# Paul Yi Won Chung

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

## Research Interests

System Security, Privacy, User Authentication, Networks, Internet of Things, Applied Cryptography, and Machine Learning.

## 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: 3.94/4.00
Advisor: Rahul Chatterjee

## Publications

[1] Rishabh Khandelwal, Asmit Nayak, **Paul Chung,** and Kassem Fawaz. Unpacking Privacy Labels: A Measurement and Developer Perspective on Google's Data Safety Section. *USENIX Security, 2024*.

[2] Marina Sanusi Bohuk, Mazharul Islam, **Paul Chung,** Thomas Ristenpart, and Rahul Chatterjee. Araña: Discovering and Characterizing Password Guessing Attacks in Practice. *USENIX Security, 2023*.

[3] Rishabh Khandelwal, Asmit Nayak, **Paul Chung,** and Kassem Fawaz. Comparing Privacy Labels of Applications in Android and iOS. *Workshop on Privacy in the Electronic Society (WPES), 2023*.

[4] **Yi Won Chung** and Tae Gyeom Heo. Exploitation of Bluekeep RDP Vulnerability on Embedded Systems and Possible Mitigations. *Conference on Information Security and Cryptography-Winter (CISC-W'), 2019*.

[5] **Paul Chung** and Rahul Chatterjee. Shawshank Breakout: Uncovering State-of-the-Art Tactics Used by Network Censorship Systems. *Under Submission*, *2024*.

[6] Maryam Aldairi, Arjun Brar, Hanan Hibshi, Kuixi Song, **Paul Yi Won Chung,** Daniel Votipka, Marjan Salamati-Pour, and Akanksha Bubber. Is Sandboxing Enough? The Challenge of Engineering Privacy in iOS App Groups: A Developer Perspective. *Under Submission, 2024*.

[7] Rishabh Khandelwal, **Paul Chung,** Asmit Nayak, and Kassem Fawaz. Consistency of Self-reported Practices in Privacy Labels and Privacy Policies. *Under Submission, 2024*.

## Talks

[1] **Paul Chung**. Comparing Privacy Labels of Applications in Android and iOS. *Workshop on Privacy in the Electronic Society (WPES), 2023 (co-located with CCS 2023)*. Conference Talk.

[2] **Yi Won Chung**. Exploitation of Bluekeep RDP Vulnerability on Embedded Systems and Possible Mitigations. *Conference on Information Security and Cryptography-Winter (CISC-W'), 2019*. Poster Presentation.

[3] **Paul Chung**. Introducing Adversarial Machine Learning to CTFs using a Ramped Difficulty Framework. *CMU REUSE, 2022*. Poster Presentation.

## Honors and Awards

- 2023 Barry M. Goldwater Scholarship
- 2023 Mark Mensink Honors Research Grant
- 2023 Hilldale Undergraduate Research Fellowship
- 2023 Max Planck Institute for Software Systems CMMRS Travel Grant (*NSF-funded*)
- 2022 CMU REUSE Undergraduate Research Fellowship (*NSF-funded*)
- 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*)

## Positions

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

**UW-Madison Cybersecurity Operations Center** — Madison, WI
Cybersecurity Student Analyst Team Lead — 10/2020 ~ Present

**MetaCTF** — Remote
Content Developer — 07/2023 ~ Present

**Cybersecurity UW Student Club** — Madison, WI
President — 04/2021 ~ Present

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

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

## Research Projects

**Automated Privacy Advisor Chatbot** 10/2023 ~ Present
*UW-Madison Security & Privacy Research Group (MadS&P)* Advisor: Kassem Fawaz
- Extended the idea from the original PriBOT work to design a privacy-practices-answering chatbot
- Trained a Llama 2 model using AdaptLLM, QLoRA, and privacy documents scraped from mobile apps

**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

**Analysis of Google Data Safety Cards and Apple Privacy Labels** 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
- Modeled an inference-based analysis approach to analyze the consistencies within privacy documents

**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*

## Individual Projects

**Scalable Docker Deployment System** Cybersecurity UW, 2023
- Designed a RESTful API that deploys scalable docker instances for interactive club meetings
- Utilized the docker system to demonstrate Password Cracking, Buffer Overflow, and RF challenges

**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 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