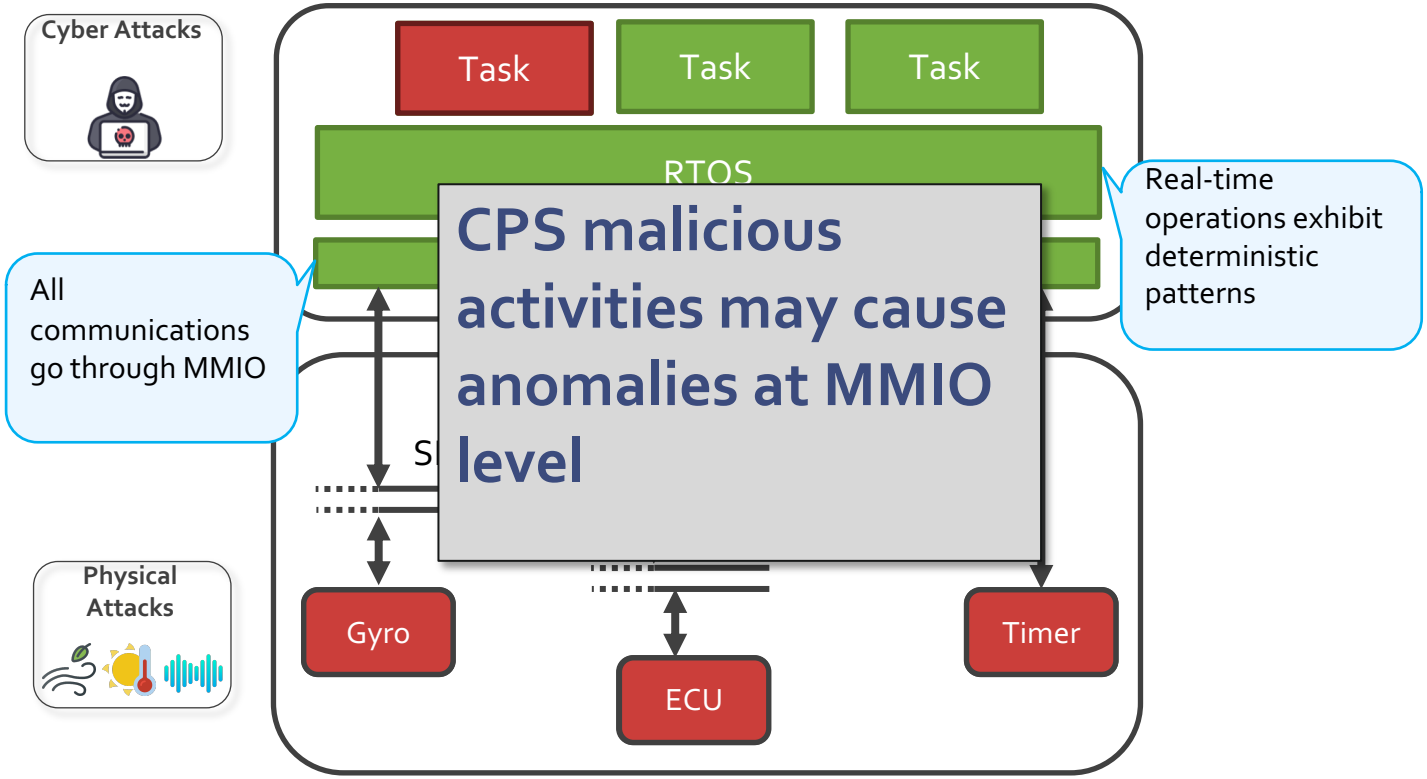
M2MON: Building an MMIO-based Security Reference Monitor for Unmanned Vehicles

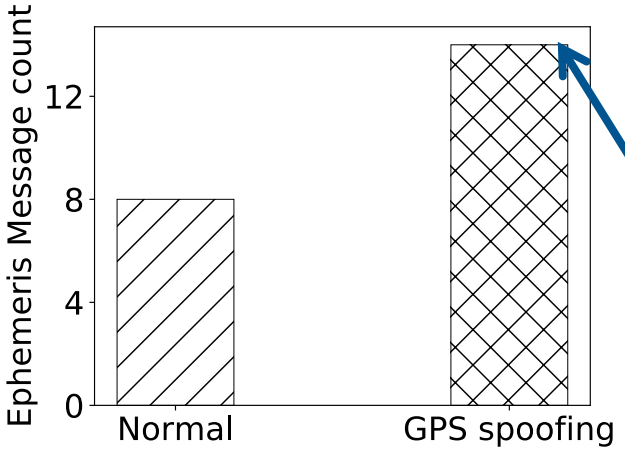
Arslan Khan†, Hyungsub Kim†, Byoungyoung Lee*, Dongyan Xu†,
Antonio Bianchi†, Dave (Jing) Tian†
†Purdue University
* Seoul National University

