Miuyin Yong Wong

Email: miuyinyong@gatech.edu Linkedin: https://www.linkedin.com/in/miuyin

SUMMARY

My research is at the intersection of usability and cybersecurity, focusing on designing user-centric solutions for security practitioners to help address real-world challenges that arise from analyzing malicious software. More specifically, I aim to empower professionals with solutions that integrate seamlessly with their workflows and enhance the usability and efficiency of reverse engineering and threat intelligence tasks. Additionally, I am interested in cybersecurity education, aiming to mitigate existing skill gaps and alleviate the initial steep learning curve challenge through the development of more effective tools. By studying the human aspect of cybersecurity, I seek to develop strategies to improve the design of security tools and their effective use, ultimately advancing cybersecurity defenses through a human-centric approach.

EDUCATION

Ph.D. in Computer Science (Cybersecurity), Georgia Institute of Technology Atlanta, Georgia
Advisor: Dr. Mustaque Ahamad Expected Dec 2024
Minor: Public Policy & International Affairs
Committee: Dr. Fabian Monrose, Dr. Frank Li, Dr. Douglas Blough

B.S. in Computer Science, Costa Rica Institute of Technology San Jose, Costa Rica
Award for Best Student from Central America and the Caribbean November 2016
Extraordinary Student Recognition from Costa Rica Institute of Technology's President

PUBLICATIONS

Yong Wong, M., Landen, M**.**, Li, F., Monrose, F., & Ahamad, M. "Comparing Malware Evasion Theory with Practice: Results from Interviews with Expert Analysts". In: Twentieth Symposium on Usable Privacy and Security (SOUPS 2024). *21% acceptance rate*

Yong Wong, M., Landen, M**.**, Antonakakis, M., Blough, D. M., Redmiles, E. M., & Ahamad, M. "An inside look into the practice of malware analysis". In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (pp. 3053-3069). *18% acceptance rate*

Valakuzhy, K., **Yong Wong, M**., Alrawi, O., Keromytis, A., Monrose, F. "Don't Miss Out on the Cross-Family Gossip: Using Shared Implementations of Behaviors to Uncover Relationships Within and Between Malware Families" (Under Review)

Fullwood, J., Palasamudram, P., Han, L., **Yong Wong, M**., Ahamad, M., Monrose, F. "What's In a Voice? Using Spectrogram-informed Augmentation to Improve Resiliency of Audio Deepfake Detectors Against Encoding Attacks" (Under Review)

Alrawi, O., Valakuzhy, K., **Yong Wong, M**., Adijbi, A., Avgetidis, A., Karakatsanis, K., Blough, D., Ahamad, M., Keromytis, A., Monrose, F., & Antonakakis, M. "SoK: An Essential Guide For Using Malware Sandboxes In Security Applications: Challenges, Pitfalls, and Lessons Learned" (Pre-print)

EXPERIENCE

Postdoctoral Researcher, **University of Maryland Cybersecurity Center**, MD Starting Jan 2024
Advisor: Dr. Michelle Mazurek

Graduate Researcher, **Georgia Institute of Technology,** Atlanta, GA Aug 2017- Present
Inside look into Malware Analysis in Practice

Collaborators: Dr. Mustaque Ahamad (advisor), Dr. Douglass Blough, Dr. Elissa Redmiles, Dr. Manos Antonakakis

- Designed and performed the first user study of real-world malware analysis, where I meticulously crafted a survey and interview questions through extensive research and pilot studies.
- Conducted comprehensive semi-structured interviews with professional malware analysts from 18 companies and employed qualitative coding to analyze interview data.
- Developed a taxonomy of malware analysts and an in-depth analysis of distinct workflows commonly followed by malware analysts in practice.

<u>Comparing Malware Evasion Theory with Practice</u>
Collaborators: Dr. Mustaque Ahamad (advisor), Dr. Fabian Monrose, Dr. Frank Li

- Performed the first systematic mapping of malware evasion countermeasures to comprehensively survey the landscape and identify knowledge gaps.
- Conducted a user study with malware experts from leading security companies to uncover challenges posed by evasive malware and understand how they handle such challenges. To ensure the reliability and validity of our findings, I followed best practices in qualitative methods (e.g., saturation and inter-coder consistency).
- Systematically compared challenging malware evasion techniques in practice with countermeasures published in the academic literature. This rigorous analysis facilitated the identification of key areas that warrant future research.

