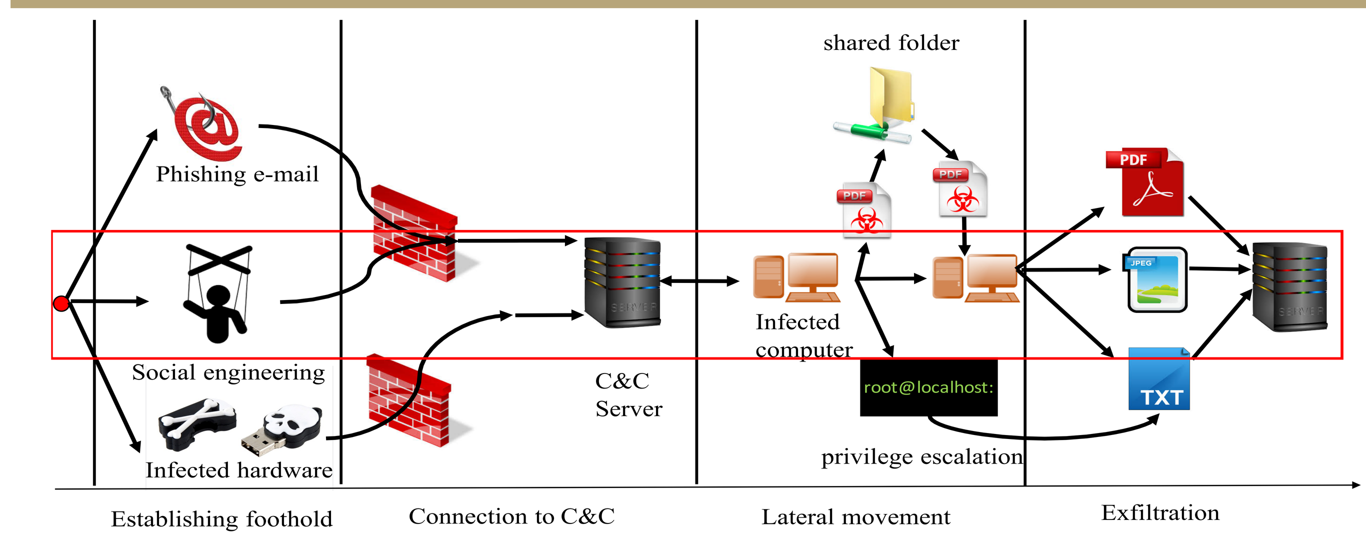
A GAME THEORETIC APPROACH FOR RESOURCE EFFICIENT DYNAMIC INFORMATION FLOW TRACKING AGAINST ADVANCED PERSISTENT THREATS

DINUKA SAHABANDU, GRADUATE STUDENT, NETWORK SECURITY LAB, UW

Introduction



- Attacks consist of multiple stages between entry and exit points
- Target multiple entry points simultaneously at each stage
- Interact with system to achieve goals while remaining undetected

Problem Formulation

Adversarial cyber interactions: At each stage adversary and system play a strategic game in which the goal of the
- **Adversary** is to **evade detection** and achieve targets in each stage
- **Defender** is to **detect adversary** before it achieves the goal

Information structure:
Complete: both players know the system, payoff of other player
Imperfect: defender is unaware of the stage of attack, which flow is malicious and adversary does not know actions of defender

Objective: Develop a game theoretic framework to model adversarial cyber interactions such that:
- Detection probability is maximized
- Cost of detection is minimized

Defense Scheme: Dynamic Information Flow Tracking (DIFT)

Tag sources tag **vulnerable** I/O channels → **Tag propagation rules** specify **data-** and control-flow-based tag propagation policy → **Tag sinks/Traps** verify **authenticity** of tagged flows

Payoffs consists of tagging costs, rewards and penalties to players

$$U_D(\mathbf{p}_D, \mathbf{p}_A) = \sum_{s\in\mathcal{S}} \mathbf{p}_D(s) C_D(s) + \sum_{j=1}^{M} p_T(j)\alpha_D + p_R(j)\beta_D^j$$

$$U_A(\mathbf{p}_D, \mathbf{p}_A) = \sum_{j=1}^{M} p_R(j)\beta_A^j + p_T(j)\alpha_A$$

