Current Topics in Privacy Seminar

Clement Fung
CMU Cylab

Title
Improving the Effectiveness of ML-based Approaches for Industrial Control Systems Security

Abstract
Industrial control systems (ICS) govern critical infrastructure and processes, such as power generation, chemical processing, and water treatment. To defend and protect ICS from potential harm, researchers commonly propose techniques based on machine learning (ML) for detecting anomalies in ICS process values. Despite strong results in research, ML-based approaches are rarely adopted in practice for ICS today. In this talk, I cover work that makes ML-based anomaly detection more effective for securing ICS, by both investigating the needs of current practice and by developing new ML-based approaches to meet these newly identified needs. First, to better understand how ML-based anomaly detection would be used in practice for ICS, we interview practitioners that work in ICS security and operations to understand their needs and requirements for adopting ML into ICS environments. Second, it is unclear if and how anomaly-detection outputs can be used to diagnose ICS anomalies; we evaluate a variety of explainable AI (XAI) approaches for attributing ICS anomalies to the underlying components that were manipulated. Finally, as an alternative to deep-learning models, we design CyPRESS, a new model architecture for ICS anomaly detection, and show that it is more efficient, interpretable, and robust.

Bio
Clement Fung is a postdoctoral research associate at Carnegie Mellon University and a member of the CyLab security and privacy institute. His research focuses on designing and evaluating ML-based approaches for securing industrial control systems in practice. He received his M.S. and B.A.Sc. from the University of British Columbia and the University of Waterloo respectively.