Paul Yi Won Chung

paulc@ucsd.edu
https://paulchu.ng/
9500 Gilman Dr, La Jolla, CA 92037

Education

University of California, San Diego — 2024 - Present
Ph.D. Student in Computer Science & Engineering — La Jolla, CA
Advisors: *Stefan Savage, Geoffrey Voelker*

University of Wisconsin-Madison — 2020 - 2024
B.S. with Honors in Computer Sciences & Data Science — Madison, WI
Advisors: *Rahul Chatterjee, Kassem Fawaz*
Thesis: "Characterizing Network Censorship Mechanisms Worldwide"

Publications

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

[2] **Consistency of Self-reported Practices in Privacy Labels and Privacy Policies**
Rishabh Khandelwal, Paul Chung, Asmit Nayak, and Kassem Fawaz
Arxiv Preprint, 2024

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

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

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

[6] **Shortcut Automation Tools on Intimate Partner Violence**
Shirley Zhang, Jacob VerVelde, Paul Chung, Rahul Chatterjee, and Kassem Fawaz
Under Submission, 2025

[7] **Academia and Industry Insights on Adversarial Machine Learning**
Vishruti Kakkad, Paul Chung, Hanan Hibshi, Maverick Woo
Under Submission, 2025

[8] **State-of-the-Art Tactics Used by Network Censorship Systems**
Paul Chung and Rahul Chatterjee
Under Submission, 2025

Talks

[1] **Towards Identifying the Censorship Ruleset Patterns and Obscure Approaches**
UW-Madison Senior Honors Thesis Symposium, 2024. Thesis Presentation.

[2] **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.

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

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

Awards

- 2024 NSF Graduate Research Fellowship - Honorable Mention
- 2024 UC San Diego Jacobs School of Engineering Fellowship
- 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 Korean Ministry of Education CTF - 5th Place (as team: *Future College Chancellor Shin Jinwoo*)

Academic Service

- PETS 2025 – Artifact Evaluation Committee Member
- SOUPS 2024 – Poster Jury

Employment

University of California, San Diego Graduate Research Assistant	La Jolla, CA 2024 - Present
University of Wisconsin-Madison – MadS&P Undergraduate Research Assistant	Madison, WI 2021 - 2024
UW-Madison Cybersecurity Operations Center Cybersecurity Student Analyst Team Lead	Madison, WI 2020 - 2024
MetaCTF Content Developer	Remote 2023
Carnegie Mellon University – CyLab Undergraduate Research Assistant	Pittsburgh, PA 2022
Igloo Security Cybersecurity Intern Analyst	Seoul, South Korea 2019

Daegu University – Information Security Institute Daegu, South Korea
High School Research Assistant 2019 - 2020

Projects

CRASHCART: Ransomware Detection and Recovery in Hospitals 2024 - Present
UC San Diego Systems and Networking Research Group (SysNet)
- Explored the NTP server selection strategies for server downtime detection

Analyzing Abuse Capabilities of Mobile Automation Tools 2024
UW-Madison Security & Privacy Research Group (MadS&P)
- Constructed threat models for data exfiltration and harassment through automation tools
- Implemented Proof-of-Concepts of the models via iOS Shortcuts and IFTTT

Usage of LLMs for Data Privacy Annotations 2023 - 2024
UW-Madison Security & Privacy Research Group (MadS&P)
- Annotated over 500 Privacy Policies to the OPP-115 taxonomy
- Trained a Llama 2 model using AdaptLLM and mobile app privacy documents

Finding Edge Cases to Circumvent Network Censorship 2022 - 2024
UW-Madison Security & Privacy Research Group (MadS&P)
- Formulated a heuristic-based approach for analyzing network censorship middleboxes
- Developed a middlebox measurement pipeline and tested it on networks under 207 ISPs

picoCTF: Introducing Adversarial Machine Learning to CTFs 2022 - 2024
Carnegie Mellon University Security & Privacy Laboratory (CyLab)
- 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

Analysis of Google Data Safety Cards and Apple Privacy Labels 2022 - 2023
UW-Madison Security & Privacy Research Group (MadS&P)
- Analyzed over 2000 developer inquiry responses about data safety card inconsistencies
- Analyzed the privacy label consistencies of apps cross-listed on both platforms

Discovering and Characterizing Password Guessing Attacks in Practice 2021 - 2023
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

Zero-day Vulnerability Analysis and Exploitation 2019 - 2020
Daegu University Information Security Institute
- 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*