Yuanhaur Chang (Oliver)

+1-929-888-3495, c.yuanhaur@wustl.edu
https://changoliver.github.io/

RESEARCH INTERESTS

Cyber-physical Security, Medical Security, Usable Security & Privacy

EDUCATION

Washington University in St. Louis   Missouri, USA
Ph.D. in Computer Science   2021 - Present
Advisor: Dr. Ning Zhang

National Taiwan University   Taipei, Taiwan
Bachelor of Science in Computer Science and Information Engineering   2017 – 2021

HONORS/AWARDS

- Symposium on Usable Privacy and Security (SOUPS) Student Grant   2025
- WashU Dean's International Award   2021
- Taiwanese Ministry of Education (MOE) Fellowship   2021

PUBLICATIONS

Conference

1. Yara Alsiyat, <u>Yuanhaur Chang</u>, Ning Zhang, Ivan Flechais
   Smart Spaces, Private Lives: A Culturally Grounded Examination of Privacy Tensions in Smart Homes
   Symposium on Usable Privacy and Security (SOUPS), 2025

2. Zhiyuan Yu, <u>Yuanhaur Chang</u>, Shixuan Zhai, Nicholas Deily, Tao Ju, XiaoFeng Wang, Uday Jammalamadaka, Ning Zhang
   XCheck: Integrity Verification for 3D Printed Patient-Specific Devices via Computing Tomography
   USENIX Security Symposium, 2023
   Distinguished Artifact Award

3. Zhiyuan Yu, <u>Yuanhaur Chang</u>, Ning Zhang, Chaowei Xiao
   SMACK: Semantically Meaningful Adversarial Audio Attack
   USENIX Security Symposium, 2023

4. Zhiyuan Yu, Zhuohang Li, <u>Yuanhaur Chang</u>, Skylar Fong, Jian Liu, Ning Zhang
   HeatDeCam: Detecting Hidden Spy Cameras via Thermal Emissions
   ACM Conference on Computer and Communications Security (CCS), 2022

Workshop Papers

1. Sinyin Chang, Ao Li, Evin Jaff, <u>Yuanhaur Chang</u>, Jinwen Wang, Ning Zhang, Hsu-Chun Hsiao
   AdapSan: Adaptive Input Sanitization in Medical Systems with eBPF
   ACM Workshop on Adaptive and Autonomous Cyber Defense (AACD), 2024

2. Ao Li, Sinyin Chang, Guirui Li, <u>Yuanhaur Chang</u>, Nathan Fisher, Thidapat (Tam) Chantem
   Software and Behavior Diversification for Swarm Robotics Systems
   ACM Workshop on Moving Target Defense (MTD), 2023

arXiv Papers

1. <u>Yuanhaur Chang</u>, Oren Heller, Yaniv Shlomo, Iddo Bar-Noy, Ella Bokobza, Michal Grinstein-Weiss, Ning Zhang
   Mind the Gap: Revealing Security Barriers through Situational Awareness of Small and Medium Business Key Decision-Makers
   arXiv preprint arXiv:2506.10025, 2025

2. <u>Yuanhaur Chang</u>, Han Liu, Chenyang Lu, Ning Zhang
   SoK: Security and Privacy Risks of Healthcare AI
   arXiv preprint arXiv:2409.07415, 2025

CVE

1. **Slic3r**: CVE-2021-44961, CVE-2021-44962 (Base score 5.5)
2. **ZBar**: CVE-2023-40889, CVE-2023-40890 (Base score 9.8)

TEACHING

Teaching Assistant
- EE5184　Machine Leaning   Spring 2020
- CSE4303 Introduction to Computer Security   Fall 2025

STUDENT MENTORING

Master Student
- Jayden Li   Sep 2025 - Now
- Evin Jaff   Sep 2023 - Dec 2024
- Zishuai Liu   Sep 2023 - May 2024
- Matthew Kim   Jan 2023 - Dec 2023
- Jack Zhai   Sep 2022 - May 2023
- Yara Alsiyat   Jan 2022 - Dec 2022

Undergraduate
- Logan Zhang   Jul 2025 – Sep 2025
- Arjun Sekar   Jun 2025 – Aug 2025
- Elysia Quah   May 2023 - Dec 2023
- Louie Kolter (Valedictorian)   Sep 2022 - May 2023
- Annika Petrikin   Sep 2022 - May 2023
- Sherry Zhang   Sep 2022 - May 2023
- Trystan Ng   Sep 2022 - Dec 2022
- Young Lin   Jan 2022 - Aug 2022

SERVICE AND LEADERSHIP

Conference Organization
- Web Chair, 10th ACM Workshop on Moving Target Defense (MTD'23)
- US-Taiwan Workshop on Cybersecurity 2025

Technical Program Committee
- ACM Conference on Computer and Communications Security (CCS) AEC: 2025
- USENIX Security Symposium AEC: 2024, 2025
- Network and Distributed System Security Symposium (NDSS) AEC: 2026
- International Conference on Autonomous Agents and Multi-Agent Systems (AAMAS): 2025
- IEEE Conference on Communications and Network Security (CNS): 2025
- IEEE Transactions on Information Forensics & Security (TIFS): 2024, 2025

- IEEE Transactions on Cyber-Physical Systems (TCPS): 2025

External Reviewer
- IEEE Symposium on Security and Privacy (Oakland)
- ACM Conference on Computer and Communications Security (CCS)
- ACM ASIA Conference on Computer and Communications Security (ASIACCS)
- Annual Computer Security Applications Conference (ACSAC)
- IEEE International Conference on Computer Communications (INFOCOM)
- ISOC The Network and Distributed System Security Symposium (NDSS)
- IEEE European Symposium of Security and Privacy (EuroS&P)
- Design Automation Conference (DAC)
- IEEE Real-Time Systems Symposium (RTSS)

Student Group
- Vice President, Taiwanese Graduate Student Association (TGSA)   2022 - 2023
- Treasurer, Taiwanese Graduate Student Association (TGSA)   2023 - 2024

Volunteering
- Student Volunteer, Office of International Affair   2018 - 2019
- Student Volunteer, College of EECS   2018 - 2019