Translational AI Center (TrAC) Seminar – Spring 2022

Shana Moothedath

February 18 at 12:00 noon (US Central Time)

https://iastate.zoom.us/j/92178103551?pwd=dlNCa2l0ckVBTEVyR1JEN2Y3b21XQT09

A Game and Control Framework for Modeling and Mitigating Advanced Persistent Threats on Cyber-Physical Systems

Abstract

Advanced Persistent Threats (APTs) are sophisticated attacks mounted by intelligent and resourceful adversaries who gain access to a targeted system and gather critical information over an extended period of time. APTs consist of multiple stages, including initial system compromise, privilege escalation, and data exfiltration, each of which involves strategic interaction between the APT and the targeted system. While this strategic interaction can be viewed as a game, the stealthiness, adaptiveness, and unpredictability of APTs imply that the information structure of the game and the strategies of the APT are not readily available. In this talk, we will present a game-theoretic approach to characterize the trade-off between effectiveness for detecting APTs and resource efficiency. Our approach to modeling APTs is based on the insight that the persistent nature of APTs introduces information flows in the system that can be monitored. One monitoring mechanism is Dynamic Information Flow Tracking (DIFT), which taints and tracks suspicious information flows through a system and performs security analysis on the tainted flows at designated locations. Since performing security analysis on all the flows will incur significant memory and performance overhead, efficient defense policies are needed to maximize the probability of detecting the APT while minimizing resource costs. In this work, we develop a multi-stage game framework for modeling the interaction between an APT and a DIFT, as well as designing an efficient DIFT-based defense. Our model is grounded on APT data gathered using the Refinable Attack Investigation (RAIN) flow-tracking framework. We will present the current state of our formulation, insights that it provides on designing effective defenses against APTs, and directions for future work.

Short Bio

Shana Moothedath is an Assistant Professor in the Department of Electrical and Computer Engineering at Iowa State University. Prior to join ISU, she was a Postdoctoral Research Scholar at the University of Washington, Seattle. She received her B.Tech. and M.Tech. degrees in Electrical and Electronics Engineering from the Kerala University, India, in 2011 and 2014 respectively, and Ph.D. degree in Electrical Engineering from Indian Institute of Technology Bombay (IITB), India, in 2018. She was awarded the Excellence in Ph.D. Thesis Award 2017-2019 at IIT Bombay and selected as a EECS Rising Star in 2019. Her research interests include network security analysis, structural analysis of large-scale control systems, and applications of systems theory to complex networks.