Remote Non-Intrusive Malware Detection for PLCs based on Chain of Trust Rooted in Hardware

Prashant Hari Narayan Rajput[1*], Esha Sarkar[1], Dimitrios Tychalas[1], Michail Maniatakos[2]

[1]Tandon School of Engineering, New York University
[2]Center for Cyber Security, New York University Abu Dhabi
*Speaker

Euro S&P 2021

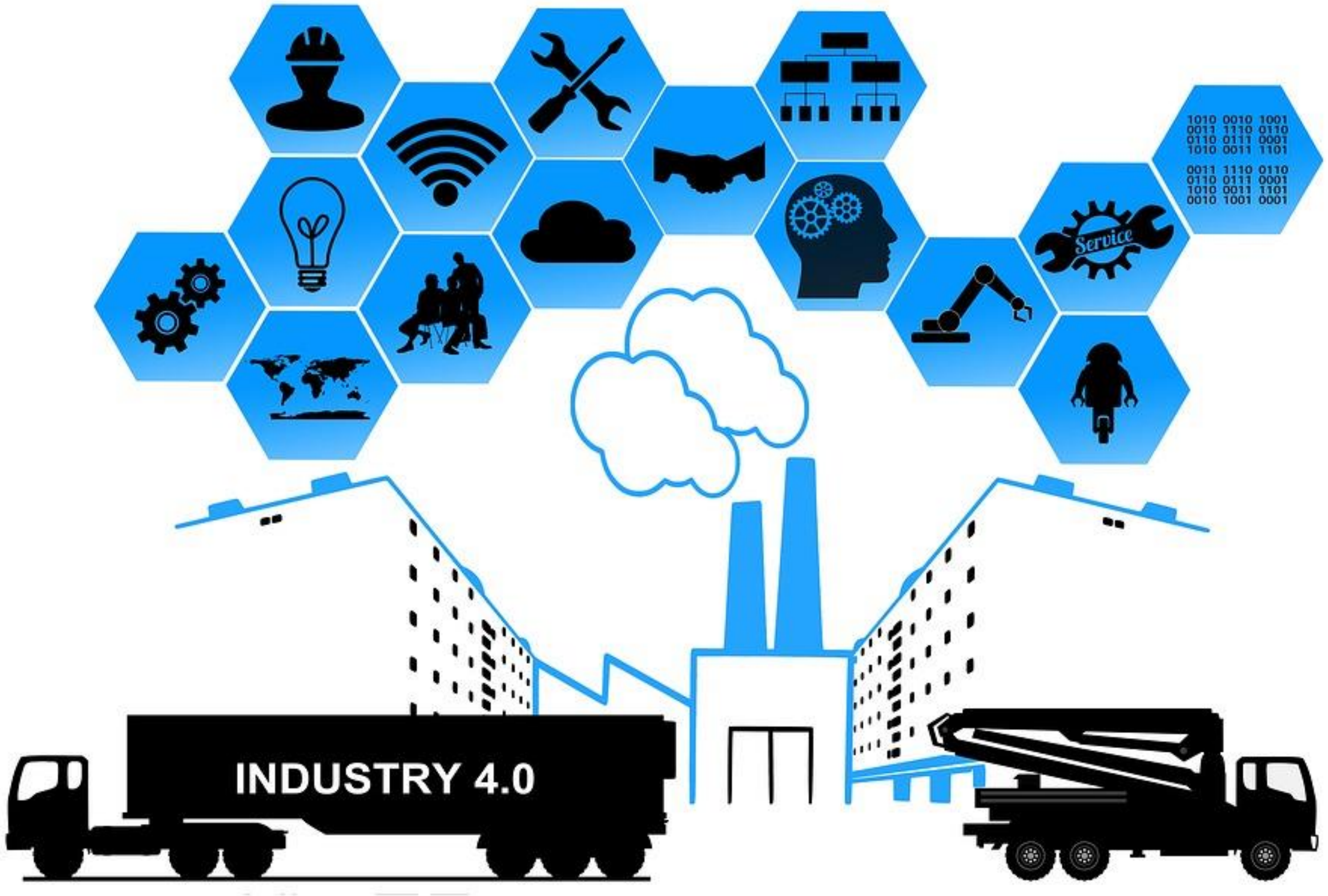
06/09/21

Industry 4.0

And its security aspects

- Improves industry output by integrating IoT with OT.