Motivation


Cyber Attacks
Task
Task
Task
RTOS
Real-time operations exhibit deterministic patterns
All communications go through MMIO
CPS malicious activities may cause anomalies at MMIO level
Physical Attacks
Gyro
ECU
Timer

Example of attack showing I/O anomaly

GPS Spoofing



Higher count of ephemeris message in case of spoofing.

More examples of attacks showing I/O anomalies

	Cryp…	[40]	[7]	…iew	…[44]	I/O Level Anomaly
Timer Attack [6]						■
IRQ Override [6]						■
CAN Masquerading [28]						■
Radio Replay [23]						■
Malicious Sensor [37]						◪
Flash Patch Attack [6]	–	–	–	–	–	■
GPS Spoofing [25]	■	–	–	–	–	■
Gyroscope Attack	–	–	–	–	■	■
Barometer Attack	–	–	–	–	■	■

We are motivated to build an I/O Reference Monitor for CPS.

M2MON

M2MON is an MMIO-based

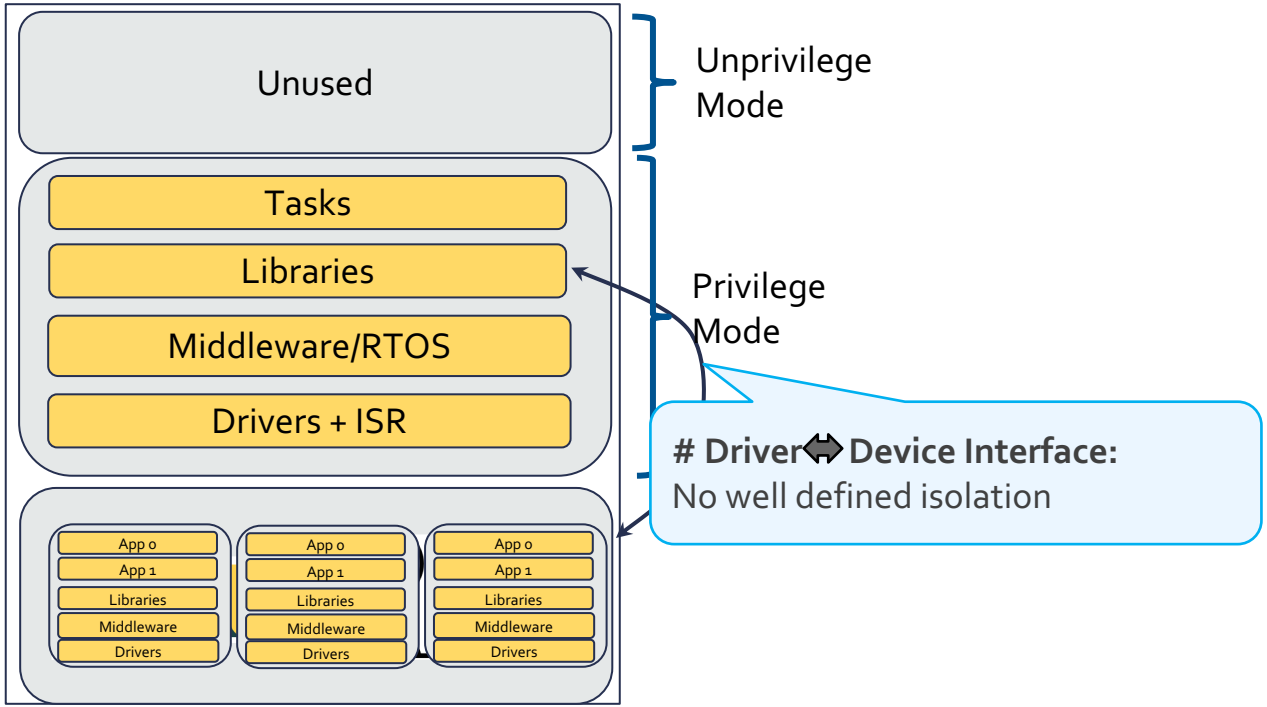
Security Reference Monitor

An untamperable, non-bypassable, always-invoked and evaluable module that controls all accesses to data objects or devices.

