呼栩朴

性别: 男　年龄: 24　18638668035　huxupu@njust.edu.cn　HomePage

教育经历

南京理工大学 (211)　**硕士**　**网络空间安全**　2023.09 – 2026.04
GPA：87.38 / 100 (前5%)　导师：周明老师、张鹏教授　江苏无锡

郑州大学 (211)　**本科**　**物联网工程**　2019.09 – 2023.06
GPA：3.25 / 4.0 (前25%)　外语水平：CET-6　河南郑州

学术成果

C = 会议论文

[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**). 已接收 (**CCF-A，第一作者导师**)

- 分析了常见嵌入式 MCU 架构的栈帧结构，使用栈帧重建机制以生成热补丁，并扩展补丁功能以支持全局变量和宏定义的修改。
- 通过嵌入式设备内置的异常处理机制实现控制流重定向，以适配异构嵌入式系统，并可以根据程序存储位置选择合适的热补丁触发策略。
- 应用于医疗设备、软 PLC 和网络服务三个真实场景，在 4 个嵌入式设备和 3 种 MCU 架构上成功修复了 102 个漏洞，热修复引入的开销仅在 260 个 MCU 时钟周期内。

[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**). 已接收 (**AR**: 38.9%, 37 / 95; **Best paper finalist**, 8 / 37)

- 利用硬件断点支持异构 BLE 设备，包括基于 Cortex-M3、Cortex-M4 和 Xtensa LX7 架构的设备。
- 利用异常处理程序将执行流从Flash中的漏洞代码重定向到 RAM 中的补丁，实现无需系统重启的实时更新。
- 在多个实时操作系统和 BLE 协议栈上修复了 25 个基于数据包的漏洞。

[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). 已接收 (第一作者导师)

- 设计了一种多层 ICS 蜜罐框架，可模拟协议状态机、控制器标识和业务流程。
- 设计了一个基于洁净室状态机的控制器模拟器，支持三种网络级 PLC 蜜罐。
- 开发了定制化威胁分析功能，能够识别恶意 IP 地址、攻击工具和威胁组织。
- 在全球部署了的 51 个边缘蜜罐，捕获了数百万次入侵尝试和可疑会话。

科研项目

国家自然科学基金 (62402225)：在线PLC固件漏洞动态修复关键技术研究。参与　2025.01 – 2027.12
国家XXX信息安全专项：入侵诱捕与漏洞验证。参与　2025.01 – 2025.12
XXX国家项目：安全大模型。参与　2024.12 – 2025.12

工程技能

嵌入式系统开发　技术栈：C/CPP + Python + Firmware + RTOS + Linux + 传感器　2019.09 – 至　今
- 熟悉嵌入式系统底层原理，能够用汇编语言手敲RTOS。独立开发了多个嵌入式系统，如智能家居系统等。

逆向工程　技术栈：Ida pro + Bindiff + Ghirda + LLVM + Angr + QEMU + Binwalk...　2023.09 – 至　今
- 熟悉逆向工程常用技术，熟悉常见架构汇编语言，担任学院逆向实训课程助教。

前端开发　技术栈：Vite + Vue 3 + Vue Router + Pinia + TypeScript (ts) + Element Plus　2023.07 – 2024.04
- 负责实验室所有前端开发项目，如数据同步运维等。

其他

- 研究兴趣：我专注于嵌入式系统与固件安全领域。硕士期间，我的研究方向为嵌入式系统的动态漏洞修复技术。此外，我的研究兴趣还包括使用大语言模型 (LLM) 解决传统程序分析领域的难题和构建高效智能的二进制程序分析工具。我正在构建安全可靠的自动化动态修复系统。
- 竞赛奖项：郑州大学程序设计竞赛一等奖等　　校园荣誉：硕士学业奖学金等