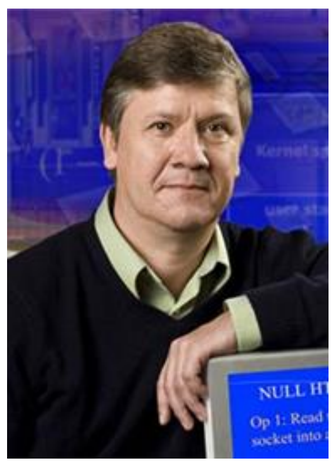
Data-Driven Study of Attacks on Cyber-Physical Infrastructure Supporting Large Computing Systems



Zbigniew Kalbarczyk, Ravishankar Iyer

University of Illinois at Urbana-Champaign

https://depend.csl.illinois.edu

Problem

We consider advances in cyber-attacks in the context of ***indirectness*** and ***automation.***

- ***Indirectness:*** *an attack that targets an auxiliary CPS that the target computing infrastructure relies on.*
- ***Automation****:* an attack through a self-learning malware to: (i) derive actionable intelligence from data and (ii) launch an attack in the most opportune time

Challenges

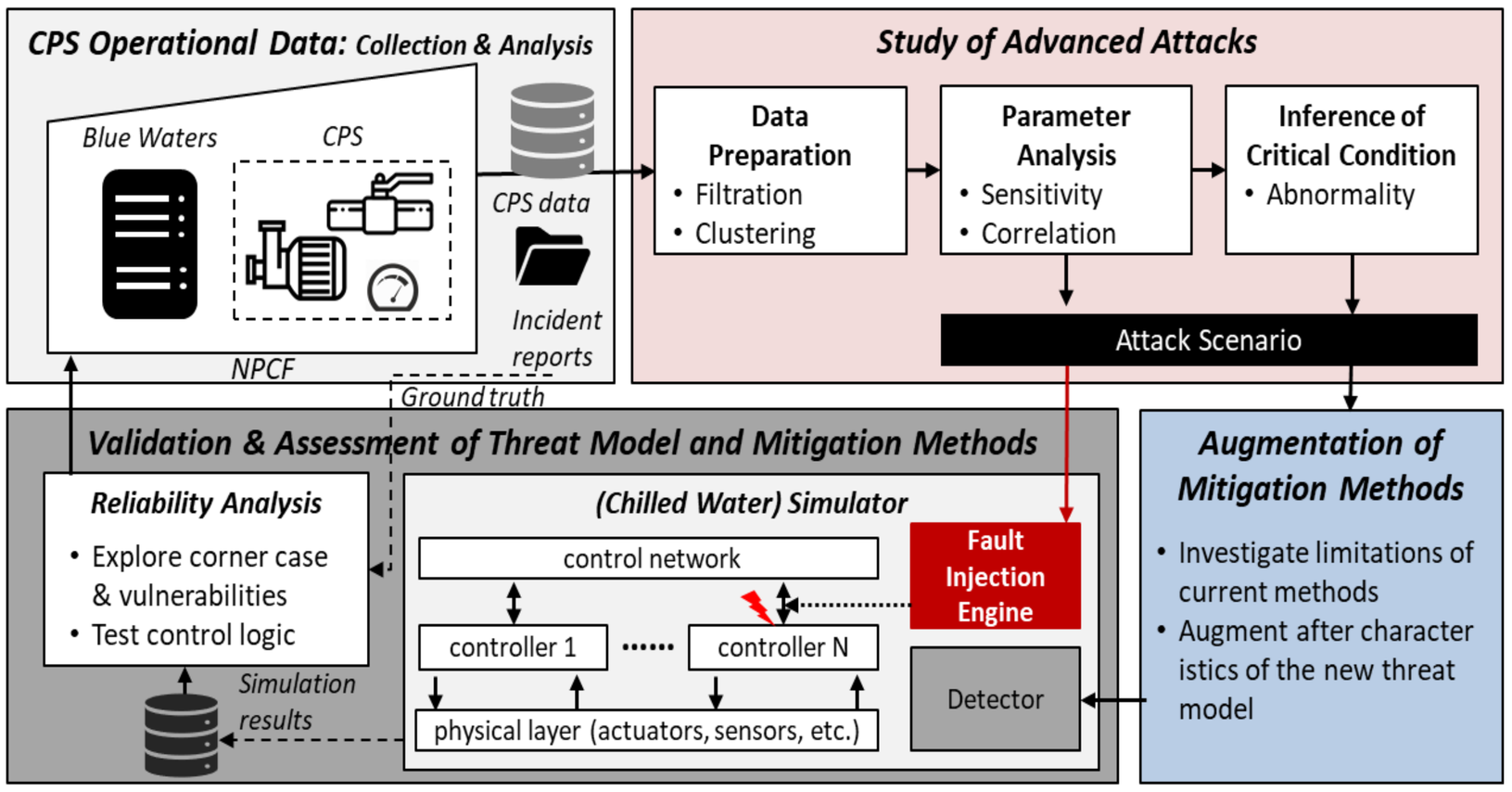
- Detect attacks deployed with self-learning malware
- Detect and distinguish attacks from random failures
- Devise and validate the protection mechanisms by using real operational data

