Zichuan Li

zichuan.li@outlook.com · https://zichuan.li

Education

Wuhan University, Hubei, China *Sep. 2020 – Jun. 2023*

M.Eng. in Cyberspace security, advised by Professor Guojun Peng, **GPA: 87.9/100**

Wuhan University, Hubei, China *Sep. 2016 – Jun. 2020*

B.Eng. in Information Security, **GPA: 3.58/4.0**

Industry Experience

OPPO Telecom. *Security Researcher* *Jun. 2022 – Sep. 2022*

Mainly worked on IoT security and learned Android Security.

- Drafted the security baseline for IoT devices.
- Found several vulnerabilities in OPPO Watch 3 Pro.
- Reverse-engineered a privacy protection feature in MIUI System and found two vulnerabilities that could bypass the protection.
- Implemented a demo feature on ColorOS, providing clipboard privacy protection.

Research Experience

Security evaluation on Huawei Taishan 2280 **Graduate Research Assistant**

Wuhan University *Dec. 2020 – Dec. 2022*

Vulnerability detection in Huawei server's firmwares (UEFI firmware and BMC firmware).

- Implemented a memory-based UEFI/BIOS emulation framework, *EFIEmulator*, based on the unicorn, which could successfully run 91 of 103 EFI files(extracted from the server).
- Built a dynamic vulnerability detection prototype system on top of the *EFIEmulator*.
- Found several vulnerabilities in Taishan 2280's UEFI and BMC firmware, including two high-risk arbitrary code execution vulnerabilities.

A large-scale vulnerability detection in UEFI firmwares **Graduate Research Assistant**

Wuhan University *May. 2022 – Oct. 2022*

Developed a static analysis tool for vulnerability detection in UEFI firmwares.

- Crawled over 3,000 unique BIOS firmwares from multiple vendors(Acer, Asus, Dell, Lenovo).
- Developed a UEFI analysis framework based on radare2 and angr, which could recognize function calls to UEFI Boot Services and Runtime Services.
- Found 10+ buffer overflow vulnerabilities in UEFI firmwares, which could be exploited to execute arbitrary code in DXE phase.

UI-Spoofing vulnerability detection in email services **Graduate Research Assistant**

Wuhan University *Dec. 2021 – Mar. 2022*

This project aims to evaluate our observation in the Datacon Competition, that many email services don't validate email sender properly during the rendering process, which could lead to email spoofing attacks. We developed an automatic tool to perform measurements, and found several vulnerabilities in various email services including qq mail, sohu mail, coremail, etc.

Vulnerability detection in several routers **Undergraduate Research Assistant**
Wuhan University *Jul. 2020 – Oct. 2020*
Vulnerability detection and exploitation on several widely used router models.

- Collected PoC of TP-Link and D-Link routers, reproduced the vulnerabilities, and wrote exploits.
- Found two vulnerabilities in Netgear R6400, which exploited the LAN interface.

Security evaluation on Huawei's Smart Home Devices **Undergraduate Research Assistant**
Wuhan University *Oct. 2019 – Sep. 2020*
Vulnerability detection in Huawei router WS5200 and Honor YOYO smart speaker.

- Tried several ways to extract the firmware: Sniffer, UART, Hardware Programmer, etc.
- Reverse engineered and analyzed the httpd and hilink binaries.
- Evaluated whether the firmware contains disclosed vulnerabilities in open-source libraries.
- Analyzed the Bluetooth traffics by using a USB Dongle.

Vulnerabilities

- LEN-99954, code execution in Lenovo's UEFI firmwares.
- LEN-99955, code execution in Lenovo's UEFI firmwares.
- CVE-2022-41415, privilege escalation in Acer's UEFI firmwares.
- CVE-2022-30426, privilege escalation in Acer's UEFI firmwares.
- CVE-2022-30078, remote code injection in Netgear routers.
- CVE-2022-30079, remote code injection in Netgear routers.

Honors & Awards

- Graduate Scholarship for Academic Excellence, Wuhan University, China *2021, 2022*
- *1st Prize*, Datacon Data Security Analytics Competition: Email Security Track, rank 1 *2021*
- *3rd Prize*, Coremail E-mail Security Competition, rank 4 *2020*
- *3rd Prize*, Chinese Information Hiding Competition, rank 4 *2019*
- *2nd Prize*, Hubei Cyberspace Security Practical Ability Competition *2018*

Professional Services

- **Sub-Reviewer**, Mobile Networks and Applications *Jun. 2021*
- **Sub-Reviewer**, Journal of Cybersecurity *Apr. 2021*
- **Teaching Assistant**, Software Security, *Online MOOC* *Spring. 2021*
- **Teaching Assistant**, Software Security, Wuhan University *Fall. 2020*
- **Organizing Committee**, *9th XDef* Network and Information Security Protection Summit *Apr. 2021*
- **Organizing Committee**, *8th XDef* Network and Information Security Protection Summit *Dec. 2019*

Skill Set

- Programming Tools: Python, C/C++, Java, LaTeX, Vim, Git;
- Security Analysis: Pwntools, IDA Pro, Ghidra, Burp Suite, etc.
- Program Analysis: QEMU, GDB, angr, radare2, etc.