Towards Non-intrusive Malware Detection for Industrial Control Systems

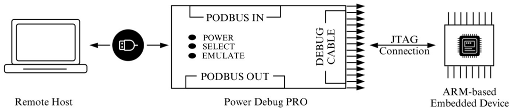
Prashant Rajput, Michail Maniatakos

BACKGROUND & MOTIVATION

- IoT devices are being integrated into the OT sector, bringing along its vulnerabilities.
- Traditional malware detection solutions cannot be directly applied to OT devices such as PLCs due to constraints such as:
  - Limited computation capabilities
  - Real-time requirements
  - Legacy OS
- WAGO PFC100 Controller operates at 600 MHz with 256MB RAM.

NEW INSIGHTS

JTAG is an OS-independent standard for system-level platform debugging



- JTAG, an IEEE 1149.1 standard, can gather relevant data from main memory.
- Perform out-of-the-device virtual to physical address translation.
- Extract data non-intrusively from a PLC device and perform computation externally.

DESCRIPTION

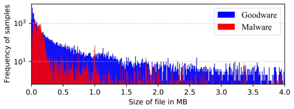
Non-intrusive out-of-the-device ML-based static analysis malware detection

Methodology

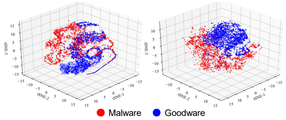
- Extract features
  - 256x256 matrix of entropy values traversing on a Hilbert curve.
  - Hashed strings to create a 16x16 histogram.
  - Hashed system calls to create a 16x16 histogram.
- Preprocess and downsample collected features.
- Amaya employs SVM for classification.

Dataset

- ARM (Malware: 4,614, Goodware: 4,647)
- x86_64 (Malware: 3,042, Goodware: 3,042)



[Fig. 1]

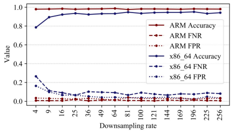


[Fig. 2]

Assumptions & Limitations

- Availability of an accessible JTAG port.
- Limited OS knowledge.
- Extracting data through JTAG is slow.
- Partial binary retrieval.
- Overwrite OSLAR register

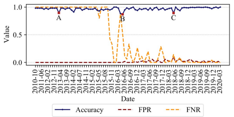
QUANTITATIVE IMPACT



[Fig. 3]

Accuracy

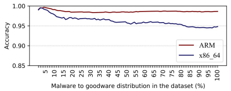
- SVM for classification
- **ARM:** 98%, [DSR 64]
- **x86_64:** 94.7%, [DSR 81]



[Fig. 4]

Concept Drift

- ML-model requires retraining.
- SVM model for ARM is more resilient.



[Fig. 5]

Spatial Experimental Bias

- **ARM:** above 98%
- **x86_64**: below 95%

CONCLUSION

- Amaya is a non-intrusive out-of-the-device, ML-based static analysis malware detection tool for OT devices.
- Utilize JTAG for non-intrusive memory access.

Contact: Prashant Rajput, *NYU Tandon School of Engineering, prashanthrajput@nyu.edu*

github.com/momalab/amaya