Xupu Hu

Gender: Male | **Age**: 24 | **Phone**: +86 18638668035 | **Email**: huxupu@njust.edu.cn | : Homgpage

Education

- **Nanjing University of Science and Technology (NJUST) [🌐]** *Sept. 2023 - Apr. 2026*
  *Master of Science in Cybersecurity, advised by **Dr. Ming Zhou** and **Prof. Peng Zhang**. GPA: 87.38 / 100*
- **Zhengzhou University (ZZU) [🌐]** *Sept. 2019 - Jun. 2023*
  Bachelor of Engineering in Internet of Things (IoT) Engineering. GPA: 3.25 / 4.0 CET - 6

Publications

C = Conference

[C.1] Ming Zhou, **Xupu Hu**, Zhihao Wang, Haining Wang, Hui Wen, Limin Sun, Peng Zhang∗. ***Dynamic Vulnerability Patching for Heterogeneous Embedded Systems Using Stack Frame Reconstruction***. In the 32nd ACM Conference on Computer and Communications Security (**CCS 2025**). Accepted (**CCF-A, student first author**).

- Analyzed stack frame structures of common embedded MCU architectures; developed stack frame reconstruction for hot patches; extended patch functions to support global variable and macro definition modifications.
- Achieved control flow redirection via exception mechanisms for heterogeneous embedded systems; selected hot patch triggering strategies based on program storage location.
- Applied to medical devices, soft PLCs, network services; fixed 102 vulnerabilities across four embedded devices and three MCU architectures.

[C.2] **Xupu Hu**, Zhongfeng Jin, Tongjie Wei, Peng Zhang, Chonghua Wang, Ming Zhou*. ***BluePLP: Dynamic Vulnerability Patching for Heterogeneous BLE Devices***. International conference on Artificial Intelligence of Things and Systems (**AIoTSys 2025**). Accepted (AR: 38.9%, 37 out of 95; **Best paper finalists**, 8 out of 37).

- Leverage hardware breakpoints to support heterogeneous BLE devices, including those based on Cortex-M3, Cortex-M4 and Xtensa LX7 architectures.
- Use embedded exception handlers to redirect execution flow from vulnerable code to RAM-resident patches, enabling real-time updates without requiring system reboot.
- Mitigate 25 packet-based vulnerabilities across multiple real-time operating systems and BLE protocol stacks.

[C.3] Ming Zhou∗, Yunjun Ma, **Xupu Hu**, Ran Lin, Qiwen Wang, Weixuan Mao, Chengxiang Si. ***Characterizing Network Threats Against Industrial Control Systems Using Honeypot Technology***. International Conference on Networking and Network Applications (NaNA 2025). Accepted (student second author).

- Amulti-layer ICS honeypot framework that emulates protocol state machines, controller identities, and business workflows.
- A clean-room state-machine-based controller emulator supporting three network-level PLC honeypots.
- A tailored threat-analysis capable of identifying malicious IP addresses, exploiting tools, and threat organizations.
- A global deployment of 51 edge honeypots captured millions of intrusion attempts and suspicious sessions.

∗: *Corresponding Author.*

Research Projects

Partial List

- **Research on Key Technologies for Dynamic Vulnerability Repair of Online PLC Firmware.** *Jan. 2025 - Dec. 2027*
  - National Natural Science Foundation of China (NSFC, 62402225). Participation
- **Security Large Language Model (LLM).** *Dec. 2024 - Dec. 2025*
  - National Project of XXX. Participation
- **Intrusion Deception and Vulnerability Validation Period.** *Jan. 2025 - Dec. 2025*
  - National Information Security Special Project of XXX. Participation

Engineering Technology

Partial List

- **Embedded System Development.** *Sept. 2019 - Now*
  ◦ Tech Stack: C/CPP + Python + Firmware + RTOS + Linux
- **Reverse Engineering.** *Sept. 2023 - Now*
  ◦ Tech Stack: Ida pro + Bindiff + Ghirda + LLVM + Angr + QEMU + Binwalk...
- **Frontend Web Development.** *Jun. 2023 - Apr. 2024*
  ◦ Tech Stack: Vite + Vue 3 + Vue Router + Pinia + TypeScript (ts) + Element Plus

Other infomation

- **Research Interests :** I specialize in systems and firmware security. During my master's studies, my research focus was on live patching technologies for embedded systems. Additionally, my research interests also include using Large Language Models (LLMs) to solve challenges in the traditional program analysis field and building efficient and intelligent binary program analysis tools. I am building a secure and reliable automated live patching system.
- **Competition Awards :** First Prize in Zhengzhou University Programming Contest, etc.
- **School Honours :** Master's Academic Scholarship, etc.