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

- WashU Dean's International Award — 2021
- Taiwanese Ministry of Education (MOE) Fellowship — 2021

PUBLICATIONS

Conference

1. Zhiyuan Yu, Yuanhaur Chang, 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

2. Zhiyuan Yu, Yuanhaur Chang, Ning Zhang, Chaowei Xiao
   SMACK: Semantically Meaningful Adversarial Audio Attack
   USENIX Security Symposium, 2023

3. Zhiyuan Yu, Zhuohang Li, Yuanhaur Chang, 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, Yuanhaur Chang, 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, Yuanhaur Chang, Nathan Fisher, Thidapat (Tam) Chantem
   Software and Behavior Diversification for Swarm Robotics Systems
   ACM Workshop on Moving Target Defense (MTD), 2023

arXiv Papers

1. Yuanhaur Chang, Han Liu, Evin Jaff, Chenyang Lu, Ning Zhang
   SoK: Security and Privacy Risks of Medical AI
   arXiv preprint arXiv:2409.07415, 2024

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

National Taiwan University

- TA for EE5184 Machine Leaning Spring 2020

SERVICE AND LEADERSHIP

Conference Organization

- Web Chair, 10th ACM Workshop on Moving Target Defense (MTD'23)

Technical Program Committee

- USENIX Security Symposium: 2024, 2025
- IEEE Transactions on Information Forensics & Security: 2024, 2025
- IEEE Transactions on Cyber-Physical Systems: 2025
- International Conference on Autonomous Agents and Multi-Agent Systems: 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)

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