

# Paul Yi Won Chung

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

## Current Position

Undergraduate Student, Computer Sciences & Data Science, University of Wisconsin-Madison

## Research Interests

Building systems that enhance computer security and privacy, specifically in topics including:

- System and Network Security, Internet of Things, Usability in Security and Privacy, Emerging Technologies, Applied Cryptography, User Authentication, and Network Censorship.

## Education

<b>University of Wisconsin-Madison</b>	Fall 2020 ~ Spring 2024
B.S. with Honors, Computer Sciences & Data Science	Madison, WI
Advisor: Rahul Chatterjee	
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

- 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: *Oxb4dgers*)
- 2019 Korea Ministry of Education CTF Competition, 5<sup>th</sup> Place (as team: *Future College Chancellor Shin Jinwoo*)

## Academic Service

- SOUPS 2024 – Poster Jury

## Employment

<b>University of Wisconsin-Madison – MadS&amp;P &amp; WI-PI</b>	Madison, WI
Undergraduate Research Assistant	06/2021 ~ Present
<b>UW-Madison Cybersecurity Operations Center</b>	Madison, WI
Cybersecurity Student Analyst Team Lead	10/2020 ~ Present
<b>MetaCTF</b>	Remote
Content Developer	07/2023 ~ 08/2023
<b>Cybersecurity UW Student Club</b>	Madison, WI
President	04/2021 ~ Present
<b>Carnegie Mellon University – CyLab</b>	Pittsburgh, PA
Undergraduate Research Assistant	05/2022 ~ 08/2022
<b>Igloo Security</b>	Seoul, South Korea
Cybersecurity Intern Analyst	08/2019
<b>Daegu University – Information Security Institute</b>	Daegu, South Korea
High School Research Assistant	01/2019 ~ 02/2020

## Research Projects

<b>Usage of LLMs for Data Privacy Annotations</b>	10/2023 ~ Present
<i>UW-Madison Security &amp; Privacy Research Group (MadS&amp;P)</i>	Advisor: Kassem Fawaz
<ul style="list-style-type: none"> <li>▪ Annotated over 500 Privacy Policies to the OPP-115 dataset</li> <li>▪ Trained a Llama 2 model using AdaptLLM and privacy documents scraped from mobile apps</li> </ul>	
<b>Shawshank Intel: An Evasion-based Analysis of Network Censorship Tactics</b>	09/2022 ~ Present
<i>UW-Madison Security &amp; Privacy Research Group (MadS&amp;P)</i>	Advisor: Rahul Chatterjee
<ul style="list-style-type: none"> <li>▪ Formulated a heuristic-based approach for analyzing network censorship middleboxes</li> <li>▪ Developed an internet filtering measurement pipeline and tested it on networks under 207 ISPs</li> </ul>	
<b>Analysis of Google Data Safety Cards and Apple Privacy Labels</b>	11/2022 ~ Present
<i>UW-Madison Security &amp; Privacy Research Group (MadS&amp;P)</i>	Advisor: Kassem Fawaz
<ul style="list-style-type: none"> <li>▪ Analyzed over 2000 developer inquiry responses about data safety card inconsistencies</li> <li>▪ Analyzed the privacy label consistencies of apps cross-listed on both platforms</li> </ul>	
<b>Engineering Privacy in iOS App Groups</b>	Summer 2022
<i>Carnegie Mellon University Information Networking Institute (INI)</i>	Advisor: Hanan Hibshi
<ul style="list-style-type: none"> <li>▪ Implemented a data leakage threat model for the iOS app group containers</li> <li>▪ Analyzed the group containers for 200 iOS apps to detect potential leakage for restricted data</li> </ul>	
<b>picoCTF: Introducing Adversarial Machine Learning to CTFs</b>	Summer 2022
<i>Carnegie Mellon University Security &amp; Privacy Laboratory (CyLab)</i>	Advisor: Hanan Hibshi
<ul style="list-style-type: none"> <li>▪ Developed five NLP-based and five CNN-based Adversarial Machine Learning challenges</li> <li>▪ Introduced “ramped” difficulty system, optimized for beginning learners</li> <li>▪ Contributed one Bag-of-words challenge to the 2023 IC3 Games, hosted by MetaCTF</li> </ul>	

**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 Institute*

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*