# Haohuang Wen

https://onehouwong.github.io/ mailto:wen.423@osu.edu
https://github.com/onehouwong +1 (614)-256-0676

## Education

**South China University of Technology** **Guangzhou, China**
*B.Eng. in Software Engineering, Excellent Engineer Class* *Sep 2014 - July 2018*

**The Ohio State University** **Columbus, US**
*Ph.D. in Computer Science and Engineering* *Aug 2018 - May 2024*

## Research Interest

**Mobile** and **Cellular Network** (5G / Future G) Security; OpenRAN; **Program analysis** and Reverse engineering; **Automotive** and **IoT** Security

## Publications

**Highlight**: **SEVEN** (Co-)First-Authored papers in top-tier ("Big-Four") computer security venues (USENIX Security'20'23, CCS'20'24, NDSS'20'23'24)

- **[CCS'24]** Wenqiang Li*, **Haohuang Wen***, and Zhiqiang Lin." (* *indicates equal contribution*) BaseMirror: Automatic Reverse Engineering of Baseband Commands from Android's Radio Interface Layer ". In proceedings of the 31st ACM Conference on Computer and Communications Security (*Acceptance rate: TBD*).

- **[NDSS'24]** **Haohuang Wen**, Phillip Porras, Vinod Yegneswaran, Ashish Gehani, and Zhiqiang Lin."5G-Spector: An O-RAN Compliant Layer-3 Cellular Attack Detection Service". In the Network and Distributed System Security Symposium 2024 (*Acceptance rate: 140/694=20.2%*).
  ★ **Distinguished Artifact Award** (*2 out of 38 submitted artifacts among 140 papers*).

- **[NDSS'23]** **Haohuang Wen**, Phillip Porras, Vinod Yegneswaran, and Zhiqiang Lin. "Thwarting Smartphone SMS Attacks at the Radio Interface Layer". In the Network and Distributed System Security Symposium 2023 (*Acceptance rate: 94/581=16.2%*).

- **[USENIX Security'23]** **Haohuang Wen** and Zhiqiang Lin. "Egg Hunt in Tesla Infotainment: A First Look at Reverse Engineering of Qt Binaries". In proceedings of the 32nd USENIX Security Symposium (*Acceptance rate: 422/1444=29.2%*).

- **[EmergingWireless'22]** **Haohuang Wen**, Phillip Porras, Vinod Yegneswaran, and Zhiqiang Lin. "A Fine-Grained Telemetry Stream for Security Services in 5G Open Radio Access Networks". In the 1st Workshop on Emerging Topics in Wireless.

- **[RAID'22]** Jun Yeon Won, **Haohuang Wen**, and Zhiqiang Lin. "What You See is Not What You Get: Revealing Hidden Memory Mapping for Peripheral Modeling". In Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses (*Acceptance rate: 35/139=25.2%*).

- **[PETS'22]** Christopher Ellis, **Haohuang Wen**, Zhiqiang Lin, and Anish Arora. "Replay (Far) Away: Exploiting and Fixing Google/Apple Exposure Notification Contact Tracing". In Proceedings of the 29th Privacy Enhancing Technologies Symposium (*Acceptance rate: 128/534=24.0%*).

- **[CCS'20]** **Haohuang Wen**, Zhiqiang Lin, and Yinqian Zhang. "FirmXRay: Detecting Bluetooth Link Layer Vulnerabilities from Bare-Metal Firmware". In Proceedings of the 27th ACM Conference on Computer and Communications Security (*Acceptance rate: 121/715=16.9%*).
- **[SecureComm'20]** **Haohuang Wen**, Qingchuan Zhao, Zhiqiang Lin, Dong Xuan, and Ness Shroff. "A Study of the Privacy of COVID-19 Contact Tracing Apps". In Proceedings of the International Conference on Security and Privacy in Communication Networks.
- **[SecureComm'20]** Qingchuan Zhao, **Haohuang Wen**, Zhiqiang Lin, Dong Xuan, and Ness Shroff. "On the Accuracy of Measured Proximity of Bluetooth-based Contact Tracing Apps". In Proceedings of the International Conference on Security and Privacy in Communication Networks.
- **[NDSS'20]** **Haohuang Wen**, Qingchuan Zhao, Qi Alfred Chen and Zhiqiang Lin. "Automated Cross-Platform Reverse Engineering of CAN Bus Commands from Mobile Apps". In Proceedings of the Network and Distributed System Security Symposium (*Acceptance rate: 88/506=17.4%*).
- **[USENIX Security'20]** **Haohuang Wen**, Qi Alfred Chen, and Zhiqiang Lin. "Plug-N-Pwned: Comprehensive Vulnerability Analysis of OBD-II Dongles as A New Over-the-Air Attack Surface in Automotive IoT". In Proceedings of the 29th USENIX Security Symposium (*Acceptance rate: 157/977=16.1%*).
- **[CCS'19]** Chaoshun Zuo, **Haohuang Wen**, Zhiqiang Lin and Yinqian Zhang. "Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps". In Proceedings of the 26th ACM Conference on Computer and Communications Security (*Acceptance rate: 149/934=16.0%*).
- **[APSEC'18]** **Haohuang Wen**, Juanru Li, Yuanyuan Zhang, and Dawu Gu. "An Empirical Study of SDK Credential Misuse in iOS Apps". In Proceedings of 25th Asia-Pacific Software Engineering Conference.
- **[IEEE Access]** **Haohuang Wen**, Lei Yang, and Zhenyu Wang. "ParGen: A Parallel Method for Partitioning Data Stream Applications in Mobile Edge Computing". In IEEE Access 2017.