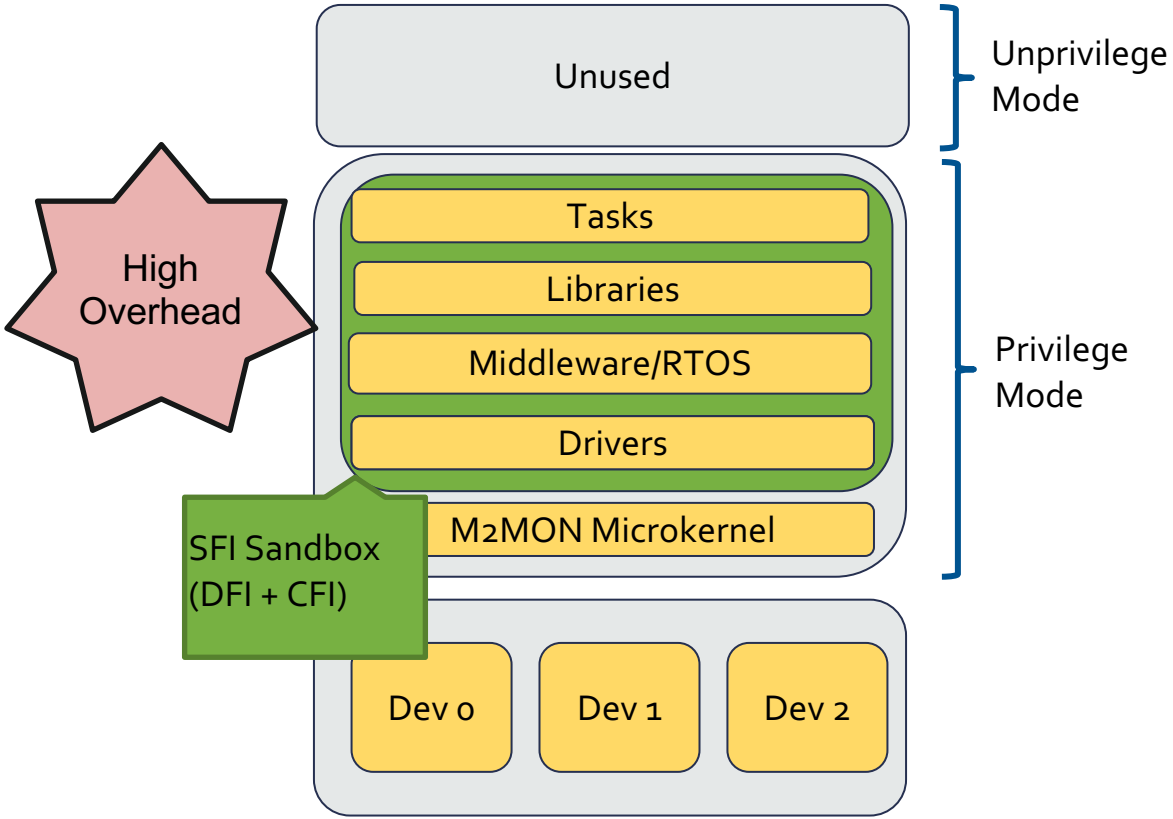
Design Challenges

Many real-time, low-power CPS have:

