Hanqing Guo

Contact Information

Computer Science and Engineering
Michigan State University
East Lansing, MI 48824 USA

Phone: (765) 760-7245
Email: guohanqi@msu.edu
Website: https://hanqingguo.github.io/

Research Interests

My research interest is **Cybersecurity**, and related research areas fall on the intersection of **Mobile Systems**, **Trustworthy AI**, and **Wireless Communications**. As a cybersecurity researcher, I discover the vulnerabilities of existing mobile systems, design the countermeasures of advanced attacks targeted AI models and systems, and explore the potential innovations to boost the usability of real-world applications. My highlight research primarily focuses on:

1) **Enable the Secured AI System:** Discover the fault of AI-enabled speech recognition and speaker identification systems [Mobicom'23, RAID'23, CCS'22, NDSS'22, NDSS'20], and propose countermeasure solutions to secure the open-source AI models and the commercial systems [AsiaCCS'22, Mobicom'23, ICLR'23, Under Review by S&P'24].

2) **Enable the Privacy-Preserving System:** Explore the intelligent solutions to protect the privacy leakage, defend against eavesdropping attacks [DSN'22], and deepfake-speech telecommunication fraud [Wisec'23].

3) **Boost the Wireless Communication System:** Innovate the AI solutions on wireless communication scenarios, to boost the LoRa signal communication distance [SenSys'21], and to facilitate underwater navigation system [Mobicom'22].

In addition, my research innovation has been applied to other studies, including speech dataset watermarking [Under Review by S&P'24], large-language model security [RAID'23, Under Review by USENIX Security'24], IoT security [ICDE'23, Major Revision by VLDB'24], Wireless Sensing and communication [GLOBECOM'19, ICME'19, ICC'19].

Education

Michigan State University, East Lansing, Michigan USA

Ph.D. Candidate, Computer Science (expected graduation date: May 2024)

- Dissertation: "Toward Private, Secure, and Robust AI-Enabled Voice Services"
- Adviser: Dr. Li Xiao and Dr. Qiben Yan

Ball State University, Muncie, Indiana USA

MS, Computer Science, May, 2019

- Thesis: "Real-time Human Activity Recognition Based on Radar"
- Adviser: Dr. Shaoen Wu

Chongqing University of Posts of Telecommunications, Chongqing, China

BS, Telecommunications engineering, May, 2015

Honors and Awards

Best Paper Honorable Mention, ACM CCS	**2022**
Best Paper Award, ACM SenSys	**2021**
Best Paper Award, IEEE Globecom	**2019**

Student Grants

Student Travel Grant, ACM CCS	**$1100, 2022**
Student Travel Grant, IEEE DSN	**$800, 2022**

Research Experience

Michigan State University, Department of Computer Science, East Lansing, MI USA

Research Assistant **Aug, 2019 - Present**

Research on cybersecurity in real-world AI systems. Research on wireless sensing and mobile communications.

Amazon, Account Integrity Team, San Diego, CA USA

Applied Scientist Intern **Jun, 2023 - August, 2023**

Research on "Customer Profiling on Impersonation Scams". Details are confidential due to the company policy.

Samsung Research America, Knox AI/Mobile/Privacy Group. Mountain View, CA USA

Research Intern **May, 2022 - Dec, 2022**

Research on "Discover the Vulnerabilities of Voice ID systems", and "Adopting Diffusion Model for Speech Command Purification". Details are confidential due to the company policy.

Ball State University, Muncie, IN USA

Research Assistant **Jan, 2017 - Aug, 2019**

Research on wireless communication and signal processing.

Selected Publication

I have published 31 research/poster papers (10 first-author papers) in high-impact venues for cybersecurity (e.g., CCS, NDSS, AsiaCCS, RAID), mobile systems (Mobicom, SenSys), and wireless communications (GLOBECOM, ICC, ICME). These papers have obtained more than 400 citations, and has been reported by media such as ACM TechNews, New Scientist, BBC Radio, Forbes, Science Daily, etc,

