YINUO DU

Phone: (412)-553-9934 | Email: yinuod@andrew.cmu.edu | Personal Website | Google Scholar | LinkedIn

RESEARCH INTEREST

Human factor, Cyber Security, Human-AI Teaming, Cognitive Modeling, Dynamic Decision Making, Multi-Agent Systems

EDUCATION

Carnegie Mellon University Pittsburgh, PA
Ph.D. in Societal Computing Sep 2021 – May 2026(expected)
Master of Science in Information Technology, GPA: 3.81/4.0 Sep 2019 – May 2021
Xi'an Jiaotong University Xi'an, China
Bachelor of Engineering in Software Engineering, GPA: 3.76/4.0 Sep 2015 – Jun 2019
National University of Singapore Singapore
Summer Course "Biometric in Depth" Jul. 2017-Aug. 2017

RESEARCH EXPERIENCE

Dynamic Decision Making Lab | CMU Pittsburgh, PA
Research Intern May 2020 – May 2021

- Conducted research to enhance effectiveness of honeypots and improve cyber defense
- Designed and launched human experiments
- Build cognitive models of human behavior using instance-based learning theory (IBLT)

Mobile, Embedded, & Wireless Security Lab | CMU Pittsburgh, PA
Practicum Student Sep 2020 – Dec 2020

- Identify vulnerabilities in Zigbee protocols and commercial products
- Create monitoring, analysis, detection, and visualization tools that can view the IoT system holistically in real time

Key Lab for Intelligent Networks and Network Security | XJTU Xi'an, China
Software Engineering Research Intern June 2018 – Sep 2018

- Developed an intelligent deployment platform in Python, which is used for software installation recording, orchestration and playback

INDUSTRY EXPERIENCE

BlockApps Inc. New York, NY
Software Engineering Intern May 2020 – Aug 2020

- Developed STRATO launchpad in Python, a user-friendly multi-platform command line interface tool to extend the configuration and deployment of STRATO from Linux-only to macOS, windows and *nix-based system

Sichuan Hwadee Information Technology Co., Ltd Chengdu, China
Software Engineering Intern Feb 2018 – Mar 2018

- Designed and implemented a platform with function of storing and processing mass data

PUBLICATIONS

[1]. **Yinuo Du**, Baptiste Prébot, Xiaoli Xi, Cleotilde Gonzalez, "Towards Autonomous Cyber Defense: Predictions from a cognitive model", HFES, Atlanta, Georgia, October 10-14, 2022
[2]. **Yinuo Du**, Palvi Aggarwal, Kuldeep Singh, Cleotilde Gonzalez, "A Cognitive Model of Multi-Defender Collaboration in a Cyber-Security Scenario", MathPsych/ICCM, Toronto, Canada, July 23-27, 2022
[3]. **Yinuo Du**, Zimeng Song, Stephanie Milani, Cleotilde Gonzalez, Fei Fang, "Learning to Play an Adaptive Cyber Deception Game", OptLearnMAS, Auckland, New Zealand, May 9--13, 2022
[4]. Palvi Aggarwal, **Yinuo Du**, Kuldeep Singh, Cleotilde Gonzalez, "Decoys in Cybersecurity: An Exploratory Study to Test the Effectiveness of 2-sided Deception", IJCAI-ACD , Montreal, Canada, August 21--23, 2021

WORKING PAPERS

[1]. Palvi Aggarwal, **Yinuo Du**, Kuldeep Singh, Shashank Uttrani, Varun Dutt, Cleotilde Gonzalez, "Effectiveness of Deploying Honeypots in Different Network Topologies", submitted to Journal of Information Security and Applications.
[2]. Baptiste Prébot, **Yinuo Du**, Xiaoli Xi, Cleotilde Gonzalez, "Cognitive Models of Dynamic Decisions in Autonomous Intelligent Cyber Defense", submitted to AICA 2022.

[3]. **Yinuo Du**, Baptiste Prébot, Xiaoli Xi, Cleotilde Gonzalez, "A Cyber-War Between Bots: Human-Like Attackers are More Challenging for Defenders than Deterministic Attackers" , submitted to HICSS 2023.
[4]. Palvi Aggarwal, **Yinuo Du**, Kuldeep Singh, Cleotilde Gonzalez, "Modeling Attackers' Decisions in Cyber-Deception Scenarios", submitted to HICSS 2023.

WORK IN PROGRESS

- Multi Defender Game of Cyber Threat Intelligence Sharing. Work with Cleotilde Gonzalez, Palvi Aggarwal and Kuldeep Singh.
- Autonomous Cyber Defense. Work with Cleotilde Gonzalez, Baptiste Prébot and Xiaoli Xi.
- Cyber Deception Evaluation. Work with Cleotilde Gonzalez, Fei Fang, Vyas Sekar, Lujo Bauer, and Brian Singer

PRESENTATIONS

Talks

- "A Cognitive Model of Multi-Defender Collaboration in a Cyber-Security Scenario", ICCM, July 2022
- "Multi-Defender Collaboration in a Cyber-Security Scenario", CRA seminar, June 2022

Poster Presentations

- "Towards Autonomous Cyber Defense: Predictions from a cognitive model", HFES, October 2022

HONORS AND AWARDS

- Foho Technical Innovation Grants from Jiangsu Foho High-Tech Industrial Development Zone 2018
- National Encouragement Scholarship (top 5%) 2017-2018
- National Encouragement Scholarship (top 5%) 2016-2017
- National Encouragement Scholarship (top 5%) 2015-2016

SKILLS

Programming language: R, Java, Python, JavaScript, C/C++
Platforms: Django/Flask, OpenStack, Ansible
Experiments: mTurk, Prolific, NodeGame, CyberVAN
Data Visualization: ggplot2, Matplotlib, Pandas