THESIS PROPOSAL

Software and Societal Systems Department

Societal Computing Ph.D.

Human and AI Decision Making in Cybersecurity: A Multiagent Modeling Perspective

Yinuo Du

Thursday, June 6th, 2024
TCS 358
12:00 PM - 14:00 PM

Decision-making in cyber defense is a complex challenge, arising from multiple factors. First, it involves strategic interaction among multiple decision-makers—attackers, defenders, and end-users. Second, the diversity of adversaries, ranging from sophisticated nation-state actors to opportunistic script kiddies, adds another layer of difficulty. Third, the network security status is constantly evolving due to the progressive nature of attacks, making it even more challenging to maintain robust defenses. This challenge is exacerbated when integrating human and AI elements in the decision-making process. Limited research has been done to address this multifaceted challenge comprehensively. In this thesis, the goal is to integrate human and AI defense research to counteract the diverse and dynamic threats in network environments. Specifically, the thesis addresses four key challenges: reasoning about diverse adversary strategies, developing adaptive defenses in an evolving security landscape, exploring human-AI defense teams, and fostering cross-organizational collaboration. My completed, in-progress, and proposed work tackles these challenges using game theory, reinforcement learning, human behavior modeling, and human experimentation.

Committee:

Prof. Cleotilde Gonzalez (Co-Chair), Prof. Fei Fang (Co-Chair),
Dr. Christian Lebiere, Prof. Prashanth Rajivan (UW), Prof. Tiffany Bao (ASU)

S3D Software and Societal Systems Department