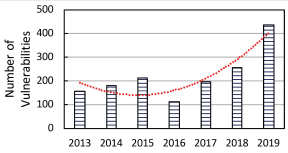
Automatic Exploits Detection and Mitigation for Industrial Control System Protocols

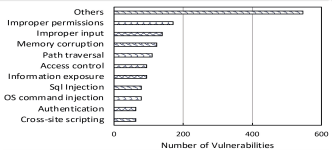
Award# CNS- 2051621

Type: Small; Start date: Sep 01, 2021

PI: Muhammad Taqi Raza (University of Arizona)

Practical Attacks



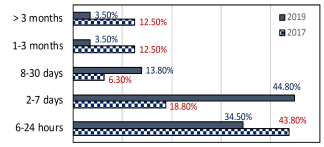


Severity Level	# of Vulner.	%	Root Cause Examples
Low	15	1	The controller does not properly validate the input.
Medium	328	21	Unauthenticated packets can cause DoS at service ports.
Critical	390	25	No authorization check when connecting to the device.
High	825	53	Cryptographic key is hard coded into the binary file.

Most of the vulnerabilities (around 60%) target authentication, authorization, and access control of ICS components.

Limitations of Existing Solutions

It takes from several hours to several days in detecting the compromise. In consequence, attackers can infiltrate into the industrial system.



- **Post-vulnerabilities guidelines:** Vulnerabilities are addressed based on learned lessons rather considering design principles.
- **Adhoc and isolated mitigation of attacks:** Rolling out patches.
- **Middlebox solutions partially help:** Spoofing attacks are possible; zero-day attacks are not detected.

Research Challenges

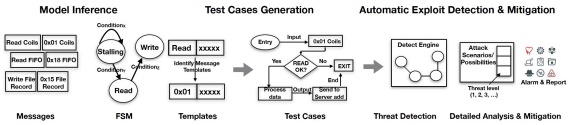
Goal: Performing vulnerability analysis to locate, determine the magnitude of, and prioritize any flaws in the design and implementation of the industrial control system (ICS) protocols.

Challenges: The security analysis requires a complete understanding of protocols' specification and their working. However, most of the ICS protocols are proprietary: their specifications do not exist, their communication patterns are obscure, and their operations are not certified for compliance.

Research Questions:

- Can we infer the working of all ICS protocols?
- How can we ensure complete coverage of vulnerable use cases?
- Can we perform run-time vulnerability analysis ?

Model Inference based Testing



Step 1 Model Inference: Reason about the message contents and the fine state machine of ICS system protocols by inferring: (a) the protocols' traffic; (b) common data structures; and (c) data flows.

Step 2 Test Case Generation: Generate functional test cases that validate the working of ICS protocols.

Step 3 Automatic exploit detection and mitigation: Developing a real-time exploit detection and mitigation system to discover security vulnerabilities in ICS protocols through testing.

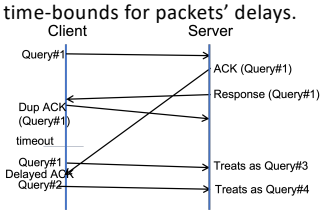
Empirical Evaluation

Threat Model: Adversary is acting as man-in-the-middle who simply delays the packets exchanged between client and the server.

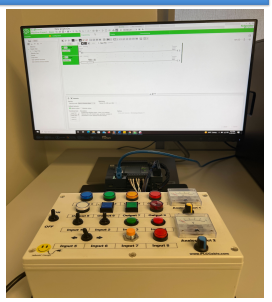
Attack Impact:

- Temporal invariants alter the functional logic of ICS sensors controlling critical components (e.g., conveyor belt and robots).
- Arbitrary components' actions result into faulty assembly line.
- Attacker can control the order of components' movements.

Solution: (1) determine the round-trip time for each class of packets; (2) determine the path invariants of such packet; (3) learn (and calculate) the time-bounds for packets' delays.



Our solution identifies that the server will treat the Modbus packet incorrectly (figure above) and hence drop the Query#1 retransmission packet



Outreach Impact

By using the platforms of Women in Science and Engineering (WISE) and Early Academic Outreach (EAO) at Uarizona, PI is fostering the research interests on ICS in the outreach community.

Also, PI has used Research Opportunities Consortium's (UROC)-PREP platform at the University of Arizona to announce the research positions in the Industrial Control Systems Security lab; and an UG student is enrolled in the research.

Educational Impact

PI has introduced a new direction of cloudifying ICS processes in his Cloud Computing Fundamental class that he teaches in the Fall semesters.

PI has also introduced hands-on labs on ICS in the Penetration Testing and Ethical Hacking class that he teaches.

PI has increased undergraduate students' educational participation by allowing senior year undergraduate students to enroll in the graduate class.

Research Impact

The proposed techniques can be applied to model proprietary protocols in other industries such as automotive and avionics industries.

The proposed approach can be applied to generate comprehensive test cases for cellular (e.g., 4G and 5G protocols) and the Internet of Things (e.g., LoRA, Zigbee) standards.

This research is beneficial to securing operational networks and industries.