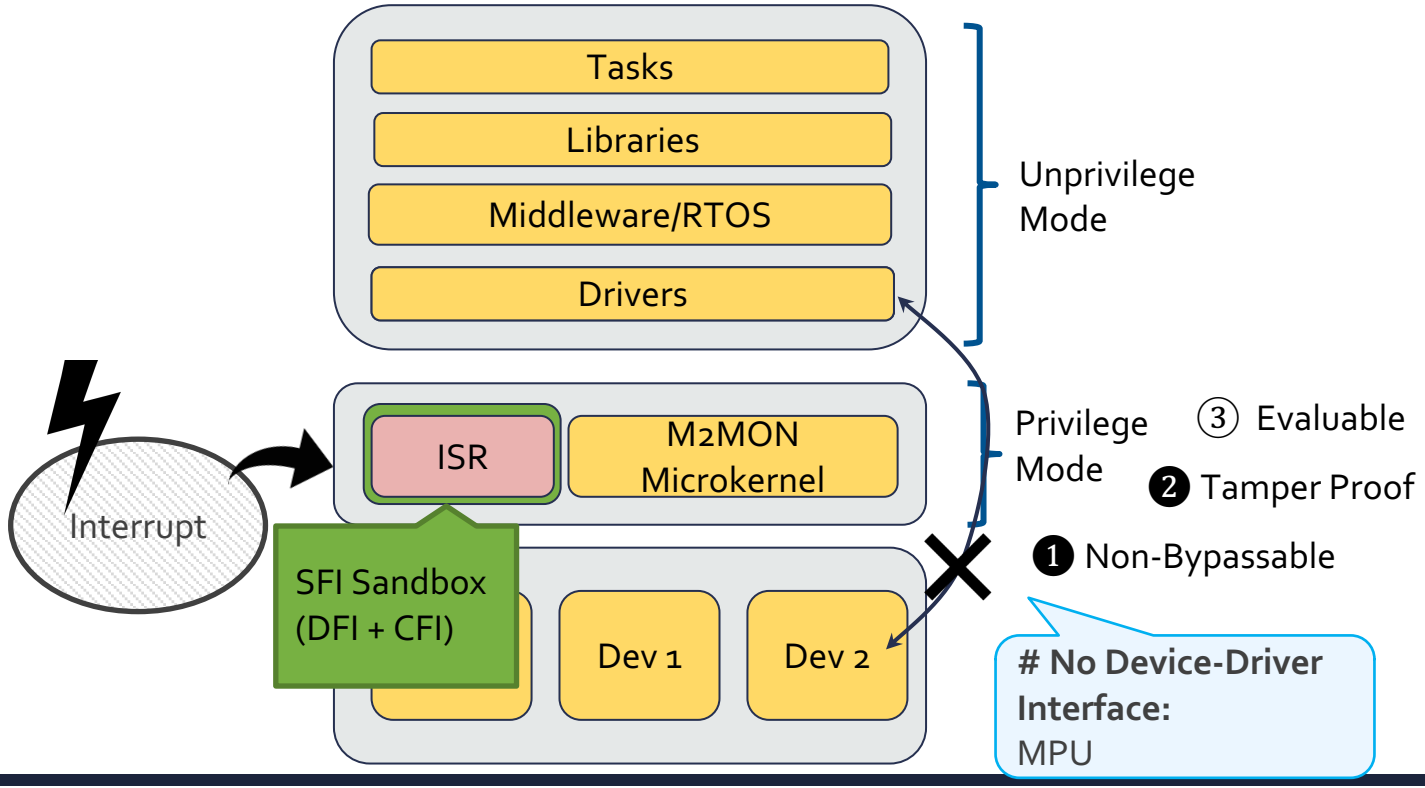
- No privilege separation (i.e., user space/kernel space)
- No MMU and Fewer Execution Modes



M2MON Design



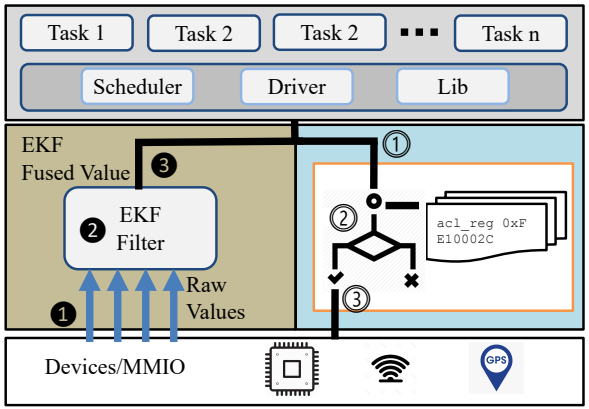
M2MON Design



M2MON Applications

Instantiation of M2MON Microkernel

- To detect multiple types of attacks against drone
  - Kalman Filter
  - Access Pattern Filter
    - Access Frequency
    - Access Chain
    - Access List

