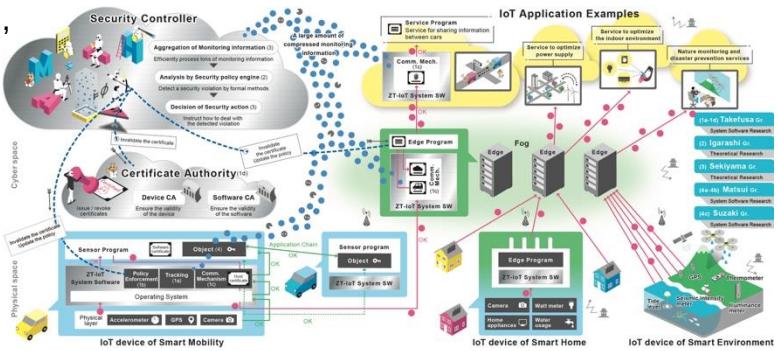
Zero Trust based IoT Security

https://zt-iot.nii.ac.jp/en/

This project aims to realize **secure Internet of Things (IoT)** systems by the concept of **zero trust** by the fusion of **formal verification** and **system software** technologies. In formal verification research, we provide mathematical proofs for the legitimacy of IoT trust chains and address undiscovered threats by combining static and dynamic verification. In system software research, we develop mechanisms for isolated execution, automatic detection and automatic countermeasures in conjunction with the theoretical results to demonstrate **zero trust IoT (ZT-IoT)**.



System Software

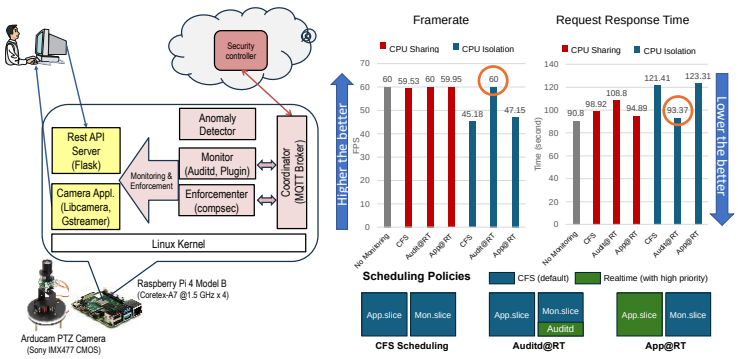
Resilience of IoT Software (SW)

- ***Software certification framework (SCF)*** to assure SW reliability, where the user can confirm:
  - Integrity of the SW by the digital signature of the SW developer/integrator
  - Vulnerability assessment results with the digital signature by the authorized third-party organization.
  - Prototype implementation to assess container-based SW using CI/CD pipelines with GitHub Actions, Docker Scout and digital signature by OpenSSL.
- ***Over-the-air (OTA) SW update framework***[*1] for SW life cycle management:
  - Deploy reliable SW to IoT devices co-working with SCF.
  - Automatically update installed vulnerable SW.

[*1] N. Aoki, A. Takefusa, Y. Ishikawa, Y. Ono, E. Sakane, K. Aida, "ZT-OTA Update Framework for IoT Devices toward Zero Trust IoT," Proc. COMPSAC, NETSAP, Jul. 2024.

Monitoring & Policy Enforcement

- A monitoring and enforcement framework[*2] based on Linux Audit and MQTT for IoT devices is being designed and implemented.
- While many existing works using Linux Audit have pointed out undesirable runtime overhead to the system, applying proper Linux ***cgroup*** carries out a real-time execution environment for application and system security monitoring as shown in the right figure.

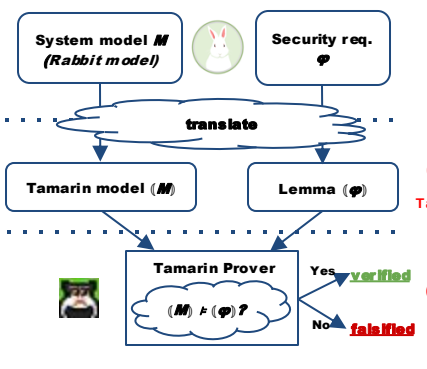


[*2] J. Yin, Y. Ishikawa, A.Takefusa, "A Linux Audit and MQTT based Monitoring Framework for IoT Devices and Its Evaluation," IPSJ Journal vol. 34 No. 8, Aug. 2024.

Formal Verification

- ***Rabbit*** [*3] is a system modeling language for formally verifying cybersecurity, its main target being non-experts in formal verification.
- System models can be described by using OS-level notions (such as processes, channels and files) and access control mechanism *à la* SELinux.
- The (current) implementation of Rabbit works as a translator to the input lang. of the Tamarin Prover, a model checker designed for security protocols.

This work was supported by JST, CREST Grant Number **JPMJCR21M3.**



[*3] T. Inaba, Y. Ishikawa, A. Igarashi, T. Sekiyama. "Rabbit: A Language to Model and Verify Data-Flow in Networked Systems," Proc. ISNCC, Oct. 2024.

ZT-IoT

NII posters are available at: