CAREER: Understanding Adaptive Adversarial Behavior and Decision-Making Processes in Cyberattacks

Aunshul Rege, Associate Professor, Temple University

Sites.temple.edu/care

Research Goal

The objective of this project is to analyze dynamic behavior, decision-making, and adaptation of cyberadversaries during cyberattacks to predict their movement and shift the reactive management of cyberattacks towards proactive cybersecurity

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.

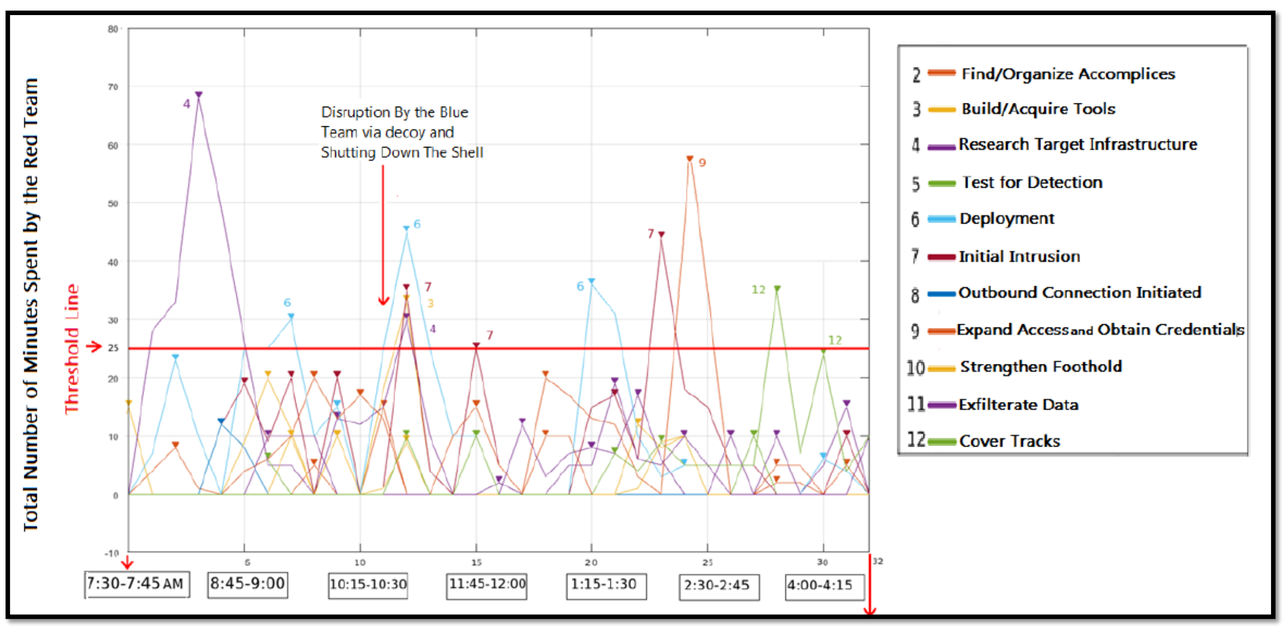
Methodology

Qualitative

- Real-time red/blue cybersecurity training exercises
- 1-2 days; 6-10 hours
- 5 case studies
- Professional penetration testers
- Observations and interviews

Mixed-methods ('thick' data as 'big' data)

- Time series
- Graph/network theory
- Machine learning



Findings #1: Adversarial decision-making

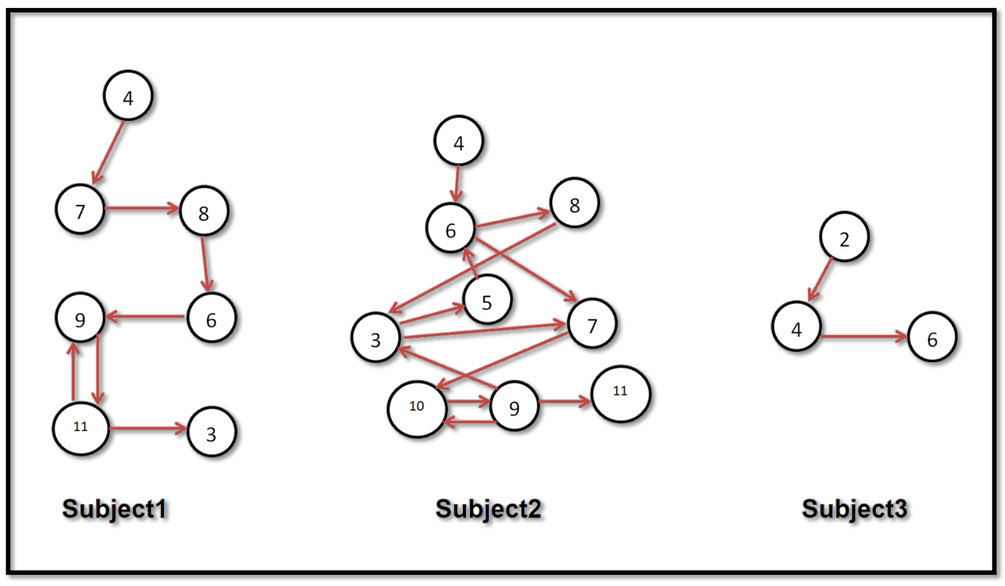
Rege, A., Obradovic, Z., Asadi, N., Singer, S. & Masceri, N. (2017). "A Temporal Assessment of Cyber Intrusion Chains Using Multidisciplinary Frameworks and Methodologies". Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA).

Findings # 3: Machine Learning

Rege, A., Obradovic, Z., Asadi, N., Parker, E., Pandit, R., Masceri, N., Singer, B. (2018) "Predicting Adversarial Cyber Intrusion Stages Using Autoregressive Neural Networks," IEEE Intelligent Systems PP(99):1-1.

Predicted adversarial movement (for two datasets) for 60 % of the intrusion stages despite variations in:

- Exercise **duration** (8 hours vs. 5 hours)
- **Structure** (RBTE vs. paintball)
- **Setting** (cyber-physical facility vs. virtual city)
- Team **size** (10 members vs. 4 members)
- Team members' **familiarity** (randomly assembled vs. some prior relationship)



Findings # 2: Group dynamics & movement

Asadi, N. , Rege, A. & Obradovic, Z. (2018). "An Assessment of Group Dynamics During Cyber Crime Through Temporal Network Topology". Proceedings of the 10th International Conference on Social Computing, Behavioral-Cultural Modeling & Prediction and Behavior Representation in Modeling and Simulation (SBP-BRiMS)

Impact on society

- Cyber range exercise design
- Training participants on divisions of labor and efficiency
- Lessons learned on adversarial group dynamcis and operations

Education & outreach

- Hands-on course projects
  - Critical infrastructure security
  - Social engineering
- Course project downloads & evaluation surveys
  - Shoulder surfing (40), pretexting (34) terms & conditions (28)
  - Worldwide hits (US 85%, Europe 6%, UK 3%, Canada 3%, Asia 3%)
- Data repositories
  - Infrastructure ransomware attacks
- Training workshops
  - 2019 NSF Cybersecurity Summit