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 — Fall 2020 ~ Spring 2024
B.S. Honors Candidate, Computer Sciences & Data Science — Madison, WI
Thesis: Characterizing Network Censorship Mechanisms Worldwide — GPA: 3.97/4.00
Advisor: Rahul Chatterjee

Neung-In High School — Spring 2017 ~ Fall 2019
STEM High School Degree — Daegu, Republic of Korea

Positions

University of Wisconsin-Madison - MadS&P — Madison, WI
Undergraduate Research Assistant — 06/2021 ~ Present

University of Wisconsin-Madison - WI-PI — Madison, WI
Undergraduate Research Assistant — 10/2021 ~ Present

UW-Madison Cybersecurity Operations Center — Madison, WI
Cybersecurity Intern Analyst — 10/2020 ~ Present

Cybersecurity UW Student Club — Madison, WI
President & CTF Team Lead — 04/2023 ~ Present

Max Planck Institute for Software Systems — Saarbrücken, Germany
Visiting Scholar — Summer 2023

Carnegie Mellon University – CyLab — Pittsburgh, PA
Undergraduate Research Assistant — Summer 2022

Igloo Security — Seoul, Republic of Korea
Cybersecurity Intern Analyst — Summer 2019

Research

Shawshank Intel: A Heuristic-based Analysis of Network Censorship Mechanisms — 09/2022 ~ Present
UW-Madison Security & Privacy Research Group (MadS&P) — Advisor: Rahul Chatterjee
- Formulated a heuristic-based approach for analyzing network censorship middleboxes
- Developed an internet filtering measurement pipeline and tested it on networks under various nations

Automatic Enforcement of Google Data Safety Cards — 11/2022 ~ Present
UW-Madison Security & Privacy Research Group (MadS&P) — Advisor: Kassem Fawaz
- 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

Engineering Privacy in iOS App Groups — Summer 2022
Carnegie Mellon University Information Networking Institute (INI) — Advisor: Hanan Hibshi
- 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

picoCTF: Introducing Adversarial Machine Learning to CTFs — Summer 2022
Carnegie Mellon University Security & Privacy Laboratory (CyLab) — Advisor: Hanan Hibshi
- 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

CookieEnforcer: Automated Cookie Notice Analysis and Enforcement — 02/2022 ~ 07/2022
Wisconsin Privacy & Security Research Group (WI-PI) — Advisor: Kassem Fawaz
- 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

Araña: Discovering and Characterizing Password Guessing Attacks in Practice — 06/2021 ~ 10/2022

UW-Madison Security & Privacy Research Group (MadS&P) Advisor: Rahul Chatterjee

- Analyzed 30 million network packets to find a pattern of credential stuffing attacks
- 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 03/2019 ~ 05/2020

Daegu University Information Security Research Group 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 became active users of the chatbot by 2 months of release

Honors and Awards

- 2023 Barry M. Goldwater Scholarship
- 2023 Hilldale Undergraduate Research Fellowship
- 2022 Carnegie Mellon University Summer Undergraduate Research Fellowship
- Fall 2020 ~ Fall 2022, UW-Madison Dean's List
- 2022 National Cyber League Spring Team Game, Top 2% (as team: *0xb4dgers*)
- 2019 Korea Ministry of Education 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