Huizhen Zhou
https://re1own.github.io/about/
Email : hzhou9@gmu.edu
Mobile : +1-571-332-9683

Education

- **George Mason University** — Fairfax, VA, USA
  Doctor of philosophy in Computer Science — *September. 2025 –*
- **George Mason University** — Fairfax, VA, USA
  Master of Science in Computer Science; GPA: 3.83 — *January. 2024 – May. 2025*
- **Heilongjiang Institute of Technology** — Hardbin, China
  Bachelor of Engineering in Computer Science and Technology; GPA: 3.75(1/154 in Junior Year)Aug. 2018 – July. 2022

Experience

- **George Mason University** — Fairfax, VA
  Part-time Research Assistant — *Aug 2024 - Present*
  - **Side Channel Attack on Cryptocurrency Hardware Wallet**: Doing Power side channel attack on Trezor hardware wallet (Advisor: Dr. Xiaokuan Zhang)

  Research Project
  - **Side Channel Attack on Hardware implementation of BIKE**: Doing power side channel attack key recovery on BIKE hardware implementation and published a paper (Advisor: Prof. Kris Gaj)
- **Institute of Sotfware, Chinese Academy of Sciences** — Beijing, China
  Full-time Research Assistant — *Oct 2021 - March 2022*
  - **CVE reproduction**: Responsible for reproducing the Dahua camera CVE-2021-33044 vulnerability and analyzing the cause of the vulnerability; learned to simulate the startup of IoT firmware.
  - **CVE reproduction**: MikroTik RouterOS-CVE-2019-13954 Vulnerability Replication, written in an article:https://www.anquanke.com/post/id/254635
  - **Trojan horse reverse analysis**: Analyzed the Trojan Attack Patterns in the infected devices in emergency response; successfully deciphered the encrypted string in the sample through reverse technology and located the hidden ip of the attacker.
  - **Fuzzing**: Fuzz testing of components within the OpenEuler system was conducted, employing AFL (American Fuzzy Lop) and libFuzzer for this purpose. A comprehensive study of AFL's source code was undertaken to deepen the understanding and enhance the effectiveness of the fuzzing strategies implemented.
  - **Competition**: Took charge of the code writing to detect dangerous functions in IoT firmware and post-game problem solving in the Chinese DataCon2021 Internet of Things Security Competition.
- **Cybersecurity Society of Heilongjiang Institute of Technology** — Harbin, China
  Leader of the Society — *2020.09-2022.01*
  - **CTF competition**: Formed teams in the school laboratory to participate in many information security competitions.
  - **Teaching**: Gave lectures to members and shared cybersecurity knowledge and experience with members.Responsible for organizing CTF training in the summer and winter vacations; created good cybersecurity learning atmosphere for the members
- **Huawei Hardware Security Summer Camp** — Dongguan, China
  Learning — *Summer 2020*
  - **Learning**: Conducted the HWS hardware security learning and participated in the offline competition 2020.08. Participated in the 7-day offline training at Huawei Songshan Lake European Town and enhanced the knowledge of kernel security, firmware security and hardware security .

Publication

- Luke Beckwith, **Huizhen Zhou**, Jens-Peter Kaps, Kris Gaj. "Power Side-Channel Key Recovery Attack on a Hardware Implementation of BIKE." in 2024 Asian Hardware Oriented Security and Trust Symposium

HONORS & AWARDS

- Ranked 17th in China's DataCon 2021 Internet of Things Security Competition (10/2021).
- Discovered the unauthorized access vulnerability of wechat small program "Security Management Platform of Heilongjiang Institute of Technology", submitted the vulnerability and obtained the vulnerability number CNVD-68007. (08/2021)
- 1st Prize of 8th Programming Competition of Harbin University of Science and Technology in 2018 (12/2018).
- 1st Prize of 2018 Heilongjiang Institute of Engineering Program Design Competition (12/2018).

Programming Skills

- **Languages**: C, C++, Assembly-x86, Java, VHDL **Technologies**: Reverse Engineering, PWN(CTF), Side Channel Attack, Firmware Reverse Analysis, Operating System Kernel, FPGA Design, Algorithm, Data Structure, Post-Quantum Cryptography, Quantum Algorithm