

# (PAUL) YI WON CHUNG

Madison, WI ◊ he/him/his  
+1 (763) 290-8855 ◊ paul.chung@wisc.edu ◊ <https://pywc.dev/>

## RESEARCH INTERESTS

Cybersecurity, Privacy, Machine Learning, Operating Systems, Networking, Cloud Computing, Cryptography

## EDUCATION

<b>University of Wisconsin-Madison</b> Candidate for Bachelor of Science in Computer Sciences & Data Science Honors Candidate in Liberal Arts	Fall 2020 ~ Present GPA: 4.0/4.0
<b>Neung-In High School</b> Vice Chancellor for Class of 2020 Student Council	March 2016 ~ February 2020 Daegu, Republic of Korea

## POSITIONS

<b>UW-Madison Cybersecurity Operations Center</b> Cybersecurity Intern Analyst <ul style="list-style-type: none"><li>Participated in campus incident response and client-side and server-side malicious traffic analysis</li><li>Designed an automated report and notification generation system with Bash, Python, and Confluence API.</li></ul>	Madison, WI October 2020 ~ Present
<b>Cybersecurity UW</b> Head Officer <ul style="list-style-type: none"><li>Made presentations on various Cybersecurity and Machine Learning topics to undergraduate students.</li><li>Formed <i>0xbadg3rs</i> CTF division and participated in numerous cybersecurity competitions.</li></ul>	Madison, WI September 2020 ~ Present
<b>Indie Hackers Forum</b> Founder, President & Competition Team Lead <ul style="list-style-type: none"><li>Made presentations on various cybersecurity topics at several organizations.</li><li>Formed a competition team and participated in numerous cybersecurity competitions as the team lead.</li></ul>	Daegu, Republic of Korea March 2016 ~ February 2020
<b>Igloo Security</b> Student Intern <ul style="list-style-type: none"><li>Learned and participated in basic Cybersecurity Incident Response.</li><li>Collected multiple malware samples to be used in the Machine Learning pipeline for predicting malware patterns.</li></ul>	Seoul, Republic of Korea August 2019

## RESEARCH

<b>Engineering Privacy in iOS App Groups</b> <i>Carnegie Mellon University Information Networking Institute (INI)</i> <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>	June 2022 ~ August 2022 Advisor: Hanan Hibshi
<b>picoCTF: Cybersecurity Education through Gamification Theory</b> <i>Carnegie Mellon University Security &amp; Privacy Laboratory (CyLab)</i> <ul style="list-style-type: none"><li>Developed five NLP-based and five CNN-based Adversarial Machine Learning challenges</li><li>Constructed a user study for the challenges to be released at picoCTF 2023</li><li>Introduced “ramped” difficulty system, optimized for beginning learners</li></ul>	May 2022 ~ August 2022 Advisor: Hanan Hibshi
<b>CookieEnforcer: Automated Cookie Notice Analysis and Enforcement</b> <i>Wisconsin Privacy &amp; Security Research Group (WI-PI)</i> <ul style="list-style-type: none"><li>Explored the results of the front-end interface user study for the CookieEnforcer backend</li><li>Developed a Chrome Extension that connects the CookieEnforcer backend with the React.js frontend</li><li>Published the extension to Chrome Extension Store</li></ul>	February 2022 ~ Present Advisor: Kassem Fawaz
<b>Securely Measuring Password-based Logins</b> <i>UW-Madison Security &amp; Privacy Research Group (MadS&amp;P)</i> <ul style="list-style-type: none"><li>Analyzed 30 million network packets to find a pattern of credential stuffing attacks</li><li>Used Pandas and Matplotlib of Python to visualize and find edge cases from the data</li><li>Found multiple patterns that exhibited anomalies</li></ul>	June 2021 ~ Present Advisor: Rahul Chatterjee
<b>Zero-day Vulnerability Analysis and Exploitation</b> <i>Daegu University Information Security Research Group</i> <ul style="list-style-type: none"><li>Analyzed the risk factor of CVE-2019-0708 (Bluekeep) RDP vulnerability on traditional embedded systems</li><li>Designed a Python Proof of Concept script that sends payloads to execute arbitrary code on the vulnerable system</li><li>Poster presented the research as the primary author at <i>Conference on Information Security and Cryptology-Winter, 2019</i></li></ul>	March 2019 ~ May 2020 Advisor: Chang Hoon Kim

## PUBLICATIONS

---

- [1] **Yi Won Chung**, Tae Gyeom Heo. Exploitation of RDP Bluekeep on Embedded Systems and Possible Mitigations. *Proceedings of the Conference on Information Security and Cryptography-Winter, 2019*.

## PROJECTS

---

### 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 resulting web app “FoodSurfers”, similar with the AirBnB platform to Microsoft Azure

### Voice-based Interactive Chatbot

Neung-In High School Scholarly Awards, 2018

- Used Django and BeautifulSoup4 to design a school chatbot server and to parse lunch and academic calendar from the school website
- Deployed the app to Google Cloud Platform and used the Google Dialogflow API to service it via Google Assistant
- Attained school affiliate usage rate of 85% by 2 months of release.

## HONORS AND AWARDS

---

- Top 2%, National Cyber League Spring 2022 Team Game
- 5<sup>th</sup> Place, Korea Ministry of Education Cybersecurity CTF Competition, 2019 (Team “*College Chancellor Aspirant Shin Jinwoo*”)
- Research of the Year, Neung-In Scholarly Awards, 2018

## SKILLS

---

- Programming Languages: Python, C, C++, Java, JavaScript, PHP, Rust
- Technologies:
  - General: Git, LaTeX, Numpy
  - Data Analysis: Pandas, Matplotlib, R
  - Machine Learning: Scikit, TensorFlow, Keras, NLTK
  - Systems: Socket, Docker, CMGR
  - Web: HTML, Flask, Django, Jekyll, Hugo, React.js
  - Security: Pwntools, Elasticsearch, Cisco AMP
  - Database: MySQL, PostgreSQL, MongoDB
  - Cloud: Google Cloud, Microsoft Azure, Amazon AWS
- Language: English and Korean (Native), Japanese and Spanish (Basic)