- **<u>ICS constraints</u>**
- Limited computational capabilities
- Realtime requirements
- Limited OS support



. [1] I-Scoop. (2020) Industry 4.0: the fourth industrial revolution – guide to industrie 4.0. [Online]. Available: https://www.i-scoop.eu/industry-4-0/

Contributions

Research question

Is it possible to detect malware on an ICS device non-intrusively without disrupting industry operation, in real-time?

ORRIS

- Novel methodology for JTAG-based non-intrusive PLC monitoring for malware
- ORRIS evaluation using spatial bias and unseen malware samples
- End-to-end case-study of desalination plant using ORRIS
- Development of an ARM-based malware dataset

Threat model

Chain of trust established by ORRIS

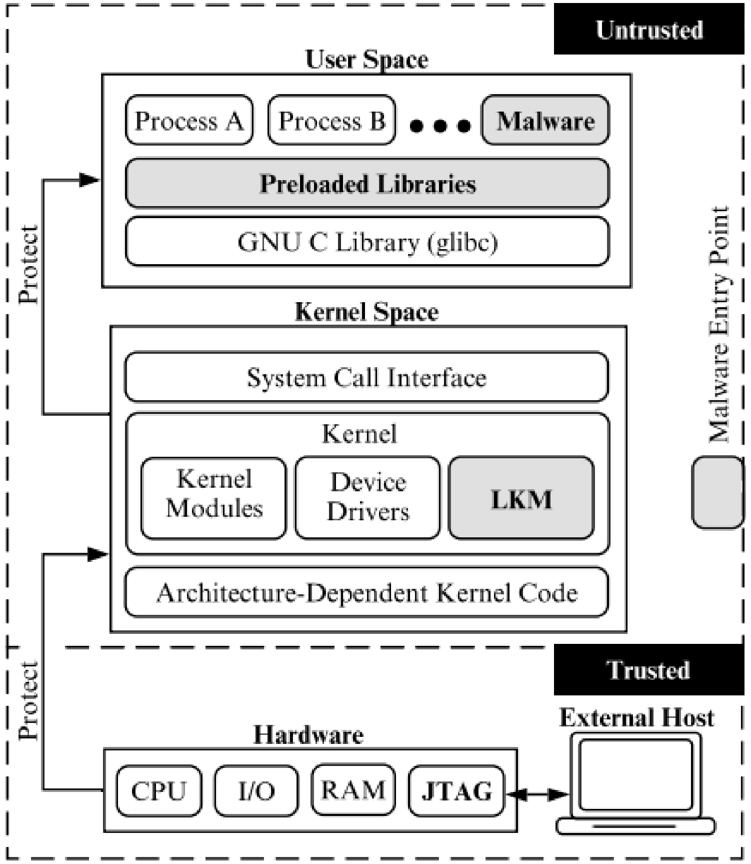


Fig. 1: Chain of trust

- Adversary can obtain elevated privileges
- Can exploit vulnerabilities in the PLC OS

- JTAG establishes a hardware root of trust
- Hardware –> Kernel space –> User space

Designing ORRIS

Kernel-level rootkits

- Protection against rootkit that alter static kernel data structures
- Set watchpoint over syscall table
- Monitor for any write operation over the table (watchpoint)

User-level rootkits

- Hook to write syscall
- Monitor writes on /etc/ld.so.preload
- Get file path and use static features for detection

Malware

- Extract semantic and microarchitectural event counts
- Check the overall state of the PLC

Malware detection methodology

- Feature collection with JTAG
- Balancing sampling rate for performance and responsiveness

Pre-processing of malware dataset

- <u>Manual scrubbing</u>: Remove constants, static identifiers, zeroes, process identifiers, and memory addresses
- <u>Statistical:</u> Standard scaling with 99.75% accuracy

Machine learning based models

- MI between output labels and features reduces the feature set by 39.
- OCSVM –> user-level rootkit
- SVM –> malware (99.75%)