1. **Hanqing Guo**, Xun Chen, Junfeng Guo, Li Xiao, Qiben Yan
   "MASTERKEY: Practical Backdoor Attack Against Speaker Verification Systems".
   The 29th Annual International Conference On Mobile Computing And Networking (ACM MobiCom), 2023
   [Project Webpage]
2. **Hanqing Guo**, Guangjing Wang, Yuanda Wang, Bocheng Chen, Yuanda Wang, Qiben Yan, Li Xiao
   "PhantomSound: Black-Box, Query-Efficient Audio Adversarial Attack via Split-Second Phoneme Injection"
   The 26th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2023
3. Guangjing Wang, **Hanqing Guo**, Anran Li, Xiaorui Liu, Qiben Yan
   "Federated IoT Interaction Vulnerability Analysis"
   The 39th IEEE International Conference on Data Engineering (IEEE ICDE), 2023
4. Yuanda Wang, **Hanqing Guo**, Guangjing Wang, Bocheng Chen, Qiben Yan
   "VSMask: Defending Against Voice Synthesis Attack via Real-Time Predictive Perturbation"
   The 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec), 2023
5. Bocheng Chen, Guangjing Wang, **Hanqing Guo**, Yuanda Wang, Qiben Yan
   "Understanding Multi-Turn Toxic Behaviors in Open-Domain Chatbots"
   The 26th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2023
6. Junfeng Guo, Yiming Li, Xun Chen, **Hanqing Guo**, Lichao Sun, Cong Liu
   "SCALE-UP: An Efficient Blackbox Input-level Backdoor Detection via Analyzing Scaled Prediction Consistency"
   The 11th International Conference on Learning Representations (ICLR), 2023
   [Project Code]

7. **Hanqing Guo**, Yuanda Wang, Nikolay Ivanov, Li Xiao, Qiben Yan
"SpecPatch: Human-In-The-Loop Adversarial Audio Spectrogram Patch Attack on Speech Recognition"
The 29th ACM Conference on Computer and Communications Security (ACM CCS), 2022
[Project Webpage] Best Paper Honorable Mention.

8. **Hanqing Guo***, Chenning Li*, Lingkun Li, Zhichao Cao, Qiben Yan, Li Xiao
"NEC: Speaker Selective Cancellation via Neural Enhanced Ultrasound Shadowing" [1]
The 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (IEEE DSN), 2022
[Project Webpage], Media coverage: New Scientist and ACM TechNews

9. **Hanqing Guo**, Qiben Yan, Nikolay Ivanov, Ying Zhu, Li Xiao, Eric J. Hunter
"SuperVoice: Text-Independent Speaker Verification Using Ultrasound Energy in Human Speech"
The 17th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS), 2022
[Project Webpage]

10. Xiao Zhang, **Hanqing Guo**, James M Mariani, Li Xiao
"U-star: An underwater navigation system based on passive 3d optical identification tags"
The 28th Annual International Conference On Mobile Computing And Networking (ACM Mobicom), 2022

11. Yuanda Wang, **Hanqing Guo**, Qiben Yan
"GhostTalk: Interactive Attack on Smartphone Voice System Through Power Line"
Network and Distributed System Security (NDSS), 2022

12. Chenning Li, **Hanqing Guo**, Shuai Tong, Xiao Zeng, Zhichao Cao, Mi Zhang, Qiben Yan, Li Xiao, Jiliang Wang, Yunhao Liu
"NELoRa: Towards Ultra-low SNR LoRa Communication with Neural-enhanced Demodulation"
The 19th ACM Conference on Embedded Networked Sensor Systems (SenSys), 2021
Best Paper Award [Project Code]

13. Nikolay Ivanov, **Hanqing Guo**, Qiben Yan
"Rectifying administrated ERC20 tokens"
Information and Communications Security: 23rd International Conference (ICICS), 2021

14. Qiben Yan, Kehai Liu, Qin Zhou, **Hanqing Guo**, Ning Zhang
"Surfingattack: Interactive hidden attack on voice assistants using ultrasonic guided waves"
Network and Distributed System Security (NDSS), 2020
[Project Webpage]

15. **Hanqing Guo**, Nan Zhang, Shaoen Wu, Qing Yang
"Deep Learning Driven Wireless Real-time Human Activity Recognition"
The IEEE International Conference on Communications (IEEE ICC), 2020

16. Shaoen Wu, **Hanqing Guo**, Junhong Xu, Shangyue Zhu, Honggang Wang
"In-band full duplex wireless communications and networking for IoT devices: Progress, challenges and opportunities"
Future Generation Computer Systems, 2019

17. Junhong Xu, Shangyue Zhu, **Hanqing Guo**, Shaoen Wu
"Automated labeling for robotic autonomous navigation through multi-sensory semi-supervised learning on big data"
IEEE Transactions on Big Data, 2019