## Work Experience

**SRI International** — **Remote**
*Security Research Intern* — *May 2023 - Aug 2023*

**The Ohio State University** — **Columbus, US**
*Graduate Teaching Assistant (CSE 5474 - Software Security)* — *Jan 2023 - May 2023*

**SRI International** — **Remote**
*Security Research Intern* — *May 2022 - Aug 2022*

**SRI International** — **Remote**
*Security Research Intern* — *May 2021 - July 2021*

**The Ohio State University** — **Columbus, US**
*Graduate Research Assistant* — *Aug 2018 - Present*

**Shanghai Jiao Tong University** — **Shanghai, China**
*Security Research Intern* — *Mar 2018 - May 2018*

**Tencent Technology Co., Ltd** — **Guangzhou, China**
*Android Developer Intern* — *July 2017 - Sep 2017*

## Professional Service

**Conference Program Committee / Reviewer**:
- The ACM Web Conference: 2024
- EAI International Conference on Security and Privacy in Communication Networks (SecureComm): 2023
- Annual Computer Security Applications Conference (ACSAC) Artifact Evaluation Committee: 2019

**Journal Reviewer**:
- IEEE Transactions on Intelligent Transportation Systems: 2024
- IEEE Transactions on Mobile Computing (TMC): 2024
- IEEE Internet of Things Journal (IoT-J): 2023
- IEEE Communications Magazine: 2023
- IEEE Security & Privacy Journal: 2022

**External Reviewer**: CCS (22, 20), IEEE S&P (24, 22, 21), USENIX Security (22, 21), NDSS (20, 19), ACSAC (22, 20, 19), DSN (22, 21, 20), ESORICS (22), SecureComm (19), DFRWS (20, 19), AutoSec (21)

## Selected Media Coverage

- NSF invests $25M to advance technologies and communications to operate securely through 5G networks. 09/21/2023.
- 5G Security-Enhanced Open Radio Access Networks - Nephio. 05/03/2023.
- NSF, DOD partner to advance 5G technologies and communications for U.S. military, government and critical infrastructure operators. 09/07/2022
- Google/Apple's contact-tracing apps susceptible to digital attacks. 08/08/2022.
- Hackers could target COVID-19 contact tracing apps on your phone: Ohio State researchers. 07/21/2022.
- HES application is one year old. Do you think he was born happy? 04/18/2021.
- The Risks Posed by Wireless Automotive Dongles. 08/12/2020.
- Hacking Bluetooth. 02/27/2020.
- Fundamental Design Flaw Leaves Bluetooth Devices Vulnerable to Hacking. 11/15/2019

## Selected Awards and Honors

- NDSS'24 Distinguished Artifact Award (2024)
- OSU Presidential Fellowship (2023)
- Departmental Graduate Research Award (2023)
- NDSS student travel grant (2020)
- CCS student travel grant (2019)
- First Class Scholarship (Top 1%), South China University of Technology (2015)

## Expertise and Skills

**Programming Languages :** Python, Java, C++, C

**Skill Set:** Mobile App Development and Reverse Engineering (iOS & Android), Binary analysis (x86 & ARM), Software-defined radio programming (USRP, BladeRF series)

**Tools/Framework:** Ghidra, Frida, IDA Pro, GDB, Jeb, Soot, Wireshark, Charles, QEMU, Docker, Ku-

bernetes, AOSP, OpenAirInterface, srsRAN, SD-RAN