

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 Adversarial Machine Learning.

Education

University of Wisconsin-Madison B.S. Honors Candidate, Computer Sciences & Data Science Thesis: Characterizing Network Censorship Mechanisms Worldwide Advisor: Rahul Chatterjee	Fall 2020 ~ Spring 2024 Madison, WI GPA: 3.94/4.00
--	--

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 Symposium*, 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 Symposium*, 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 Undergraduate Research Assistant	Madison, WI 06/2021 ~ Present
UW-Madison Cybersecurity Operations Center Cybersecurity Student Analyst Team Lead	Madison, WI 10/2020 ~ Present
MetaCTF Content Developer	Remote 07/2023 ~ Present
Cybersecurity UW Student Club President	Madison, WI 04/2021 ~ Present
Carnegie Mellon University – CyLab Undergraduate Research Assistant	Pittsburgh, PA Summer 2022
Igloo Security Cybersecurity Intern Analyst	Seoul, Republic of Korea Summer 2019

Research Projects

Automated Privacy Advisor Chatbot

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

- 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

10/2023 ~ Present

Advisor: Kassem Fawaz

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

Analysis of Google Data Safety Cards and Apple Privacy Labels

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
- Modeled an inference-based analysis approach to analyze the consistencies within privacy documents

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
- Introduced "ramped" difficulty system, optimized for beginning learners
- Contributed one NLP challenge to the 2023 IC3 Game, hosted by MetaCTF

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
- 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

06/2021 ~ 10/2022

Advisor: Rahul Chatterjee

Zero-day Vulnerability Analysis and Exploitation

Daegu University Information Security Research Group

- 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*

03/2019 ~ 05/2020

Advisor: Chang Hoon Kim

Individual Projects

Scalable Docker Deployment System

- 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

Cybersecurity UW, 2023

Node.js Full-stack Web Application

- 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

HackMIT, 2021

Voice-based Interactive Chatbot

- 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

Neung-In Scholarly Awards, 2018