Peng Liu

2024/5/20

Basic Information

littlenewton6@gmail.com
https://github.com/LittleNewton/
https://littlenewton.uk/
https://www.youtube.com/@littlenewton6/
https://space.bilibili.com/45879248/
Academy 2 of UCAS, Jingjia Road W, Huairou, Beijing, China, 101408
School of Computer Science, University of Birmingham, Edgbaston, Birmingham, B15 2TT, UK

Education

University of Birmingham (#=84 in QS WUR)

Beijing, China
May. 2024 - Present

PG *VRS* Computer Science, School of Computer Science

(1) Visiting research student with funding from Chinese Scholarship Council (CSC).
(2) Focus of security analysis of MCU-based IoT system's firmware.

University of Chinese Academy of Sciences (#=62 in QS WUR)

Beijing, China
Aug. 2022 – Apr. 2024

D.Eng. IN *Information Security*, School of Computer Science and Technology

(1) Joint Master-Doctoral Program begins in 2019, and the doctoral training phase begins in August 2022, with my Doctoral Dissertation Proposal completed in the same year.
(2) Received Second-Class Academic Scholarship in December 2022.

University of Chinese Academy of Sciences (#=62 in QS WUR)

Beijing, China
Aug. 2019 – Jul. 2022

M.Eng. IN *Information Security*, School of Computer Science and Technology

(1) Joint Master-Doctoral Program begins in 2019, and the Master training phase begins in August 2019.
(2) Received Second-Class Academic Scholarship in 2019, 2020, 2021.

Yunnan University (China 211 Project)

Kunming, China
Sept. 2015 – Jun. 2019

B.Sc. IN *Information and Computing Science*, School of Mathematics and Statistics

(1) Major in Information and Computational Science.
(2) Received academic scholarships from the school in 2016, 2017, 2018.
(3) Received the title of Outstanding Graduate.
(4) Awarded Third Prize in the National University Mathematics Cipher Challenge, China, 2018
(5) Passed the College English Test Level 6 (CET-6) with a total score of 505.

Research Publications

Journal Articles

[1] Hao Zhang, Shandian Shen, **Peng Liu**, Zelin Yang, Wei Zhou, Yuqing Zhang. (2023). **Review of Firmware Emulators in Embedded Devices**. Journal of Computer Research and Development. (EI Index, doi: 10.7544/issn1000-1239.202330476)

[2] Yue Lin, **Peng Liu**, He Wang, Wenjie Wang, Yuqing Zhang. (2020). **Overview of Threat Intelligence Sharing and Exchange in Cybersecurity**. Journal of Computer Research and Development. (EI Index, doi: 10.7544/issn1000-1239.2020.20200616)

Conference Articles

[1] A paper “Evaluating Emulation Techniques for Multi-Interrupt Testing in Firmware: A Focus on Priority Inversion and Resource Contention Anomalies”. (Status, Draft since May. 2023)

Skills

Operating Systems and System Tools

- Linux System Administration: In-depth experience with Linux system management and optimization.
- systemd Management: Proficient in using systemd for service management and system configuration.
- containerd and Kubernetes: Familiar with the use and management of the containerd runtime and K8S cluster.
- Network: Proficient in using network tools such as iproute2 for network configuration and management.
- CLI Tools: Proficient in using command line tools like tmux, zsh to enhance productivity.

Development and Programming Languages

- C/C++: Proficient in developing efficient and stable systems and applications using C/C++.
- Python 3: Proficient in scripting, data analysis, and backend development using Python 3.
- PowerShell: Proficient in Microsoft Windows system management using PowerShell.
- C#: Proficient in Microsoft Office Add-ins and desktop software development (WPF, WinForm) using C#.
- Rust: Familiar with the Rust language and understand its memory safety and concurrency features.
- JavaScript: Familiar with JavaScript and have experience in frontend development.

Programming Support Tools

- Editor: Proficient in using the neovim and VSCode editor for efficient code editing.
- Version Control: Proficient in using Git for code version management.

Problem Solving Abilities

- Technical Problem Solving: Capable of efficiently utilizing tools such as Google and ChatGPT-4 to quickly find solutions to known problems.
- Capable of fully utilizing ChatGPT-4’s plugins and Custom Instructions to quickly understand and summarize literature, conducting research with high efficiency.

Other

- Effective Communication: Capable of communicating effectively with collaborators, whether through email or face-to-face discussions.
- Project Management: Strong project management skills, including code management, documentation writing, and timely progress tracking.
- Data Visualization: Proficient in using tools such as Matplotlib and MATLAB for data visualization.
- Document Writing: Fluent in using LaTeX, Markdown, and Microsoft Word for document preparation and writing.

Miscellaneous Experience

Xiaomi IoT Smart Gateway Reverse Engineering

Beijing, China
Jan. 2022 – Mar. 2022

Type: *Practical Exploration, Skill Refinement Project*

(1) Device Disassembly and Firmware Access

- Disassembled the Xiaomi Gateway to identify an JTAG interface without physical connector.
- Soldered wires from JTAG to connect to a J-link, accessed and read the firmware, and discovered the hardcoded token used for communication with cloud servers.

(2) Interception and Analysis of Firmware Update Requests

- Conducted a man-in-the-middle analysis to capture the HTTP requests for firmware updates.
- Successfully retrieved the firmware from the cloud server by emulating these requests.
- Re-linked the corresponding segments of the firmware using ld and added ELF headers, making it possible to reverse-engineer the firmware using IDA Pro.

(3) Analysis of Mi Home App and Replay Attack

- ✧ Analyzed the Android APK file of the Mi Home App to uncover the details of information transmission during the network configuration phase.
- ✧ Successfully implemented a replay attack based on this analysis.

Real Execution Trace Gathering and Comparing with Emulator's Trace

Beijing, China
Nov. 2021 – Mar. 2022

Type: *Research Paper Contribution to Semu (CCS'23)*

(1) Firmware Development for Cortex M3/M4 Based MCUs

- ✧ Wrote firmware for NXP FRDM K64F, STM32F103, Arduino Due, and other development boards based on the Cortex M3/M4 MCUs, primarily using RIOT and FreeRTOS development frameworks.
- ✧ Became proficient with the invocation of UART, I^{2}C, and other peripheral modules, as well as writing interrupt service routines (ISRs) and binding interrupt events to ISR functions.

(2) Online Debugging and Execution Trace Collection

- ✧ Utilized debugging interfaces such as OpenSDA v2 to perform online debugging through the **OpenOCD** tool.
- ✧ Employed the Python-GDB plugin provided by the **arm-none-eabi** toolchain and ran custom Python scripts to collect execution traces.
- ✧ Enabled trace collection at both the basic block and instruction levels.

(3) Emulator Fidelity Evaluation

- ✧ Applied edit distance-based algorithms to assess the discrepancies between the real hardware execution traces and the emulator's traces.
- ✧ The results of this analysis were used to derive a fidelity metric for the emulator.

Teaching Assistant Experience

Beijing, China
Aug. 2020 – Dec. 2023

Software and System Security Course at University of Chinese Academy of Sciences

(1) Taught laboratory classes covering a range of topics including:

- ✧ Stack overflow and control flow hijacking (ROP),
- ✧ Basic concepts of heap memory and heap exploitation,
- ✧ Network transmission and encrypted communication, and the design and implementation of network packet capturing tools.

(2) Enhanced students' understanding of network fundamentals and bolstered their ability to apply network security practices in development.

(3) Contributed to the improvement of Capture-The-Flag (CTF) competition problem explanations, and created high-quality course slides and other educational materials.