Nonzero-sum imperfect information game

Proposed Approach

Key Steps of our Approach

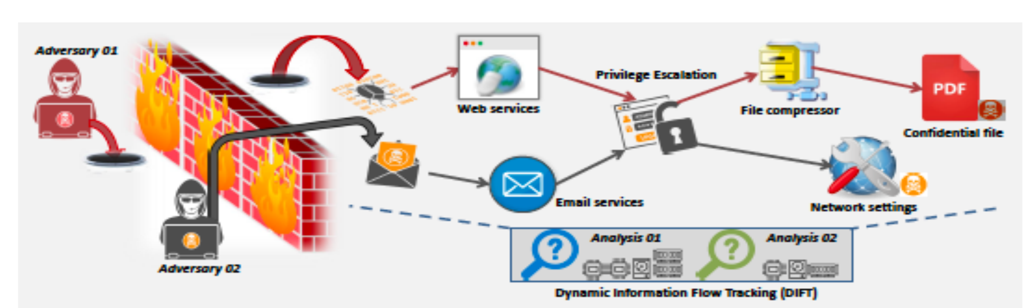
Record system logs using RAIN → Abstract information flow graph → Multi-stage dynamic game → Defender policy

Multi-stage dynamic game: At each stage adversary and system play a strategic game in which the goal of the
- **Adversary** selects an **attack path** in the information flow graph
- **Defender** (DIFT) **tags** a subset of nodes
- Each stage of attack is defined by a set of **destinations** which must be achieved **sequentially**

Solution to the game gives actionable cyber defense against multi-stage adversarial attacks

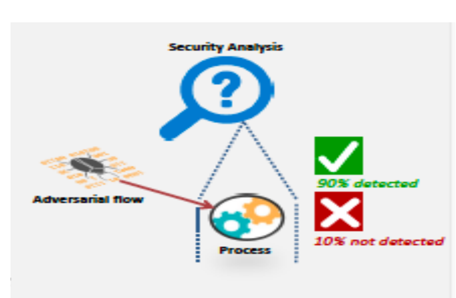
Other Related Problems Analyzed

Simultaneous Detection of Multiple Adversaries



- Multiple adversaries with different attack capabilities
- Security analysis of different granularities with limited resources

Stochastic DIFT Games



- Captures false negatives of DIFT
- Tackles unknown state transitions

Key Results

Result 1. For a given adversary strategy $\mathbf{p}_A$,
- The **defender's utility** function $U_D(\mathbf{p}_D, \mathbf{p}_A)$ is **submodular** in $\mathbf{p}_D$.
- There exists an algorithm that computes at least a **1/2-optimal best response solution to the defender** in poly-time.

Result 2. For a given defender's strategy $\mathbf{p}_D$, the best response of the **adversary** is obtained from a **shortest path algorithm** on the information flow graph with edge weight $-\log(1-\mathbf{p}_D(s_i))$ to every incoming edge to s_i.

