Understanding Adaptive Adversarial Behavior and Decision-Making Processes in Cyberattacks

PIs: Aunshul Rege, Department of Criminal Justice, Temple University
https://sites.temple.edu/care/

Research Goal

The objective of this project is to analyze malicious dynamic behavior and decision-making to predict adversarial movement and shift the reactive management of cyberattacks towards proactive cybersecurity.

Advanced Persistent Threats (APTs)

- Nation-state actors, organized crime group members, cybercriminals and hacktivists threaten the intellectual property, financial assets, reputation, and security of organizations and nation-states.

Research Objectives

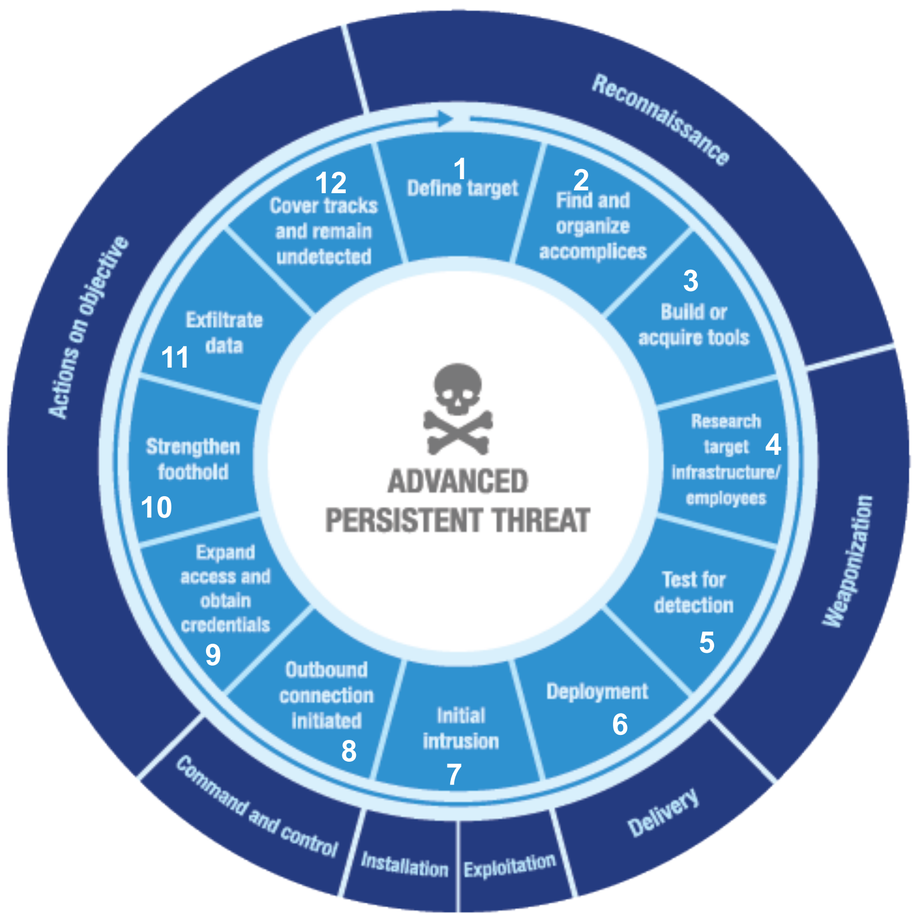
1. Investigate adversary-defender interaction and identify adversarial trajectories