[1] * denotes authors contributed equally

18. **Hanqing Guo**, Nan Zhang, Wenjun Shi, S. AIQarni, Shaoen Wu
"HICFR: Real Time 3D Indoor Human Image Capturing Based on FMCW Radar"
The IEEE International Conference on Multimedia and Expo (IEEE ICME), 2019
19. **Hanqing Guo**, Shaoen Wu, Honggang Wang, Mahmoud Daneshmand
"DSIC: Deep learning based self-interference cancellation for in-band full duplex wireless"
The IEEE Global Communications Conference (IEEE GLOBECOM), 2019
Best Paper Award
20. Qiwei Liu, **Hanqing Guo**, Junhong Xu, Honggang Wang, Aron Kageza, Saeed AlQarni, Shaoen Wu
"Non-contact non-invasive heart and respiration rates monitoring with MIMO radar sensing"
The IEEE Global Communications Conference (IEEE GLOBECOM), 2018
21. Juhong Xu, **Hanqing Guo**, Shaoen Wu
"Indoor multi-sensory self-supervised autonomous mobile robotic navigation"
IEEE international conference on industrial internet (ICII), 2018
22. **Hanqing Guo**, Junhong Xu, Shangyue Zhu, Shaoen Wu
"Realtime software defined self-interference cancellation based on machine learning for in-band full duplex wireless communications"
International Conference on Computing, Networking and Communications (ICNC), 2018
23. Shangyue Zhu, Junhong Xu,**Hanqing Guo**, Qiwei Liu, Shaoen Wu, Honggang Wang
"Indoor human activity recognition based on ambient radar with signal processing and machine learning"
IEEE international conference on communications (IEEE ICC), 2018

Grants Experience

I assisted in the preparation of proposals for the following research grants:

NSF: Computer and Network Systems (CNS), Request Budget: $600,000, 2023/10/01-2026/09/30 (Session: SaTC; Award Number: 2310207; Project Title: Robust Speaker and Speech Recognition Under AI-Driven Physical and Digital Attacks.)

NSF: Resilient & Intelligent NextG Systems (RINGS), (Project Title: Learning Resilient Beamforming Control with Spatiotemporal Modeling.)

NSF: Electrical, Communications and Cyber Systems (ECCS), Request Budget: $250,000, 2019/01/01-2020/12/31 (Session: SpecEES; Award Number: 1923712; Project Title: Collaborative Research: Enabling Secure, Energy-Efficient, and Smart In-Band Full Duplex Wireless.)

Teaching Experience

Michigan State University, Department of Computer Science and Engineering, East Lansing, MI USA

Teaching Assistant **Aug, 2019 - Present**

- CSE 260 — Discrete Structures in Computer Science: Spring 2022
- CSE 410 — Operating System: Fall 2021
- CSE 232 — Introduction to Programming II: Fall 2019

Professional Activities

PC member of the *IEEE DSN Doctoral Forum* **2023**

Journal Reviewer of

- *Transactions on Information Forensics & Security (TIFS)* **2022-2023**
- *Transactions on Dependable and Secure Computing (TDSC)* **2022-2023**
- *Transactions on Sensor Networks (TOSN)* **2021-2022**

Conference Reviewer of

- *IEEE INFOCOM 2020, 2021, 2022, 2023, 2024*
- *IEEE ICDCS 2021, 2022*
- *IEEE DSN 2023*
- *IEEE ICC 2021, 2022*

Talks

Michigan State University **Oct. 2023**
Graduate Seminar
" Backdoor Attack Against Speaker Verification Systems"

Southeast University **Dec. 2022**
Cybersecurity Seminar
" Toward private, secure, and robust voice services"

ACM CCS 2022 **Nov. 2022**
Conference Presentation
"SpecPatch: Human-In-The-Loop Adversarial Audio Spectrogram Patch Attack on Speech Recognition"

IEEE DSN 2022 **July. 2022**
Conference Presentation
"NEC: Speaker Selective Cancellation via Neural Enhanced Ultrasound Shadowing"

ACM AsiaCCS 2022 **May. 2022**
Conference Presentation
"SuperVoice: Text-Independent Speaker Verification Using Ultrasound Energy in Human Speech"

Michigan State University **March 2022**
Graduate Seminar
" SuperVoice: Speaker Verification Using Ultrasound"

Development Experience

Smart Voice Recording Jammer
- Design a smart conversation jammer with an ultrasound speaker and AI models. (Conference publication 4)
- **Matlab, Python, Ultrasound speaker, Raspberry Pi**

Speaker Verification System
- Collect a Speech dataset containing 7700 audio samples and 641 minutes of speech. Leverage the ultrasound component of human speech to design an end-to-end speaker verification system (Conference publication 5).
- **Matlab, NI DAQ, Pytorch, Android**

Fraud Detection Application
- Develop programs to assist the company in identifying vulnerable customers so that the customers can be protected in advance. Details are confidential due to the company policy.
- **Python, AWS EC2, AWS Sandbox**

Children Sleep Activity Monitoring Application
- Design application to monitor the children's sleep quality and activities with IP camera and AI models.
- **Tensorflow, OpenCV, Hadoop, Java**

(TA project) Operating System Class Project Design
- Design projects for Operating system class, including Multi-process/thread, memory allocation, deadlock detection, and file systems.
- **C++, Unix**