Last Updated: July 2025

Runtao He / 何润涛

runtaohe@hdu.edu.cn · blog · @RuntaoHe

EDUCATION

Hangzhou Dianzi University, Hangzhou, Zhejiang 2022 – 2026

Bachelor, Intelligent Security (Cyber Security), Zhuoyue Honors College

PROFESSIONAL EXPERIENCE

UCLA 2025 May – Present

Summer Research Intern, remote

Advised by Prof. Yuan Tian.

G.o.S.S.I.P, SJTU, Shanghai, China 2023 Jul – 2025 May

Undergraduate Research Intern, hybrid

Advised by Dr. Juanru Li.
G.o.S.S.I.P is the short version of Group of Software Security In Progress leaded by Dr.Juanru Li at Shanghai Jiao Tong University. My internship at GoSSIP covered a wide range of security academic learning, including paper reading, conducting academic research, participating in competition as well as doing experiments. All the experiences enhanced my professional knowledge and made me become more interested in academic research.

Shanghai Qizhi Institute, Shanghai, China 2023 Jul – Sep

Security Research Intern, on-site PI : Juanru Li

Conduct systematic security analysis on open source and operating systems currently used in common network equipment (routers, optical modems, etc.), summarize typical security issues and design and implement relevant security analysis tools. Specifically, I **discovered some issues with authentication flaws exists in OpenWRT system add-ons**. And we proposed a tool named **ChkAPIC** to automatically detect 8 kinds of authentication misuse in networking related add-ons.

PROJECTS

Development

ChkAPIC

ChkAPIC is a static code analysis tool that implements an approach to Check for flawed implementations of Authentication Procedures with Improperly used Credentials in open-source router OS add-ons. ChkAPIC is built on top of the Clang Static Analyzer source code analysis engine and utilizes an NLP-enhanced code pre-processing to complement its static code analysis-based flaw detection against authentication credentials. In particular, the NLP-enhanced pre-processing not only identifies credential-related variables and functions in source code but also replaces function pointers. With the pre-processed source code, ChkAPIC conducts a more accurate data flow analysis and tracks the propagation of credentials. To precisely detect insecure uses of credentials, ChkAPIC adopts a multi-tag taint analysis which maps specific security properties to different tags. By checking the propagation of certain tags, ChkAPIC can detect eight typical security violations.

- Website: ChkAPIC

Public Course Labs

MIT 6.S081: Operating System Engineering

Having completed several labs within the renowned MIT Operating System Engineering course, I have acquired a wealth of knowledge pertaining to system fundamentals. This immersive experience has deepened my understanding of critical aspects such as system calls, system architecture, and file systems, enriching my expertise in the intricate workings of operating systems.

PUBLICATIONS

PAPERS

- **Detecting Vulnerable Custom Authentication Schemes in Router OS Add-ons.** Under Review

INVITED TALKS

- **Research on authentication security based on OpenWRT system add-ons code**
  Alibaba Cloud Xian Zhi Security Salon, Hangzhou, Zhejiang
  [Slides]

AWARDS & HONORS & CTF

First-Class Prize, School Scholarship	2024 & 2025
First Prize, CISCN Southeast China Regional Tournament	2024
Host, D^3CTF2024	2024
4th, The Second Aliyun(Alibaba Cloud) CTF	2024
3rd & Outstanding Prize, RealWorld CTF 2024	2024
Excellent Team Award, Datacon 2023	2023
Third-Class Prize, School Scholarship	2023
6th, RealWorld CTF 2023	2023
6th, Aliyun(Alibaba Cloud) CTF	2023
6th, PWNHUB 2022	2022
Second-Class Prize, School Scholarship	2022
1st, Zhijiang Cup Industrial Safety International Elite Challenge	2022

VULNERABILITY CREDITS

- CVE-2023-34924
  I found this vulnerability in my freshman year. Here is the bug description:
  H3C Magic B1STW B1STV100R012 router was discovered to contain a stack overflow via the function SetAPInfoById. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.
  Repository

PUBLIC EXPERIENCES

Blackhat Asia 2024 Student Pass	2024
Alibaba Cloud White Hat Conference	2024
Huawei Tech x Security Invited Talks 2024	2024
Huawei Tech x Security Invited Talks 2023	2023

Huawei Kunpeng Developer Innovation Day 2022

LEADERSHIP

Vidar-Team 2022 – 2023

CTF Team Leader

Zhuoyue Honors College Study Community 2022 – 2023

CTF Learning Community Leader

SKILLS

- Programming: C / C++ / Python / Assembly
- Security: Binary Security Exploit & Defence (PWN) / Program Analysis (IDA, GDB) / Static Analysis (LLVM-CSA) / IoT Security (Routers)
- Others: Linux / Windows / Git / Docker / NLP

MISC

- Personal Blog: https://l0tus.vip
- GitHub: https://github.com/ChrisL0tus
- Language: English - Full professional proficiency / Chinese - native / Spanish - green hand
- Art & Philosophy: Violin & Poem; Fond of Friedrich Nietzsche
- Sports: Body building & Tennis