin, Q.
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.

References (cont.)

[8] Xu, M., Huber, M., Sun, Z., England, P., Peinado, M., Lee, S., Marochko, A., Mattoon, D., Spiger, R., and Thom, S.
Dominance as a New Trusted Computing Primitive for the Internet of Things.
In *2019 2019 IEEE Symposium on Security and Privacy (SP)* (Los Alamitos, CA, USA, may 2019), IEEE Computer Society, pp. 1223–1238.