GENGDA SHE

+86 14789891018 | m202171734@hust.edu.cn | https://github.com/sgd88888 |https://sgd88888.github.io/

EDUCATION

Huazhong University of Science and Technology Wuhan, China
MSc in Cyber Security Sep 2021 – Present

- AVG: 86.47/100;
- Selected Awards: First-Class Master's Academic Award (2021-2022), Second-Class Master's Academic Award (2022-2023);
- Core Courses: *Fundamental of Computing Theory, Epidemic Model of Computer Virus, Quantum Computing and Quantum Cryptography, Information Retrieval, Software Reverse Analysis Technology and Its Application, Modern Cryptography, Intelligent Media Computing.*

Huazhong University of Science and Technology Wuhan, China
Bachelor of Engineering (Information Security) Sep 2017 – Jun 2021

- GPA:3.81/4, AVG 86.5/100;
- Selected Awards: Self-improvement Scholarship (2017 & 2018), Public Welfare Scholarship (2019 & 2020), Academic Excellence Scholarship (2018, 2019 & 2020), Outstanding Graduate of 2021;
- Core Courses: *Wireless Network Security, Network Security Programming, Program Analysis for Security, Network Forensic, Reverse Engineering Technology, Advanced Cryptography Application, Assembly Language Programming, Comprehensive Practice of Network Security.*
- Thesis: Fuzz Testing for Linux Hardware Drivers. (Supervisor: Dr. Cai Fu)

RESEARCH EXPERIENCE

HUST – NetSec Academy of the National Cybersecurity Talent Base (Wuhan)

Research Assistant to Prof. Cai Fu (PI: Cybersecurity Lab) May 2020 – Present

Main Project: *Kernel Driver Vulnerability Mining Using Fitness and Input Constraint Models*

- Directed the project's design, from conceptualization to code development in *Python* and *C*, to ensure rigorous research trial management;
- Utilized advanced instrumentation with *eBPF*, *Kprobes*, and *IDA Pro* for precise basic block probing;
- Formulated a tailored input constraint model that was derived from in-depth driver code analysis to optimize the fuzzing process;
- Formulated a unique fitness computation strategy that integrates state-of-the-art genetic algorithms to amplify vulnerability detection capabilities;
- Authored an academic paper on the project (refer to the "Publication" section).

Main Project: *EFPSDN - Intelligent Protection Solution for Scalable and Resilient SDN Controller*

- Strategized the overall system blueprint to ensure it met the latest cybersecurity standards;
- Led the coding and implementation phase using *Python, Mininet, and Hping3*;
- Simulated real-world data center environments using *mininet* to craft an authentic topology map for testing;
- Employed *ping3* to simulate realistic DDOS attacks, assess and prove the system's robust defense capabilities;
- Secured the Second Prize in the 2022 Network Technology Challenge, Central China Region.

Other Projects:

Basic Theory and Techniques of Liquid Code；

Online Integrated Management Prototype System for Mobile Terminals；

Tensor-based approach for cross-platform vulnerability detection in binary code.

Roles:

- Designed and rolled out the DOP system's demonstration interface for the Liquid Code research to enhance the visual representation of the data-driven programming techniques;

- Employed *IDA Pro* and *Python* scripts for Tensor project to automate function window information extraction and streamline feature vector extraction;
- Configured and tested a simulated server environment using *VMware* for the Mobile Terminal Management project to guarantee robust system integration on the *Bear-Pi* platform;
- Collected and analyzed vulnerabilities containing gadgets within the Liquid Code research, and identified potential CVEs in openharmony vulnerabilities for more in-depth experimentation;
- Oversaw testing of all functionalities of the Integrated Management Prototype System to solidify mobile terminal security and optimize cryptographic resource protocols.

PUBLICATION

She, G., Fu, C., Cen, Z., & Lü, J. (2023). Kernel Driver Vulnerability Mining - Based on Fitness and Input Constraint Models. *Computer Application Research*, 40(7). ISSN: 1001-3695.

PROGRAMMING

Languages:

- Python;
- C, C++;
- HTML.

Tools:

- Hping3, Django, Iperf, Kcov, Ping3.

Frameworks:

- eBPF, Kprobes, IDA Pro, VMware, Mininet, AFL, Syzkaller,Origin OllyDebug.

Operating Systems:

- Ubuntu, Linux, Fedora, Android.

Development Environments:

- Pycharm, Codeblocks.