2. Understand adversarial adaptability when attack paths are disrupted at different stages

3. Examine the importance and characteristics of the attack paths and stages

4. Improve the transparency, consistency and validation of adversarial attack models.

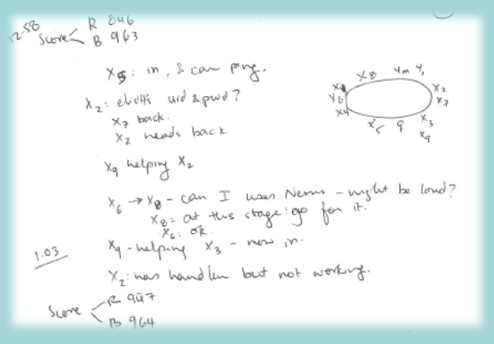
Adversarial Intrusion Chain



Approach

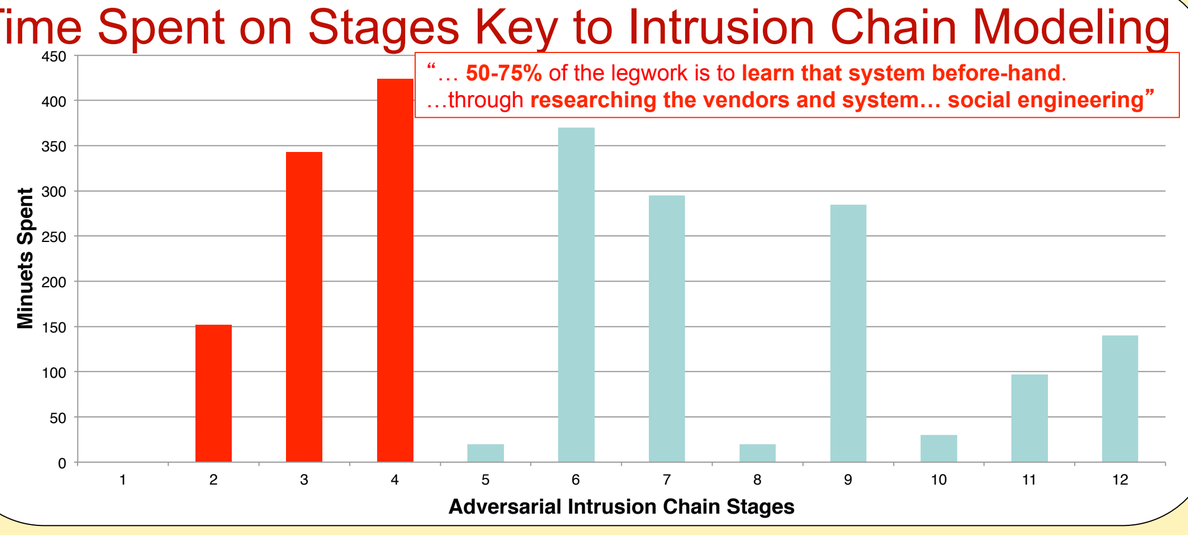
Qualitative Methodology

- Real-time red/blue cybersecurity training exercises
- 1-2 days; 8 hours
- 3 case studies
- Professional penetration testers
- Observations and interviews



NCFTA · MICHIGAN merit CYBER RANGE Powered by merit · INL Idaho National Laboratory · U.S. Department of Homeland Security · ICS-CERT INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Time Spent on Stages Key to Intrusion Chain Modeling



Adversarial Capacity to Adapt Varies

1. Limited Knowledge

"**Learning the IT tools while expecting to implement them quickly is frustrating**. I will be of great use if we get into the ICS [industrial control systems] network".

2. Self-Disruptions

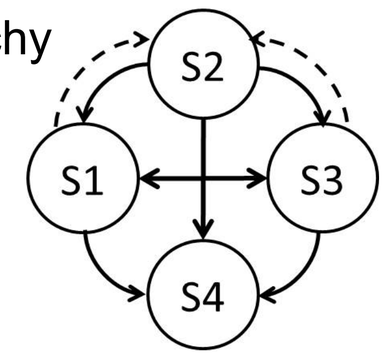
Closed previously acquired connections by error. Adaptations required starting from scratch to establish outbound connections again.

3. Defense Disruptions

Subject	Disruption	Adversarial Adaptation
2	Shut down shell	Backtracks, changes administrative password to bolster access
7	"Someone knocked me out"	Assesses impact level ("Good thing I deleted things when I did"); Regain access, changes blue team's IP address to secure his foothold.
4	Mislead by decoy	Googled for connection but no other adaptation

Adversarial Group Structure, Interdependencies and Roles Shape Decision-making and Adaptability

- Lateral with minimal hierarchy
- Unilateral and multilateral interdependencies
- Transient sub-groups
- Roles based on skill-set



Subject	Background and Skills
1	Linux, Sniffing
2	Metasploit
3	PLC Programmer, Minimal Linux, Strategy Planning
4	Project SCADA, Metasploit

Subject 1: "Send phishing?"
Subject 3: "Should I do this?"
Subject 2: "Yes, yes do what you must!"

Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
Jan. 9 - 11th 2017
Arlington, VA

National Science Foundation WHERE DISCOVERIES BEGIN

TEMPLE UNIVERSITY