SAND2019-3610C

CERIAS

The Center for Education and Research in Information Assurance and Security

IoT2 – A Security Benchmark for the Internet of Things

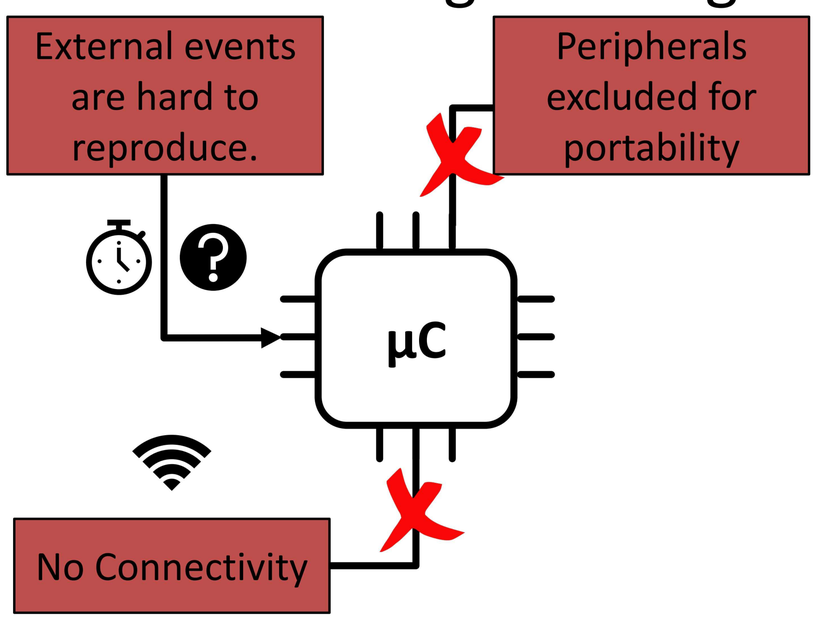
Naif Saleh Almakhdhub, Abraham A. Clements, Mathias Payer, and Saurabh Bagchi

Microcontroller-based IoT systems (IoT-µCS)

A significant portion of the IoT.

- Examples:
  - Wifi SoC.
  - Amazon Dash Button.
- Traditionally an isolated system with no network connectivity.
- Suffers from poor security practices.
- Increasingly under attack with the rise of IoT.

