Automatic Exploits Detection and Mitigation for Industrial Control System Protocols

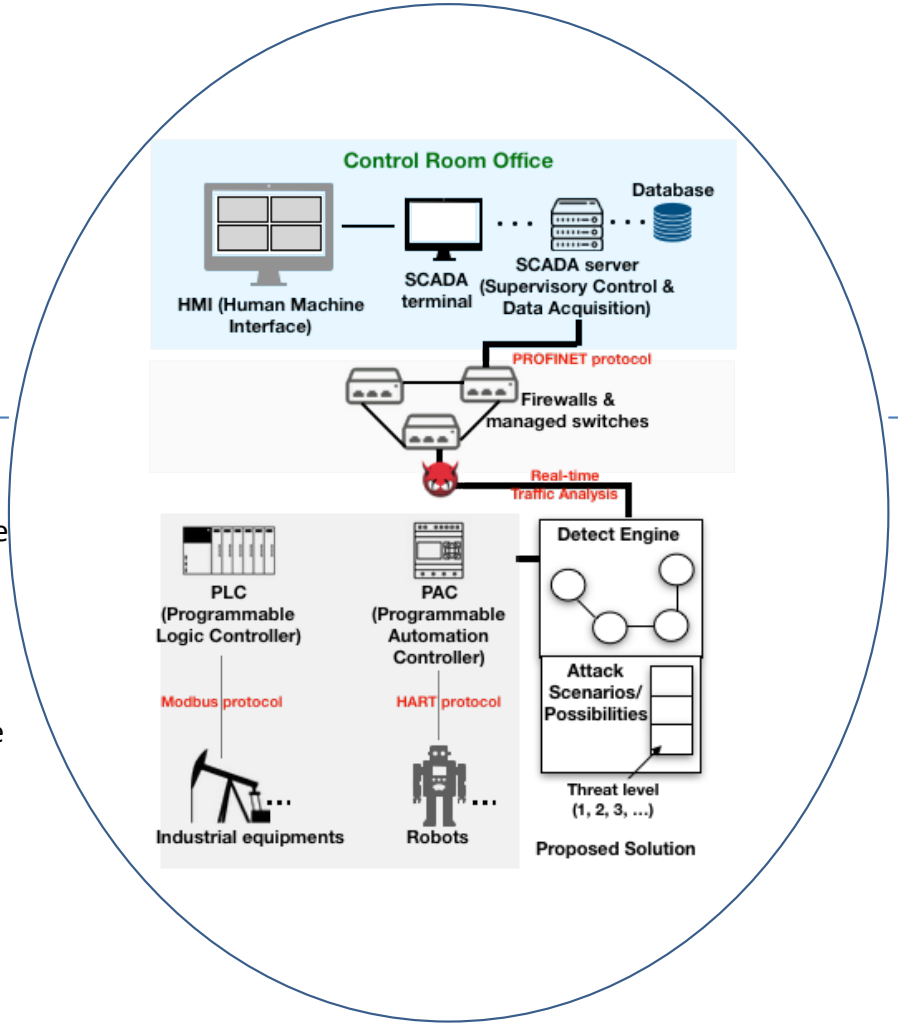
THE UNIVERSITY OF ARIZONA

Challenge:

- Proprietary and non-proprietary protocols' interactions is hard.
- Realtime and complete vulnerability analysis is desired in polynomial time.
- Threat mitigation should be automatically done.

Solution:

- Model Inference: Reason about the message contents and the fine state machine of ICS system.
- Test Case Generation: Generate functional test cases that validate the working of ICS protocols.
- Automatic exploit detection and mitigation: Developing a real-time exploit detection and mitigation system to discover security vulnerabilities.



Scientific Impact:

- Secure the critical industrial infrastructure against zero-day attacks.
- The proposed techniques can be applied to model proprietary protocols in other industries such as automotive and avionics industries.

Broader Impact and Broader Participation:

- PI is fostering research interests in women through Women in Science and Engineering (WISE) program.
- PI has also introduced hands-on labs on ICS in the Penetration Testing and Ethical Hacking.
- PI has increased undergraduate students' educational participation by allowing senior year UG students to enroll in the grad class.

PI: Muhammad Taqi Raza;
University of Arizona;

Award# CNS- 2051621;
Type: Small; Start date: Sep 01, 2021