

Paul Yi Won Chung

me@pywc.dev
https://pywc.dev/
1210 W Dayton St, Madison, WI 53706

Research Interests

Systems Security, Anti-censorship, Privacy, Networks, Operating Systems, Blockchain, Cryptography

Education

University of Wisconsin-Madison

B.S. Honors Candidate, Computer Sciences & Data Science
Thesis: Network Censorship Measurement and Evasion Framework
Advisor: Rahul Chatterjee

Fall 2020 ~ Spring 2024
Madison, WI
GPA: 3.97/4.00

Neung-In High School

STEM High School Degree

Spring 2017 ~ Fall 2019
Daegu, Republic of Korea

Positions

University of Wisconsin-Madison - MadS&P

Undergraduate Research Assistant

Madison, WI
06/2021 ~ Present

University of Wisconsin-Madison - WI-PI

Undergraduate Research Assistant

Madison, WI
10/2021 ~ Present

UW-Madison Cybersecurity Operations Center

Cybersecurity Intern Analyst

Madison, WI
10/2020 ~ Present

Cybersecurity UW Student Club

President & CTF Team Lead

Madison, WI
09/2020 ~ Present

Carnegie Mellon University – CyLab

Undergraduate Research Assistant

Pittsburgh, PA
Summer 2022

Igloo Security

Cybersecurity Intern Analyst

Seoul, Republic of Korea
Summer 2019

Research

Shawshank Intel: A Heuristic-based Analysis of Network Censorship Mechanisms

UW-Madison Security & Privacy Research Group (MadS&P)

- Formulated a heuristic-based approach for analyzing network censorship middleboxes
- Developed an internet filtering measurement pipeline and tested it on networks under various nations

09/2022 ~ Present
Advisor: Rahul Chatterjee

Automatic Enforcement of Google Data Safety Cards

UW-Madison Security & Privacy Research Group (MadS&P)

- Labeled over 500 Privacy Policies and trained them to data safety card options with DistilBERT
- Analyzed over 2000 responses from the developer inquiry about data safety card inconsistencies

11/2022 ~ Present
Advisor: Kassem Fawaz

Engineering Privacy in iOS App Groups

Carnegie Mellon University Information Networking Institute (INI)

- Implemented a data leakage threat model for the iOS app group containers
- Analyzed the group containers for 200 iOS apps to detect potential leakage for restricted data

Summer 2022
Advisor: Hanan Hibshi

picoCTF: Introducing Adversarial Machine Learning to CTFs

Carnegie Mellon University Security & Privacy Laboratory (CyLab)

- Developed five NLP-based and five CNN-based Adversarial Machine Learning challenges
- Constructed a user study for the challenges to be released at picoCTF 2023
- Introduced "ramped" difficulty system, optimized for beginning learners

Summer 2022
Advisor: Hanan Hibshi

CookieEnforcer: Automated Cookie Notice Analysis and Enforcement

Wisconsin Privacy & Security Research Group (WI-PI)

- Explored the results of the front-end interface user study for the CookieEnforcer research
- Developed a Chrome Extension that connects the CookieEnforcer backend with the React frontend
- Published the extension to the Chrome Extension Store

02/2022 ~ 07/2022
Advisor: Kassem Fawaz

Araña: Discovering and Characterizing Password Guessing Attacks in Practice

UW-Madison Security & Privacy Research Group (MadS&P)

- Analyzed 30 million network packets to find a pattern of credential stuffing attacks

06/2021 ~ 10/2022
Advisor: Rahul Chatterjee

- Used Pandas and Matplotlib of Python to visualize and find edge cases from the data
- Found multiple patterns in the clustered data that exhibited anomalies

Zero-day Vulnerability Analysis and Exploitation

Daegu University Information Security Research Group

03/2019 ~ 05/2020

Advisor: Chang Hoon Kim

- Analyzed the risk of CVE-2019-0708 (Bluekeep) on traditional embedded systems
- Designed a PoC that sends payloads to execute arbitrary code on the vulnerable system
- Poster presented the research as the primary author at *CISC-W' 2019*

Publications

-
- [1] **Yi Won Chung** and Tae Gyeom Heo. Exploitation of RDP Bluekeep on Embedded Systems and Possible Mitigations. *Proceedings of the Conference on Information Security and Cryptography-Winter, 2019*.
- [2] Marina Sanusi Bohuk, Mazharul Islam, **Paul Chung**, Thomas Ristenpart, and Rahul Chatterjee. Araña: Discovering and Characterizing Password Guessing Attacks in Practice. *32nd USENIX Security Symposium, 2023*.

Projects

Node.js Full-stack Web Application

HackMIT, 2021

- Designed a RESTful Backend API model and implemented it via Express and PostgreSQL
- Implemented a simple front-end web interface with EJS and integrated it to the backend
- Deployed resulting web app *FoodSurfers*, similar with the *Airbnb* platform to Microsoft Azure

Voice-based Interactive Chatbot

Neung-In Scholarly Awards, 2018

- Designed a chatbot pipeline that parses lunch and academic calendar info from the school website
- Deployed the app to GCP and used the Google Dialogflow API to service it on Google Assistant
- 85% of school affiliates had been active users of the chatbot by 2 months of release

Honors and Awards

-
- 2023 Hilldale Undergraduate Research Fellowship
 - 2023 Barry M. Goldwater Scholarship
 - 2022 Carnegie Mellon University Summer Undergraduate Research Scholarship
 - Fall 2020 ~ Fall 2022, UW-Madison Dean's List
 - 2022 National Cyber League Spring Team Game, Top 2% (as team: *Oxb4dgers*)
 - 2019 Korea Ministry of Education Cybersecurity CTF Competition, 5th Place (as team: *Future College Chancellor Shin Jinwoo*)

Skills

-
- Programming Languages: Python, C, C++, Java, JavaScript, PHP, Rust
 - Technologies:
 - General: Git, LaTeX, Numpy, Docker
 - Data Analysis: Pandas, Matplotlib, R, SPSS
 - Machine Learning: HuggingFace, Scikit, PyTorch, TensorFlow, Keras, NLTK
 - Network: Socket, Scapy, dpkt, aioquic
 - Web: HTML, Flask, Django, Jekyll, Hugo, React, Express
 - Security: Pwntools, Elasticsearch, Shodan, Nmap, Burpsuite, Cisco AMP
 - Database: MySQL, PostgreSQL, MongoDB, SQLite
 - Cloud: GCP, Azure, AWS