YINUO DU

Phone: (412)-553-9934 | Email: [yinuod@andrew.cmu.edu](mailto:yinuod@andrew.cmu.edu) | [Personal Website](https://aduyinuo.github.io/) | [Google Scholar](https://scholar.google.com/citations?hl=en&user=XdY3VB0AAAAJ) | [LinkedIn](http://www.linkedin.com/in/yinuo-du)

# 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

# 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

**Key Lab for Intelligent Networks and Network Security | XJTU** Xi’an, China

Software Engineering Intern June 2018 – Sep 2018

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

**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

**Yinuo Du**, Baptiste Prébot, Xiaoli Xi, Cleotilde Gonzalez, “Towards Autonomous Cyber Defense: Predictions from a cognitive model”, HFES, Atlanta, Georgia, October 10-14, 2022

**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

**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

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

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.

Baptiste Prébot, **Yinuo Du**, Xiaoli Xi, Cleotilde Gonzalez, “Cognitive Models of Dynamic Decisions in Autonomous Intelligent Cyber Defense”, submitted to AICA 2022.

**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.

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 and Palvi Aggarwal.
* Human-AI Teaming in CybORG. Work with Cleotilde Gonzalez and Baptiste Prébot.
* Cyber Deception Evaluation. Work with Cleotilde Gonzalez, Fei Fang, Vyas Sekar, Lujo Bauer, and Brian Singer

# ACADEMIC PROJECTS

**HomeKat**: **A security analysis of the HomeKit Framework from an Operating System, Network Implementation and a Network Security perspective to analyze the security of data at rest and data at flow within and outside the local network**

**O’share**: A website based on Bootstrap, Angular8 and Django RESTful, provides search engine and filtering functions for cosmetic products, allows user interaction with social network functionality, supports product purchasing.

**CloudFS**: A cloud-backed local file system using both AWS S3 and local SSD storage, provides block-level deduplication scheme to save cloud space, snapshot scheme for data backup, write back LRU cache to reduce network transfer.

**MyFTL**: A flash translation layer for solid-state disks, provides hybrid log-block mapping for address translation, a page-mapping scheme and a block assigning scheme with wear-leveling to improve SSD life span, 4 garbage collection policies

**Personal Digital Assets Storage and Evaluation Based on Ethereum:** A Decentralized Application (DApp) based on Ethereum in order to securely store users’ digital assets such as game accounts and passwords.

**Collecting Package on Behalf of Purchasers:** A Wechat Mini Program to enable the ”purchasers” students to pay the “courier” students who help them collect packages on behalf of them from couriers, when they were not available for signing for their packages in person.

# SKILLS

**Programming language:** Java, Python, JavaScript, C/C++