<u>Designing Human-Centric Evasive Malware Analysis Tool</u>
Collaborators: Dr. Mustaque Ahamad (advisor), Dr. Douglas Blough

- The objective is to design an innovative tool that could automate time-consuming and tedious tasks performed by analysts.
- Currently researching how to leverage findings from static and dynamic analysis methodologies to provide analysts insights into the evasion techniques employed by malware samples upon termination of execution within dynamic analysis systems, along with actionable next steps to extend the analysis.

<u>Assessing Trust and Safety Professionals' Readiness for 2024 Election Disinformation</u>
Collaborator: Dr. Michael Specter

- Supervising a group of graduate students in designing and conducting semi-structured interviews.
- The goal is to assess the preparedness of trust and safety professionals in addressing concerns related to disinformation ahead of the 2024 elections.

Static Malware Analysis Detection Intern, **Emerging Threats**, Remote May 2020 – Aug 2020

- Analyzed malware generated PCAPs to identify malicious network traffic.
- Generated and deployed Suricata and Snort malware detection signatures in the production environment.

Threat Researcher Intern, **Proofpoint**, Sunnyvale, CA May 2019 – Aug 2019
Advisors: Dr. Zachary Abzug

- Leveraged machine learning clustering techniques from scikit-learn library to identify and validate features utilized by malicious shortened URLs.
- Recommended feature sets are now integrated into production to proactively detect and prevent customers from clicking on tens of thousands of malicious URLs everyday.

Security Engineer Intern, **Proofpoint**, Sunnyvale, CA May 2018 – Aug 2018

- Developed a method to strategically prioritize higher-risk emails based on HTML metadata attributes.

Software Developer, **POSSIBLE**, Costa Rica Dec 2016 – Aug 2017

- Developed engaging front-end web applications for renowned companies including Starbucks, Acura, Rubbermaid, Baby Jogger, Graco, tailored to meet each company’s unique needs and objectives.

GUEST LECTURE

An Inside Look into the Practice of Malware Analysis	November 2021
Best Practices for Qualitative Research, NYU	May 2024
Best Practices for Qualitative Research, Georgia Tech School of Cybersecurity and Privacy	February 2024
Best Practices for Qualitative Research, Georgia Tech Advanced Computer Security Course	November 2023

REVIEWING

USENIX Security 2024	Sub-reviewer
ACM Conference on Computer-Supported Cooperative Work (CSCW) 2023, 2024	Reviewer
Annual Computer Security Application Conference (ACSAC) 2023	Sub-reviewer

TEACHING EXPERIENCE

Georgia Institute of Technology		
Spring 2020 & 2022	Secure Computer Systems	Teaching Assistant
Costa Rica Institute of Technology		
2015-2016	English I & II	Teaching Assistant

SKILLS

Programming: Python, Javascript, HTML, CSS, Java
Malware: x32 and x64 dbg, Cuckoo Sandbox, Snort, Suricata, IDA Pro, Ghidra
Language skills: Fluent in English, Spanish, and Mandarin Chinese.

Mentorship

Mentor, School of Cybersecurity and Privacy, **Georgia Institute of Technology** August 2023 - Present

- Served as a mentor to incoming PhD students by offering personalized guidance and support to navigate their research paths and foster their academic development.
  - Ph.D. students
    - 2023 - Present. Zeezoo Ryu
    - 2024 – Present. Pradyumna Shome
    - 2024 – Present. Anna Raymaker
  - Masters students
    - 2024 – Present. Delaney Gomen
    - 2024 – Present. Gayatri Patankar

Mentor, **Superposition** April 2021 - Present

- Led monthly mentoring sessions with one female high school student per year to guide and support their educational journey, intending to bridge the gender gap in STEM fields.
- Took the initiative to engage with high school students, actively sharing valuable insights into computer science and cybersecurity through recounting my educational journey and addressing their questions to cultivate their interest in STEM disciplines.

Founder, **Mujeres Informaticas Unidas** Sep 2016 – Aug 2017

- Founded a platform to support and encourage the participation of women in computer science.
- Collaborated with Costa Rican high schools to organize presentations aimed at educating high school girls and inspiring them to pursue a computer science degree.
- Discussed with students the opportunities available in the field of computer science, inspiring the next generation.