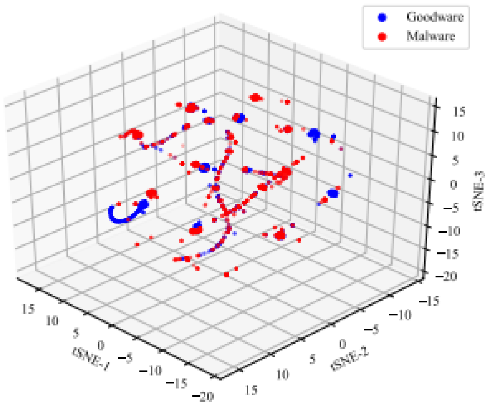


Fig. 3(a): TSNE on un-processed data

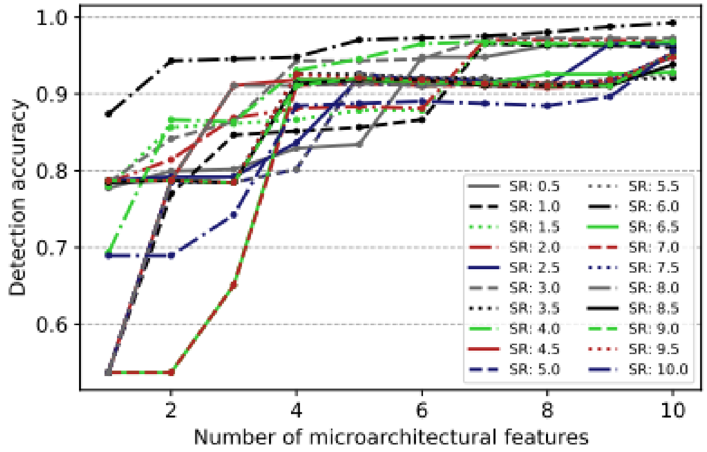


Fig. 2: Realtime detection

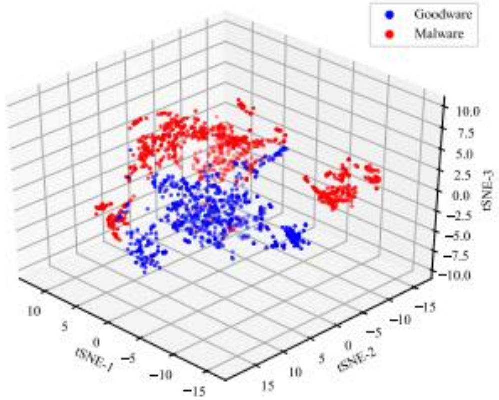


Fig. 3(b): TSNE on scaled features

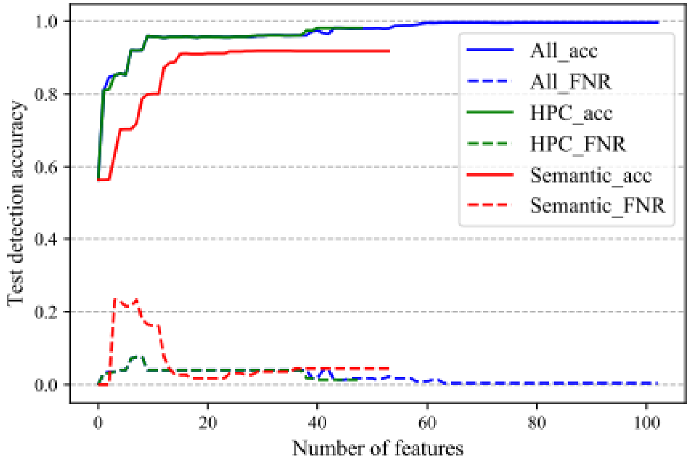


Fig. 4: Malware detection accuracy

Evaluation of ORRIS (1/2)

Testing rootkit detection and real-time implementation

Kernel-level Rootkits

- Detected all the 11 tested kernel-level rootkits

User-level Rootkits

- 4 rootkits vs. 425 shared libraries
- Accuracy of 96.3% with TNR of 96.2%
- 3.8% shared libraries are misclassified

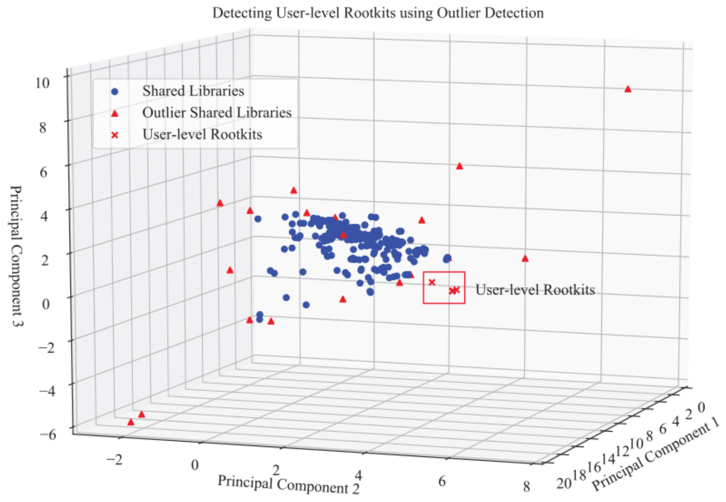


Fig. 5: Outlier detection for user-level rootkits

- Hardware-in-the-Loop simulation of MSF desalination plant
- ORRIS on a Test PLC that closes a steam flow valve at high brine temperature
- No observed delay on control logic execution

