Poster: Indirect Cyber Attacks by Perturbation of Environment Control: A Data Driven Attack Model*†‡

Keywhan Chung, Zbigniew T. Kalbarczyk, Ravishankar K. Iyer
University of Illinois at Urbana-Champaign

1 INTRODUCTION AND BACKGROUND

When the security of computing infrastructure has been considered, the focus has traditionally been on the infrastructure itself with less thought given to the surrounding systems that affect the operation of the infrastructure. Instead, our indirect attack model targets a super computer by obfuscating the control of a cyber-physical system (CPS) responsible for maintaining the operational environment.

Our study is conducted in the context of the building automation system (BAS) responsible for controlling the operational environment of the Blue Waters supercomputer at the University of Illinois. This super computer is housed in the National Petascale Computing Facility (NPCF). Cooling the supercomputer and managing the physical environment (room temperature, humidity and pressure) are critical for the reliable operation of Blue Waters. The NPCF has adopted a BAS that regulates, and delivers chilled water to the server room and keeps the server room in a predefined condition. A set of sensors (e.g., temperature) placed across the building report measurements to the control network, where a set of controllers manages the actuators to optimize the environment accordingly.

2 THREAT MODEL AND APPROACH

Our threat model takes advantage of the relatively weak security of the CPS to intrude into a well-hardened computing infrastructure. In [1], we present a scenario in which a malicious entity exploits a vulnerability in the CPS to purposely recreate failure scenarios and thereby disguise an attack as an accidental event. In this paper, we present a case in which the attack strategy is automatically inferred from failure data and requires minimal prior knowledge of, or expertise in the CPS. Specifically, we deploy a set of statistical and learning techniques to infer critical parameters and their abnormal values without prior knowledge of the detailsof the CPS that manages the operational environment. The inferred values can be injected at an opportune time, perturbing the CPS and hence, changing the operational condition for the computing-infrastructure, potentially leading to a system outage. Note that the CPS-related problems discussed in our case study have been addressed by the operation team.

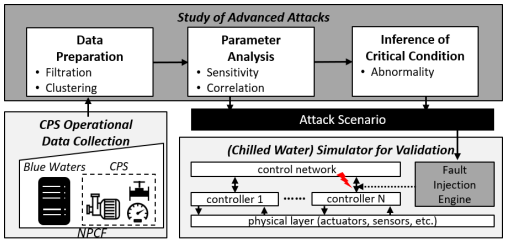

Figure 1: Approach overview

Our approach consists of four steps: data preparation, parameter analysis, inference of critical condition, and validation (Figure 1).

Data preparation. With the breach restricted to the CPS, we assume that no information on the status of the computing infrastructure is directly available to the attacker. We utilize observations of the temperature of the returning chilled water to infer the status (i.e., normal, failure or shut down) of the computing infrastructure.

Parameter analysis. Based on the inferred status, further information on the CPS can be derived from the data. With a malicious intention to corrupt the cooling capacity, we identify the parameters that are related to cooling of the computing infrastructure. The identification simplifies the computational complexity and increases the accuracy of the analysis.

Inference of critical condition. Using the reduced data set, we identify anomalies in the failure-related dataset. We consider such outliers to be the likely cause (or trigger) of the failure and attempt to attack the CPS by emulating the failure scenario.

Validation. As it would be undesirable to launch an attack on the real CPS, we built a simulator that emulates the chilled water control loop. The simulator allows us to inject abnormal CPS parameter values into the simulated CPS and verify the feasibility of attacks.

3 PRELIMINARY RESULTS

The initial results indicate that our approach would have effectively identified two CPS-related incidents. The first identified incident, in which the campus experienced a chilled water leakage at the construction site of a new building, could have caused an outage of the computing infrastructure, if had been in service. The other incident related to a maintenance operation on the campus chilled water loop, which perturbed the pressure of the chilled water and eventually shut down a set of cabinets of the compute infrastructure.

*CCS CONCEPTS
•Security and privacy; •Computer systems organization→ *Embedded and cyber-physical systems*;
†KEYWORDS
CPS-security, compromise supercomputer through cooling control system, data-driven attack
‡ACKNOWLEDGEMENT
This material is based upon work supported by the National Science Foundation under Grant No. 15-45069 and 13-14891. Any opinoins, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

HoTSoS '18, April 10–11, 2018, Raleigh, NC, USAv

ACM ISBN 978-1-4503-6455-3/18/04.
https://doi.org/10.1145/3190619.3191681

REFERENCES

[1] Keywhan Chung, Valerio Formicola, Zbigniew T Kalbarczyk, Ravishankar K Iyer, Alexander Withers, and Adam J Slagell. 2016. Attacking supercomputers through targeted alteration of environmental control: A data driven case study. In *Communications and Network Security (CNS), 2016 IEEE Conference on*. IEEE, 406–410.