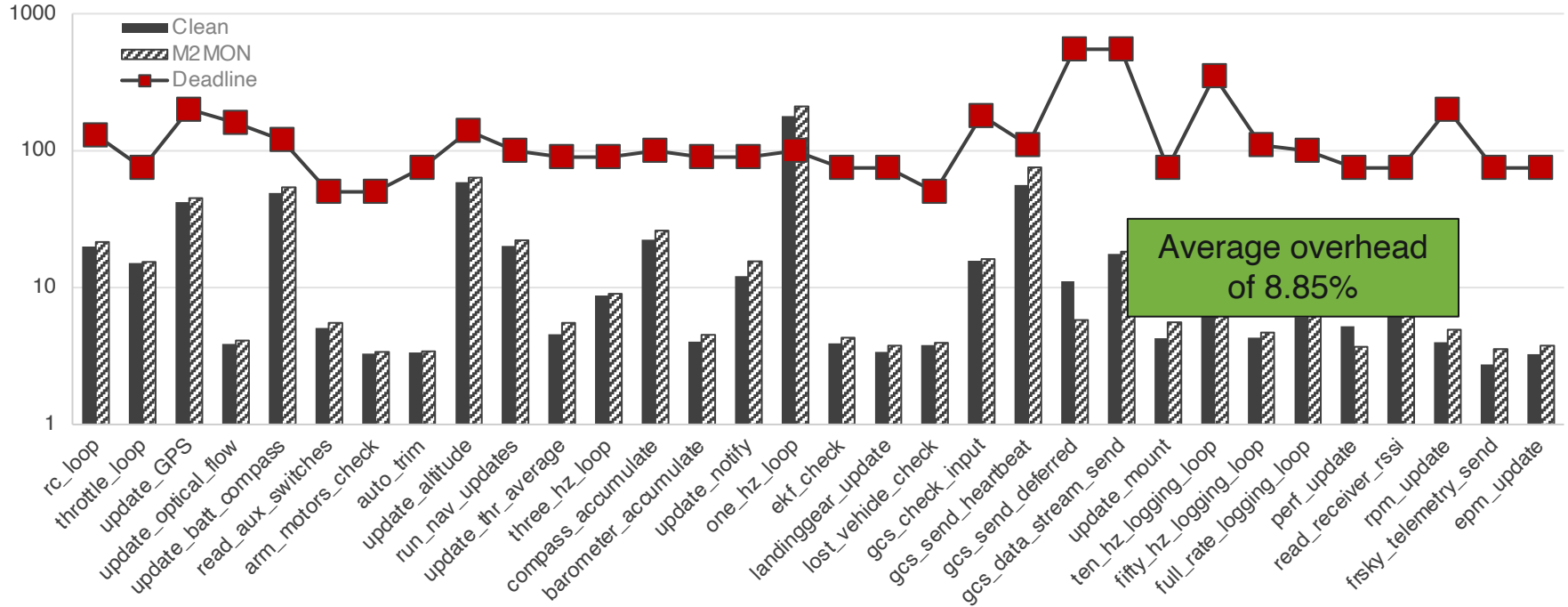


Evaluation

- Platform
  - 3DR IRIS+ UAV platform
  - Ardupilot
- Evaluation
  - Performance Evaluation
  - Security Evaluation

