Strategic Placement of Security Monitors in Industrial Control Systems

Kartik Palani, David M Nicol

Information Trust Institute, University of Illinois at Urbana Champaign

Goal

Detect the presence of a stealthy attacker in a control system network

Fundamental Questions/Challenges

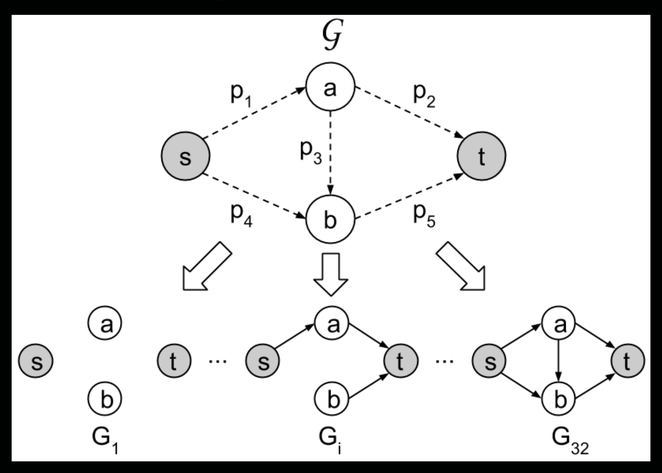
- What is the minimum number of monitors required to detect a set of attacker actions
- Given a reduced number of monitors, due to limited security budgets, how do you place them optimally
- Address uncertainty in:
  - Knowledge of attacker actions
  - Knowledge of network environment
  - Detectability of an attacker action
- Is it necessary to collect *everything* to guarantee *something*
- How does it adapt to attackers' knowledge of your placement

Research Plan

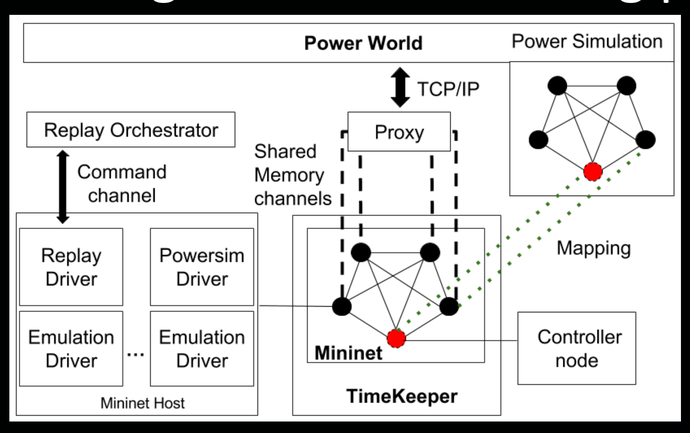
- Developing the right modeling formalism

	Limited	Unlimited
Perfect	Attack Graphs	Ideal
Imperfect	???	Redundancy

- Representing uncertainty



- Generating data for evaluating placements



Publications & Tool

Melody: Synthesized Datasets for Evaluating Intrusion Detection Systems for the Smart Grid, WSC 2017

An Approach to Incorporating Uncertainty in Network Security Analysis, HotSoS 2017

Melody: https://github.com/Vignesh2208/NetPower_TestBed.git

Contact

palani2@illinois.edu

@mosestadka

SPECIAL CYBER OPERATIONS RESEARCH AND ENGINEERING

Computational Cybersecurity in Compromised Environments
2017 Fall Workshop | October 23-25, 2017 | Atlanta, Georgia