An Integrated Approach for Enterprise Intrusion Resilience

Challenge:

- Enterprises are victims of data breaches
- Traditional defenses are not always effective
- Advanced Persistent Threats (APTs) become more and more sophisticated

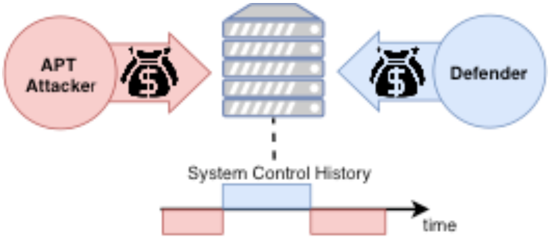
Solution:

- Holistic framework for enterprise defense
- Adaptive defenses based on Reinforcement Learning
- Anti-breach cryptography (key splitting & rotation)
- Privacy-preserving analytics for threat intelligence sharing
  - Secure chain of custody
  - Efficient private set intersection
  - First privacy-preserving hierarchical clustering protocol

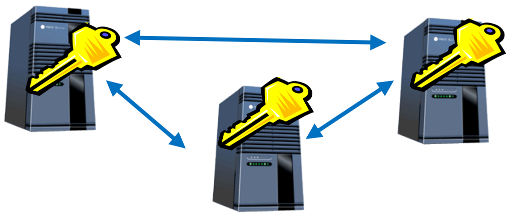
SaTC CNS-1717634 / CNS-1718782

Alina Oprea, Northeastern University
Nikos Triandopoulos, Stevens Institute of Technology

Enterprise Defense Framework



1. Game-theory Modelled Defenses



2. Cryptographic Anti-breach Defenses

3. Community-based Global Defenses

Scientific Impact:

- Novel game theoretical security modeling (based on the FlipIt game)
- Reinforcement Learning can be used to optimize cyber defense
- Privacy-preserving unsupervised learning enables global, community-based defenses across enterprises

Broader Impact:

- Model adaptive defenses against advanced attackers
- Practical protocols can be transitioned to practice
- Involved 2 undergraduate and 5 graduate students in research (3 female)
- Keynote at ACSAC 2018, FinCyberSec 2017
- Papers published in BigData 2018, GameSec 2019, arXiv