Lab of Green and secure Integrated Circuit Systems (LOGICS)

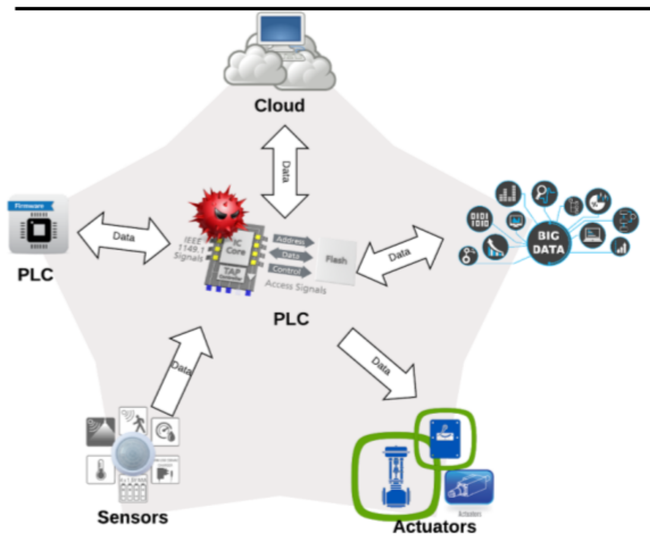
PennState College of Engineering

ArmorPLC

Diagnosing PLCs Against Cybersecurity Threats through Physical Process Monitoring and Record & Replay

Wenhui Zhang, Srivatsa Srinivasa, Nikhil Nandoskar, Asmit De, Swaroop Ghosh
School of Electrical Engineering and Computer Science, PennState

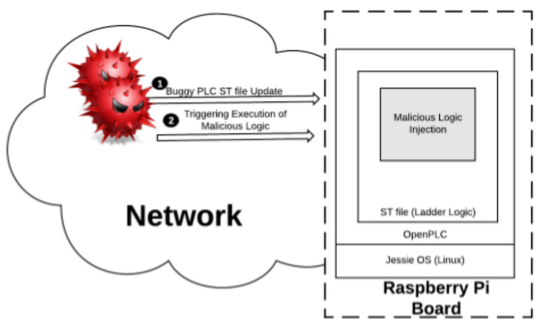
Introduction



Cyber-attacks on Industrial PLCs are reported to cause about 70 billion dollars in gross domestic product (GDP), and it also lead to lost of 42,220 U.S. manufacturing jobs over the past decade.
Smart cloud based PLC ecosystem exposes even larger threat interface to adversaries.

Vulnerabilities in PLC Ecosystem

1) Hacking PLC Configuration
2) Hacking OS
3) Modifying the User Space Programs
4) Monitoring Pin/Data/Configuration
5) Return Oriented Programming Attack

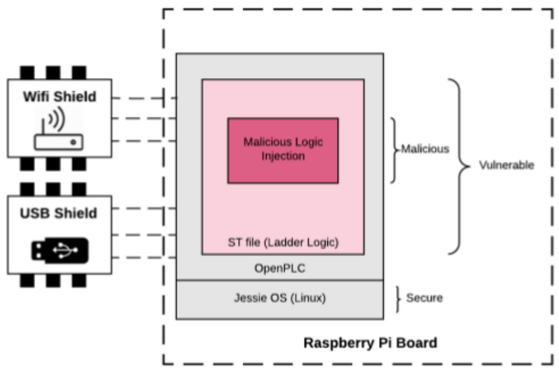


Hacking a PLC ecosystem is straightforward and painless

Threat Model

Stipulations on which our model is built:

- Network communication with cloud is **malicious**
- Raspberry Pi board is **secure**
- Jessie OS is **benign**
- OpenPLC software stack is **benign**
- Virtual PLC is **vulnerable**



Threat interface increases dramatically with exposing to network

Existing Protection Techniques

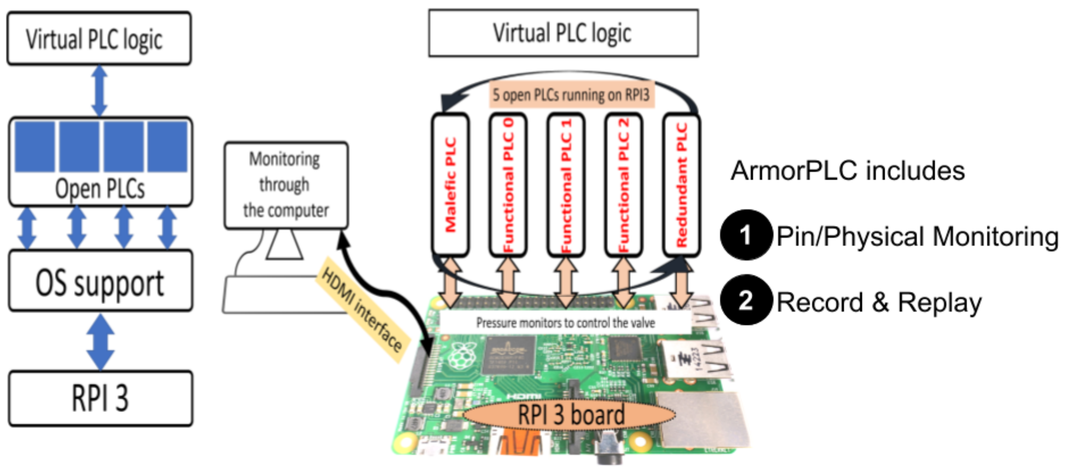
State-of-the-Art PLC protection techniques:

- Data Isolation using metadata and firmware encryption
- Process Isolation to prevent data sharing between PLC threads
- Sandboxing to filter instructions between application and OS
- Virtualization to provide separate and isolated OS environments

Novelty of proposed techniques:

- Comprehensive I/O monitoring to detect attacks in PLC logic
- Can detect attacks by malicious inputs
- Can handle secondary attacks such as compromised OS environment
- Can mitigate attacks by replaying the PLC logic on backup PLC

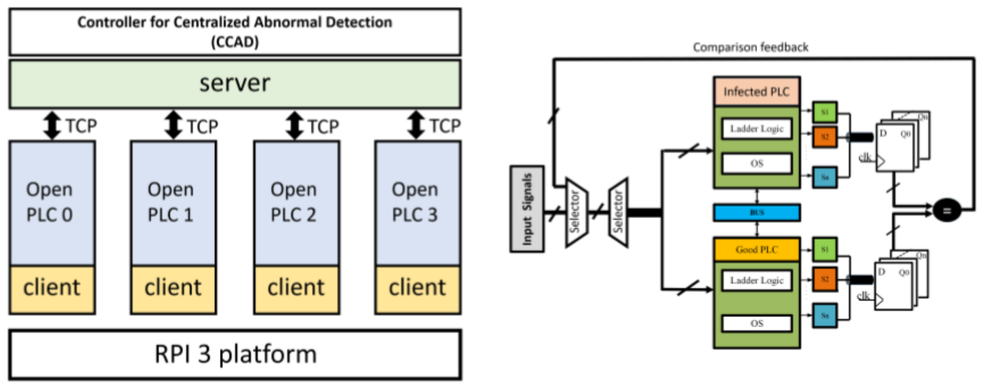
System architecture: ArmorPLC



ArmorPLC includes

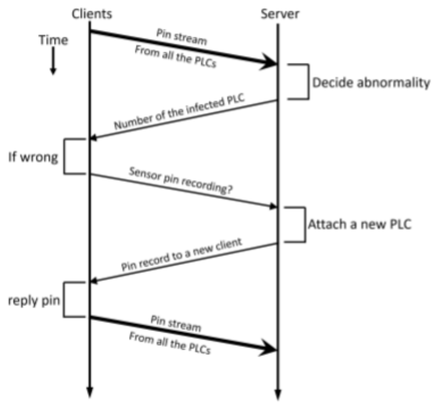
1. Pin/Physical Monitoring
2. Record & Replay

Detection: Physical Process Monitoring



Byzantine decision made for detection abnormalities

Mitigation: Record and Replay mechanism



- Capturing Stage:
  - Pin Status Recording
- Communication Stage:
  - Multi-Layer Management
- Control Stage:
  - Pin Status Replay

Recording and replay PWM pin signal at sensitivity of 50 us

Conclusion

	Attacks and Vulnerabilities			
Attacks and Vulnerabilities		Physical process monitoring. Output value configuration comparison	Computing timing comparison	Recording and reply
	Compromised pin I/O, invalid input	✓	✓	✓
	Compromised PLC logic, malicious injection	✗	✓	✓
	Compromised OS	✓	✓	✓
	Compromised configuration	✓	✓	✓
	Passive attack, monitoring pin I/O	✗	✓	✓

Bibliography:

1. Malkhi, D., & Reiter, M. (1998). Byzantine quorum systems. *Distributed computing*, *11*(4), 203-213.
2. Gomez, L., Neamtiu, I., Azim, T., & Millstein, T. (2013, May). Reran: Timing-and touch-sensitive record and replay for android. In *Software Engineering (ICSE), 2013 35th International Conference on* (pp. 72-81). IEEE.
3. Alves, T. R., Buratto, M., de Souza, F. M., & Rodrigues, T. V. (2014, October). OpenPLC: An open source alternative to automation. In *Global Humanitarian Technology Conference (GHTC), 2014 IEEE* (pp. 585-589). IEEE.

This project was sponsored in part by DARPA YFA (#D15AP00089) and NSF (CNS-1722557, CCF-1718474, DGE-1723687)