ARDUPILOT
Versatile, Trusted, Open

Performance Evaluation

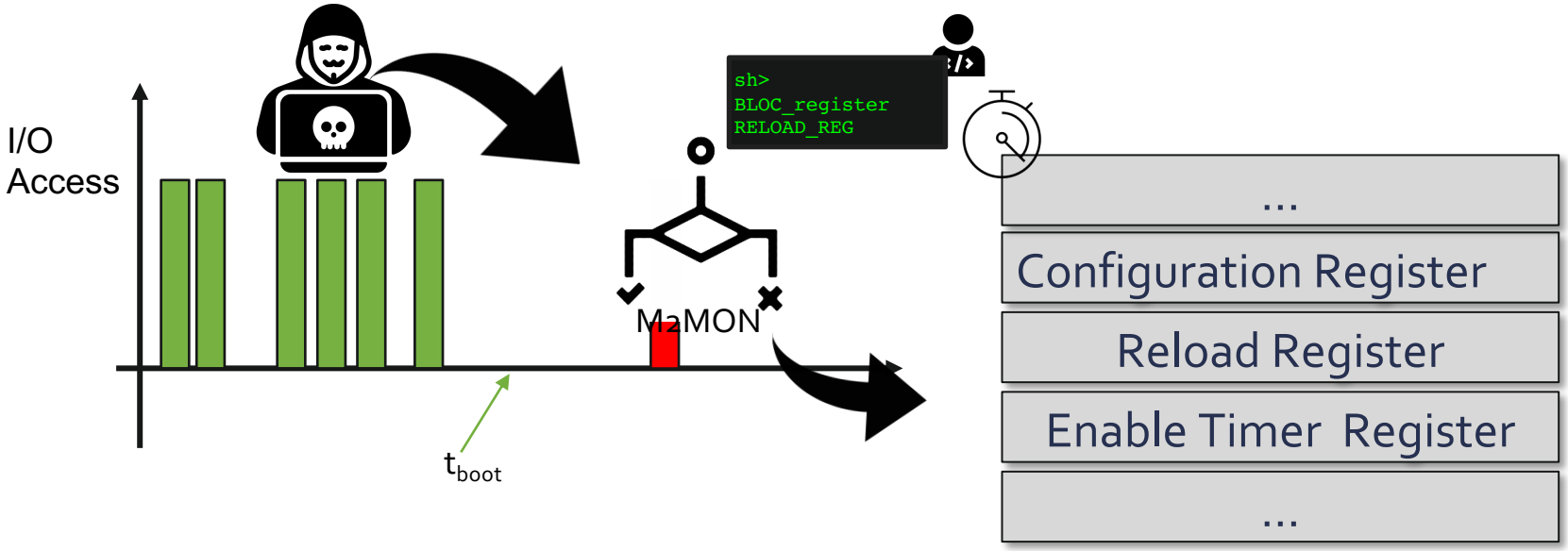


Security Evaluation

Case ID	Attack	Detection Feature	ress
1	Timer Attack	Access List	
2	IRQ Override	Access List	Vector Table Offset Register
3	Radio Replay	Access Frequency	GPIO Status Register
4	Flash Patch Attack	Access List	FPB Control Register
5	GPS Spoofing	Access Frequency	UART Data Register
6	Gyroscope Attack	Access List	Device ID 1 Command (SPI)
7	Barometer Attack	Access Chain	Device ID 3 Command (SPI)
8	Malicious Sensor values	Kalman Filtering	Data registers related to sensor values

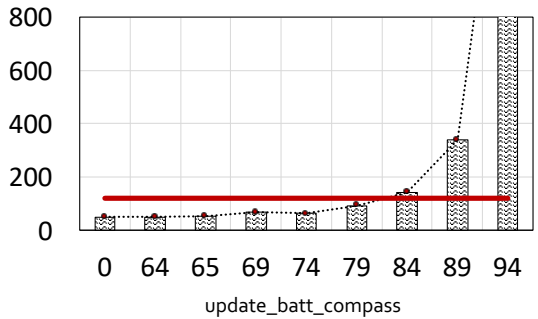
Checked by M2MON microkernel

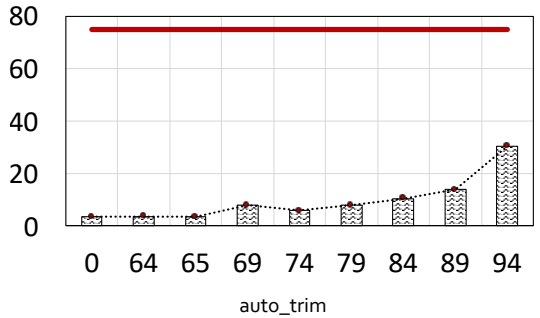
Case study (Timer Reload)

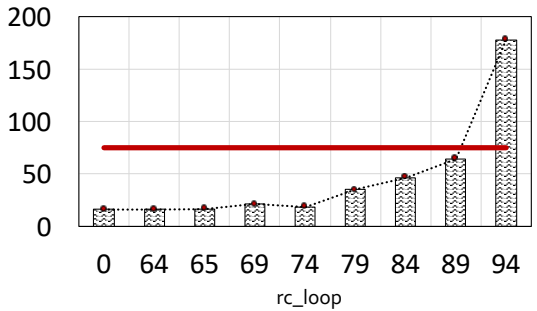


Limitations

- Complex Rules
- Zero-day attacks







Conclusion

- CPS attacks against drones usually exhibit MMIO-level anomalies
- M2Mon: a reference monitor for MMIO anomaly detection
  - MMIO Microkernel
  - Multiple Applications of MMIO Microkernel
  - Reasonable overhead on real drone controller
  - Detect a wide range of attacks

Thank you!
Questions?

khan253@purdue.edu

*This work was supported in part by ONR under GrantsN00014-20-1-2128 and N00014-17-1-204. This material is also based on research sponsored by DARPA under contract number N6600120C4031.

PURDUE UNIVERSITY

CERIAS

PurSec Lab