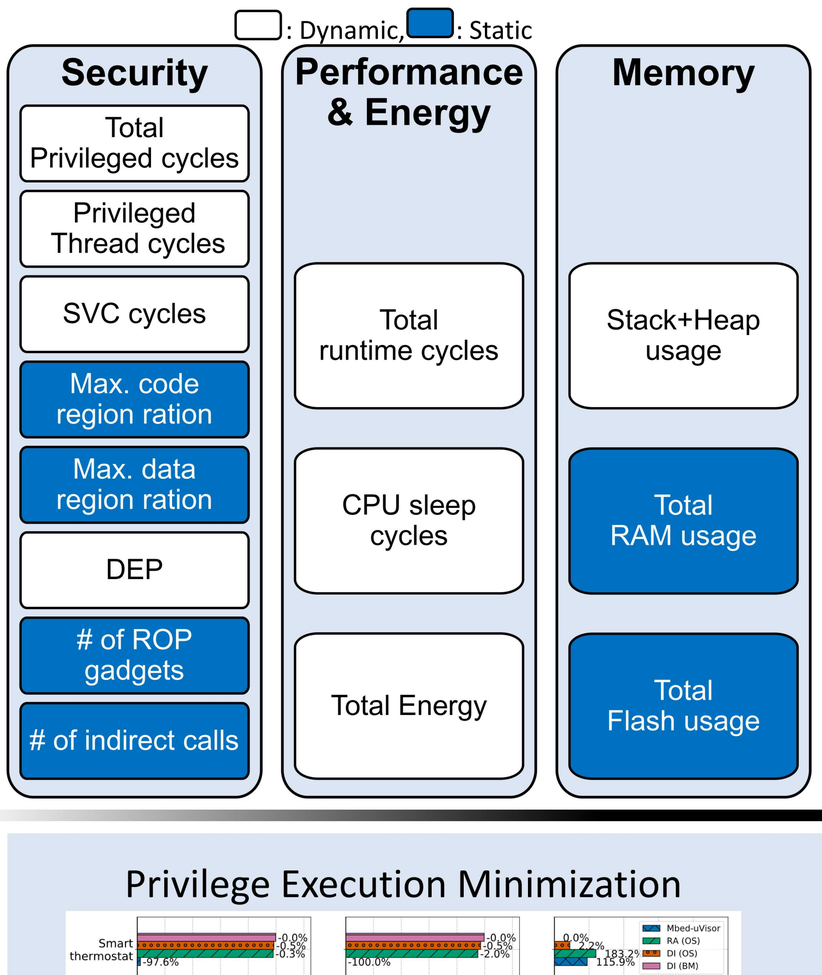
Benchmarking Challenges



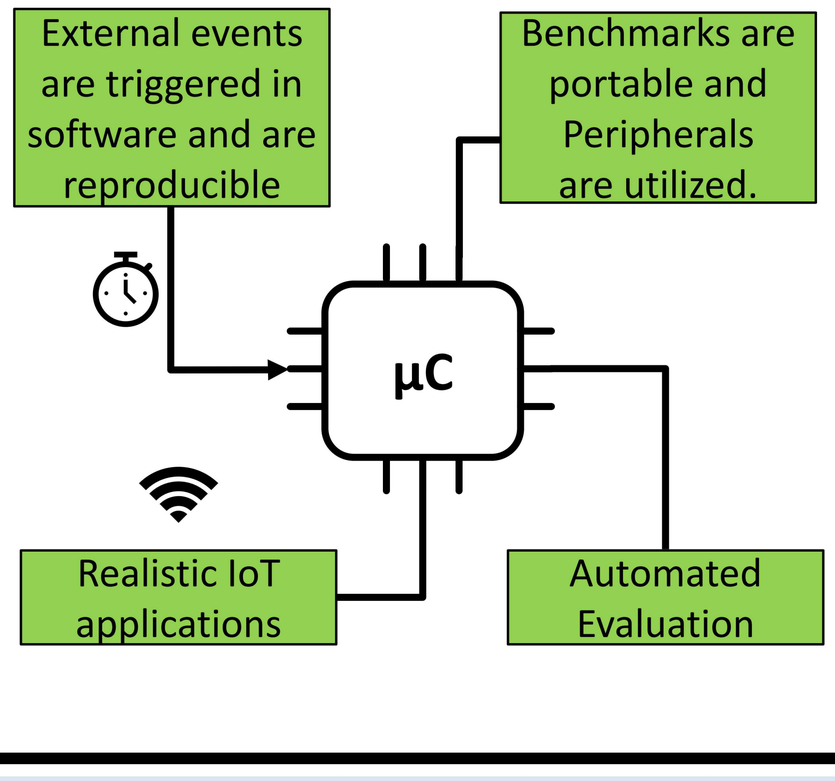
Evaluation Challenges

- IoT-µCS are constrained systems with limited Flash, RAM, and Energy.
- Evaluation is limited, manual, and tedious.
- Evaluation often depend on additional hardware.
- Security evaluation became ad-hoc as a result.

Evaluation metrics



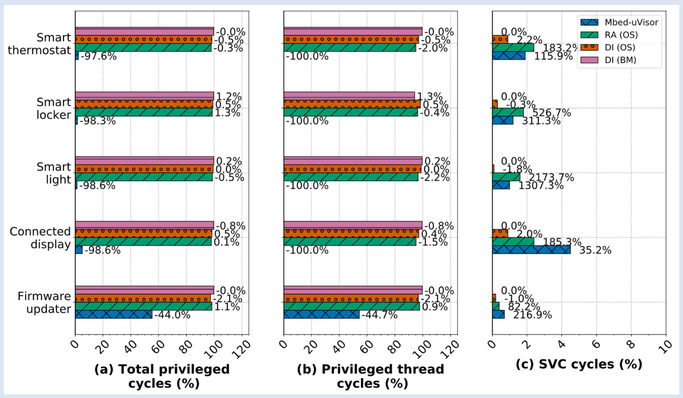
Our Solution: IoT2



Benchmarks

Benchmark	Task Type			Peripheral
	Sense	Compute	Actuate	
Smart Light	✓	✓	✓	Low-power Timer, GPIO, Real-time clock
Smart Thermostat	✓	✓	✓	ADC, Display, GPIO, uSD card
Smart-locker		✓	✓	Serial (UART),Display, uSD Card , Real-time clock
Firmware Updater		✓	✓	Flash in-application programming
Connected Display		✓	✓	Display, uSD Card