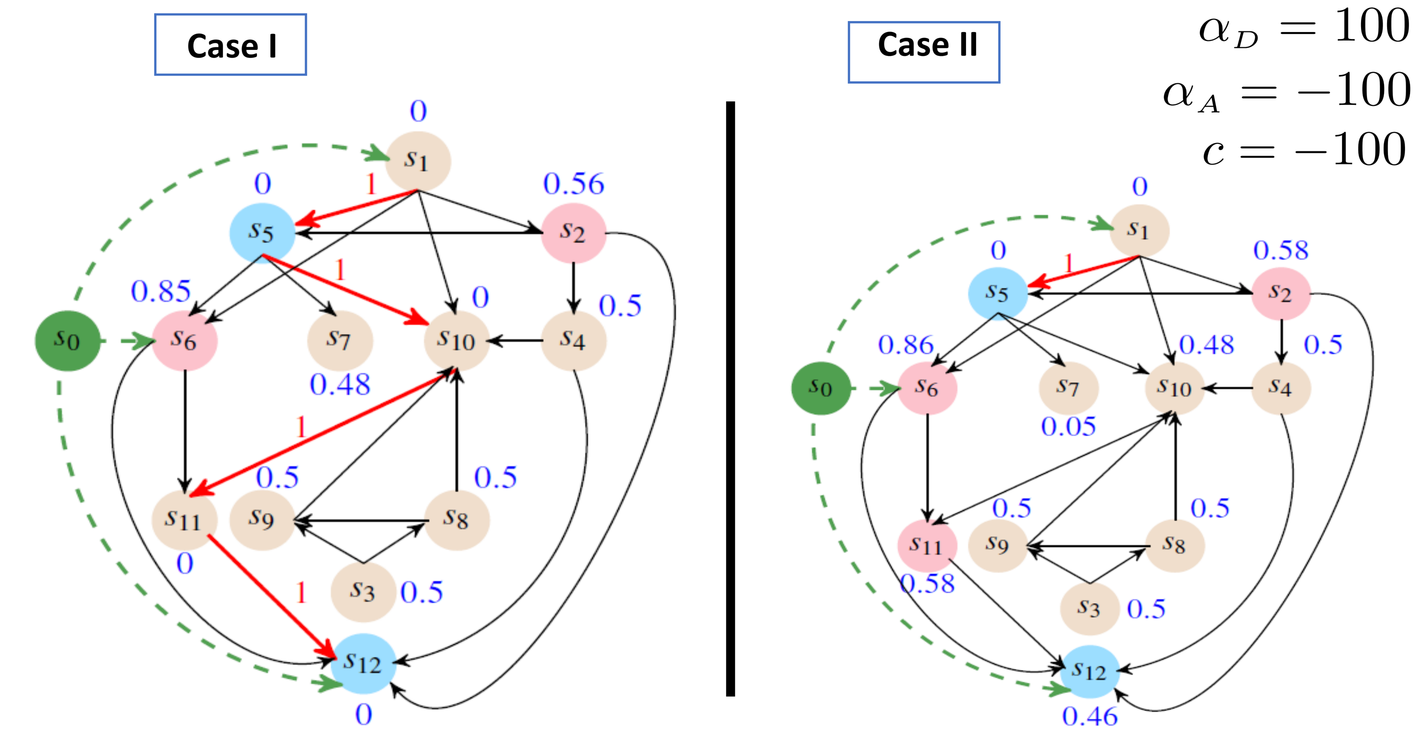
Result 3. For any $\epsilon > 0$, with probability $1-\delta$, an ϵ-**correlated equilibrium** can be obtained in $O\left(\frac{(N^2(M+1)+N)}{\epsilon^2}\ln\left(\frac{N^2(M+1)+N}{\delta}\right)\right)$ number of utility computations.

Result 4. A **Nash equilibria** of the adversary vs. DIFT game for an attack that consists of **single stage** is given by the solution to a **minimum-cut problem** and then mapping the solution to an equivalent **bi-matrix game**.

Experimental Results

- ScreenGrab attack data recorded from RAIN
- Results for two different trap settings

$$\beta_D^1 = \beta_D^2 = -300$$
$$\beta_A^1 = \beta_A^2 = 300$$
$$\alpha_D = 100$$
$$\alpha_A = -100$$
$$c = -100$$



- Choice of traps locations are critical for security
- Optimal selection of traps leads to effective detection

Conclusions

- We proposed a multi-stage dynamic game model to evaluate the performance cost and effectiveness of information flow-based detection
- We ground the approach on data collected using RAIN framework
- We computed the best response of the players; a shortest path algorithm for the adversary and a submodularity-based approach for the defender
- We gave a polynomial-time algorithm to compute the correlated equilibrium
- We tested our approach on ScreenGrab attack data obtained from RAIN

References and Sponsors

- D. Sahabandu, B. Xiao, A. Clark, S. Lee, W. Lee, and R. Poovendran. "DIFT Games: Dynamic Information Flow Tracking Games for Advanced Persistent Threats." to appear in Conference on Decision and Control (CDC), 2018.
- D. Shabandu, S. Moothedath, J. Allen, A. Clark, L. Bushnell, W. Lee, and R. Poovendran, "Dynamic Information Flow Tracking Games for Simultaneous Detection of Multiple Attackers." In IEEE Conference on Decision and Control (CDC), December 2019.
- S. Moothedath, D. Sahabandu, J. Allen, A. Clark, L. Bushnell, W. Lee, and R. Poovendran, "A Game-Theoretic Approach for Dynamic Information Flow Tracking to Detect Multi-Stage Advanced Persistent Threats," to appear in IEEE Transactions on Automatic Control, December 2020.

Project Sponsors

ELECTRICAL & COMPUTER ENGINEERING
UNIVERSITY of WASHINGTON

ADVISORS: RADHA POOVENDRAN, LINDA BUSHNELL
COLLABORATORS: SHANA MOOTHEDATH (UW), JOEY ALLEN (GA), ANDREW CLARK (WPI), WENKE LEE (GA)
SPONSORS: OFFICE OF NAVAL RESEARCH (ONR), DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA)