Human-AI Cognition for Cyber Protection Teams

Cognitive Twin Modeling

Human-AI Teaming

Adversarial Reasoning

Dr. Prashanth Rajivan
University of Washington

Prof. Cleotilde Gonzalez
Carnegie Mellon University

Dr. Palvi Aggarwal
University of Texas at El Paso

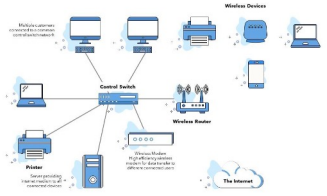
Dr. Nathan McNeese
Clemson University

Prof. Christopher Kiekintveld
University of Texas at El Paso

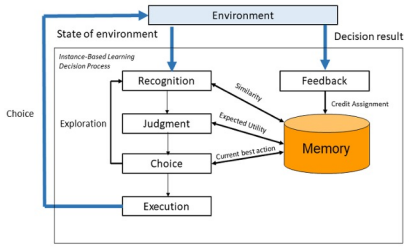
Adaptive Defense Algorithms

Cognitive Twins: Data-Driven Computational Representations for Modeling, Measuring, and Influencing Attacker Behaviors

Observed Attack Sequence



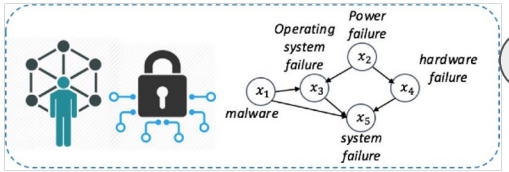
Instance-Based Learning Theory



Cognitive Agent

Strategizing with Predicted Adversarial Behaviors
Kiekintveld, Aggarwal, & Gonzalez

Cognitive Agents to Analyze Attacker Behaviors
Gonzalez, Aggarwal, & Rajivan



Intelligent Algorithms

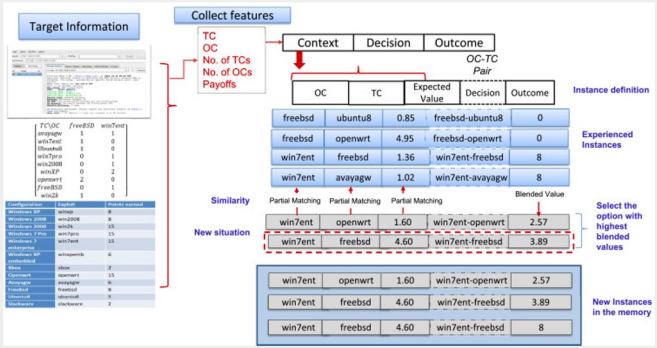
Algorithms for Dynamic and Personalized Deception
Aggarwal, Kiekintveld, & Gonzalez

Human Defender

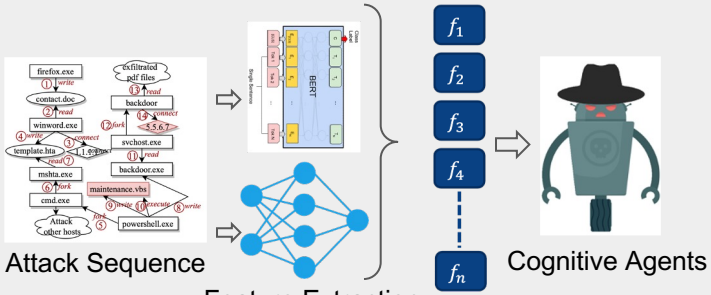
Human-AI Teaming in Cyber Protection Teams
Rajivan, McNeese, & Gonzalez

Past / Current Project Samples

Generate advanced cognitive agents of attacker behaviors



IBL cognitive Agent for Cyber Defense with Deception

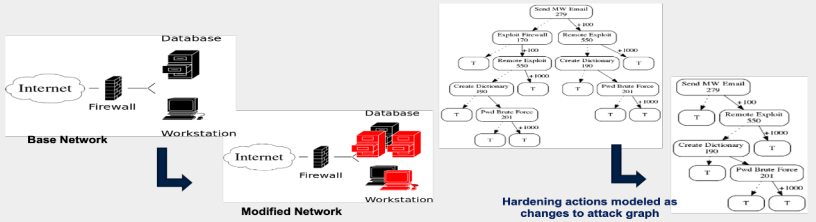


Attack Sequence

Feature Extraction (RNN, NLP)

Cognitive Agents

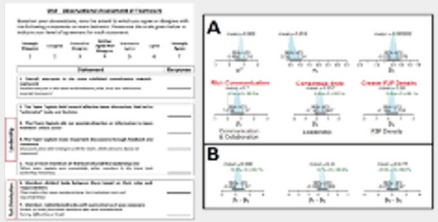
Create defense algorithms for adversarial reasoning and formulating response in near real-time



State of the art game theory and machine learning to adapt defenses based on behavioral models of attackers and defenders

Develop AI teammates for CPTs to ensure accurate, efficient, and safe human-AI collaborations

Current development of the Interactive Defense Game (***IDG***) (Prebot et al., 2022) for research on Human-AI CPTs.



Observational Assessment of Teamwork in Security (***OATS***) instrument and posterior distributions of factors in OATS predictive of CPT performance (Buchler et al., 2018)