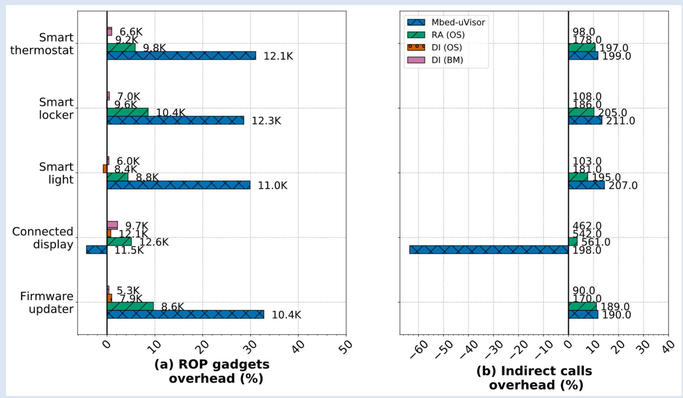
Privilege Execution Minimization



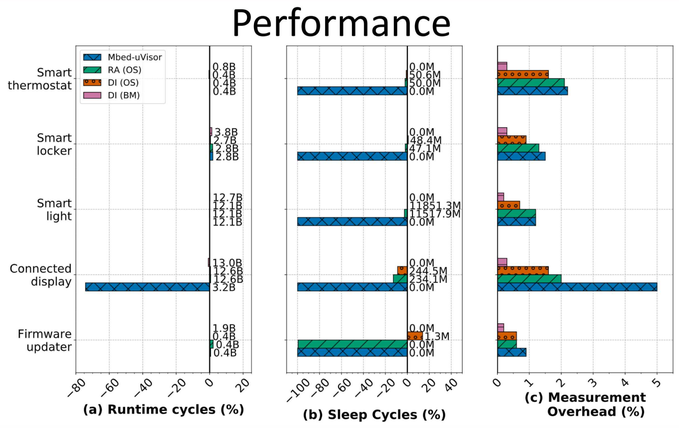
Security Evaluation

Defense	Memory Isolation and Code injection Metrics		
	Max code Reg. ratio	Max data Reg. ratio	DEP
Mbed-uVisor	1.0	1.0	✖
Remote Attestation (OS)	0.99	1.0	✓
Data Integrity (OS)	1.0	0.99	✖
Data Integrity (Bare-metal)	1.0	0.99	✖

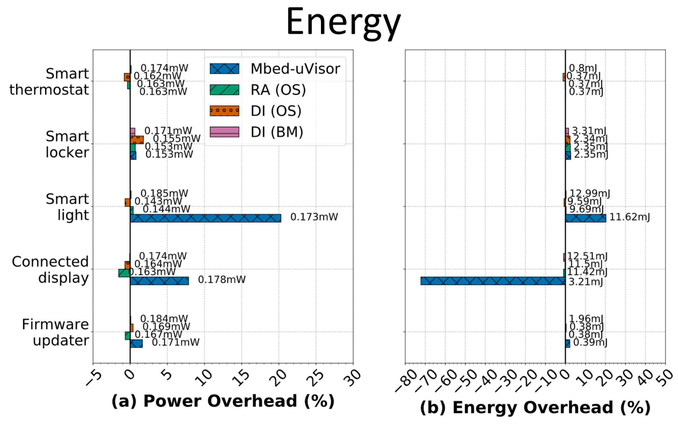
Code Reuse Protection



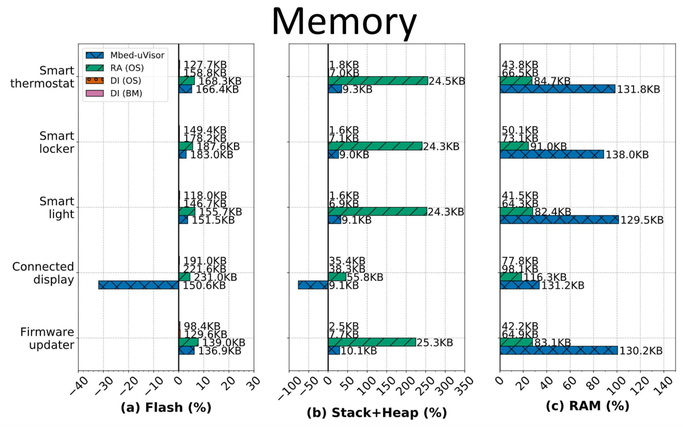
Performance



Energy



Memory



Our Team

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.