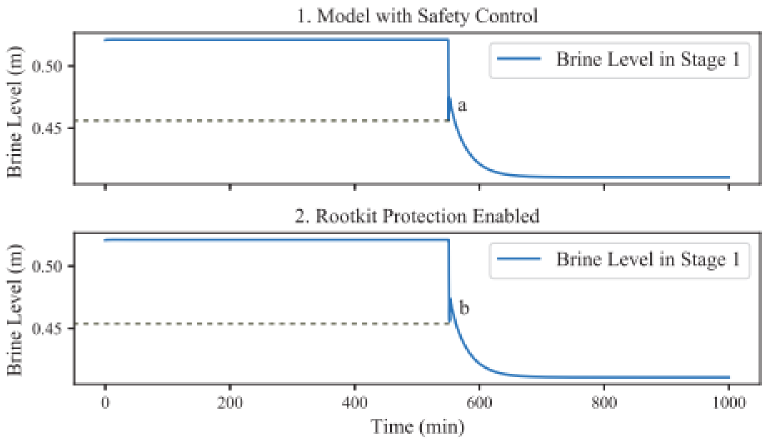


Fig. 6: Impact of ORRIS on a desalination plant

Evaluation of ORRIS (2/2)

Testing spatial bias and unseen malware

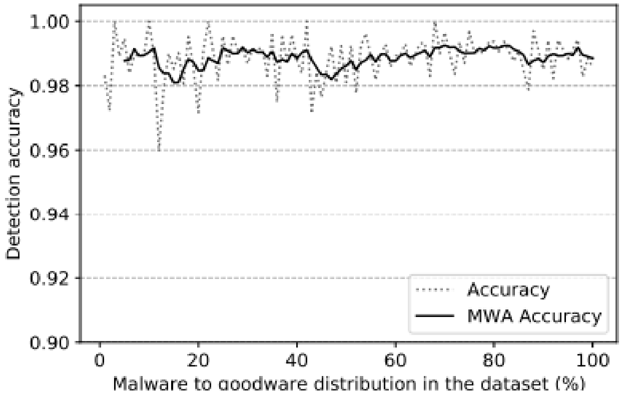


Fig. 7: Spatial bias experiment results

- Increased ratio of goodware to malware
- Moving window average accuracy stays between 98% and 100% (window size: 5)

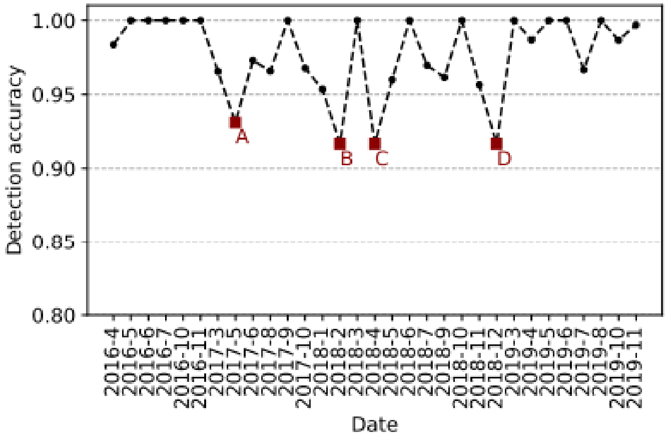


Fig. 8: Testing against unseen malware samples

Table 1: Reasons for accuracy decrease

Drift Point	Reason	Malware
A	Limited training on test malware variant	Mirai.N
B	New malware variants	Dofloo.D, Mirai.Au, Gafgyt.Az, Gafgyt.Ak, Mirai.Ax, Gafgyt.Aj, Dofloo.F and Tsunami.Bh
	New malware	Mirai.B and DnsAmp.C
C	New malware variant	Tsunami.Br
D	Limited training on test malware variants	Tsunami.Bh and Mirai.Au

Discussion and conclusion

Limitations

- JTAG is slow
- Sometimes not enabled by default
- Scalability

ORRIS

- Out-of-the device
- Non-intrusive
- Malware detector (user-level and kernel-level)

NYU TANDON SCHOOL OF ENGINEERING

MoMA LAB | nyuad.nyu.edu/momalab

Thank you

Prashant Hari Narayan Rajput

pr1365@nyu.edu

Github

github.com/momalab/orris

جامعة نيويورك أبوظبي

NYU ABU DHABI