Paul Yi Won Chung

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

Education

University of California, San Diego — 09/2024 ~ Exp. 2029
Ph.D., Computer Sciences — La Jolla, CA

University of Wisconsin-Madison — 09/2020 ~ 05/2024
B.S. with Honors, Computer Sciences & Data Science — Madison, WI

Advisors: *Rahul Chatterjee, Kassem Fawaz*
Thesis: "Characterizing Network Censorship Mechanisms Worldwide"

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

- 2024 NSF Graduate Research Fellowship Honorable Mention
- 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*)

Academic Service

- SOUPS 2024 – Poster Jury

Employment

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 ~ 08/2023

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

Carnegie Mellon University – CyLab — Pittsburgh, PA
Undergraduate Research Assistant — 05/2022 ~ 08/2022

Igloo Security — Seoul, South Korea
Cybersecurity Intern Analyst — 08/2019

Daegu University – Information Security Institute — Daegu, South Korea
High School Research Assistant — 01/2019 ~ 02/2020

Research Projects

Usage of LLMs for Data Privacy Annotations — 10/2023 ~ Present
UW-Madison Security & Privacy Research Group (MadS&P) — Advisor: Kassem Fawaz

- Annotated over 500 Privacy Policies to the OPP-115 dataset
- Trained a Llama 2 model using AdaptLLM and mobile app privacy documents

Shawshank Intel: An Evasion-based Analysis of Network Censorship Tactics — 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 a middlebox measurement pipeline and tested it on networks under 207 ISPs

Analysis of Google Data Safety Cards and Apple Privacy Labels 11/2022 ~ Present
UW-Madison Security & Privacy Research Group (MadS&P) Advisor: Kassem Fawaz

- Analyzed over 2000 developer inquiry responses about data safety card inconsistencies
- Analyzed the privacy label consistencies of apps cross-listed on both platforms

Engineering Privacy in iOS App Groups 05/2022 ~ 08/2022
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 data leakage

picoCTF: Introducing Adversarial Machine Learning to CTFs 05/2022 ~ 08/2022
Carnegie Mellon University Security & Privacy Laboratory (CyLab) Advisor: Hanan Hibshi

- Developed five NLP and five CNN-based Adversarial Machine Learning challenges
- Introduced "ramped" difficulty system, optimized for beginning learners
- Contributed one Bag-of-words challenge to the 2023 IC3 Games, hosted by MetaCTF

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 user study for the CookieEnforcer research
- Developed a Chrome Extension that connects the CookieEnforcer backend
- 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 Institute Advisor: Chang Hoon Kim

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