Scientific Impact

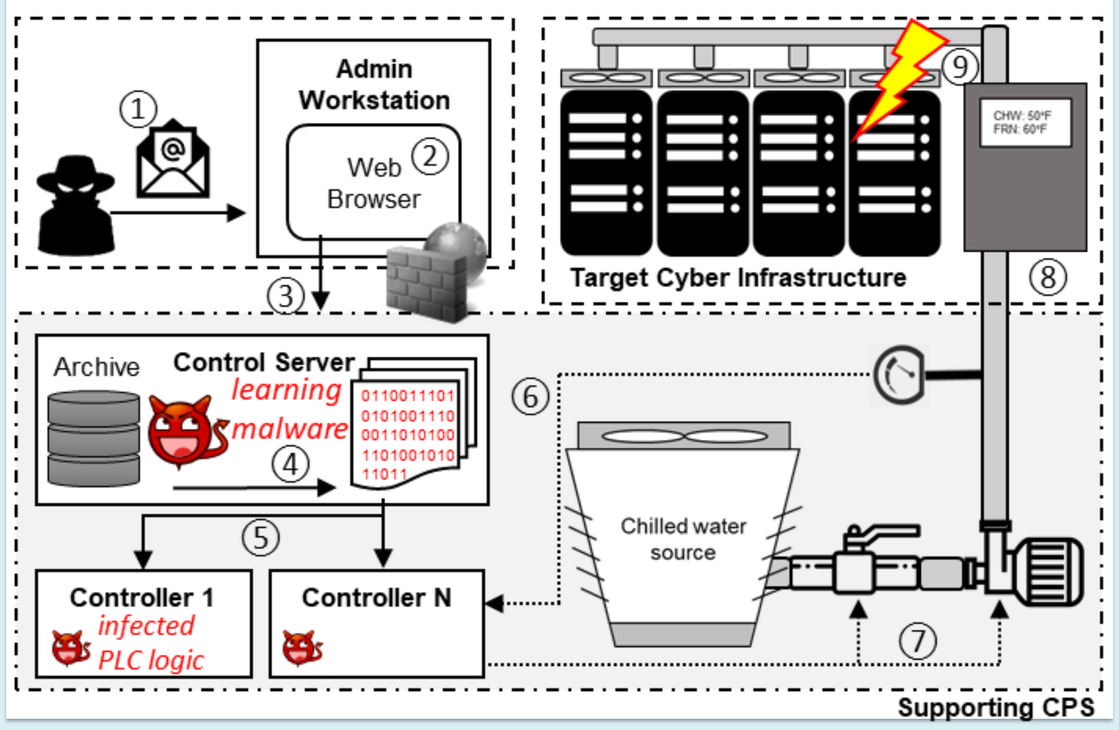
- ***Scientifically sound methods*** to jointly study reliability failures and malicious attacks against a CPS critical for the uninterruptible operation of a large computing infrastructure
- ***Demonstration of new advanced attacks*** which take advantage of machine learning to develop and execute an attack strategy
- ***Define general principles for detecting attacks***, which combines the knowledge of both CPS and the tenant computing infrastructure
- ***A data-driven simulation testbed*** that emulates the CPS behavior and enables experimentation with different attack scenarios

Approach Overview

- ***Stage 1:*** *Collection and analysis of operational data of the CPS and the cyber infrastructure.*
- ***Stage 2:*** *Study innovative ways to make the attack more sophisticated.*
- ***Stage 3****: Devise mitigation and detection methods.*
- ***Stage 4****: Validation and assessment.*

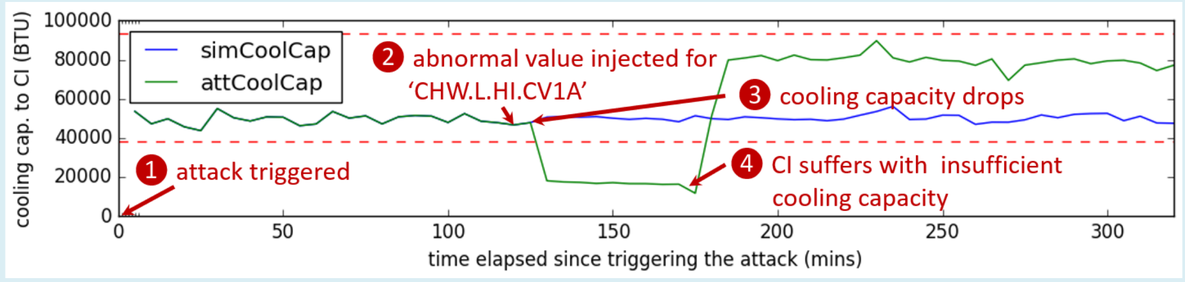


Self-learning malware attack scenario



①-③: Initial compromise - access CPS control system/network
④: Install and run learning malware (on CPS control server) to infer failure causing anomalies from CPS operational data. Anomalies are used as attack strategies.
⑤,⑥: Update malicious control logic containing the attack strategy and its triggering logic to the controller and wait for triggering condition
⑦-⑨: Abnormal event injected to the CPS and its impact cascades to the target cyber infrastructure

Sample Attack Strategy Simulation



- Supply water temperature abnormality due to power interruption
- Shortage in cooling capacity for ~1hr

Broader Impact

- Identify potential advances in security threats by demonstrating the feasibility of masquerading a security attack as a reliability failure
- Improve the security of CPSes and provide an effective methodology for in-depth monitoring for improved resiliency
- Application of the proposed approach to CPSes in other domains (e.g., robots, AVs) to eliminate potential security risks

References

[1] Key-whan Chung, Zbigniew T. Kalbarczyk, Ravishankar K. Iyer: **Availability attacks on computing systems through alteration of environmental control: smart malware approach.** ICCPS 2019

[2] Key-whan Chung, Zbigniew T. Kalbarczyk, Ravishankar K. Iyer: **Indirect cyber attacks by perturbation of environment control: a data driven attack model: poster.** HotSoS 2018

ILLINOIS
Award ID#: 18-16673