Jianwei Huang

Contact

Address: Peterson 242, TAMU, College Station, Texas
Phone: 979-985-1097
Github: https://github.com/cl0udz
E-mail: jwhuang@tamu.edu

About Me

I am a Ph.D. student in the Department of Computer Science & Engineering at Texas A&M University and my adviser is Prof. Guofei Gu. My research mainly focuses on detecting vulnerabilities with program analysis techniques.

Education Background

Texas A&M University, College Station, Texas
Ph.D. student in Computer Science 09/2019 - 12/2025 (expected)
Wuhan University, Wuhan, China
Bachelor of Engineering, Computer Science 09/2014 - 06/2018

Selected Project Experience

(ongoing) Blackbox Fuzzing on Web Application with LLM Assistance
Keywords: Fuzzing, LLM Agent Development, JavaScript Instrumentation

- Designed an LLM-driven framework for client-side fuzzing of web applications.
- Evaluating the framework on open-source web applications and conducting large-scale testing on Docker Hub images.

Security Analysis on Ethereum Name Service (ENS) [9]
Keywords: Android Reverse Engineering, Android Instrumentation, Security Analysis

- Discovered a unique security vulnerability in ENS.
- Identified inconsistencies in ENS domain normalization across popular wallets, dApps, and ENS controllers.
- Assessed security risks in 300+ widely used dApps and collaborated with vendors to mitigate them.

(in submission) Security Analysis of One-Time Tokens in Web Applications
Keywords: Threat Modeling, JavaScript Static Analysis

- Identified discrepancies between RFC specifications and real-world implementations.
- Defined the lifecycle and essential security properties of One-Time Tokens in web applications.
- Developed an automated tool to detect and assess the security properties of One-Time Tokens.
- Evaluated the security of One-Time Tokens in popular Node.js web applications, uncovering 20+ vulnerabilities.

Zero Trust Framework Design and Implementation [8]
Keywords: Linux Kernel, System Programming, Software-Defined, Intrusion Detection

- Developed *sysflow*, a Zero Trust Framework enabling unified, dynamic, and fine-grained security controls for system resources.
- Implemented two key applications leveraging *sysflow* to provide context-aware access control on Linux.
- Code @ successlab/sysflow-controller & successlab/sysflow-dataplane

Security Framework Based on Service Worker [7]
Keywords: Web Security, Client-side Defenses

- Contributed to the development of a Service Worker-based security framework to enhance website security on the client side.
- Designed and implemented several security applications within the framework.

- Code @ successlab/swapp

Hidden Property Abusing in the Node.js Ecosystem [5]
Keywords: JavaScript Static/Dynamic Analysis, Taint Analysis

- Developed an automated tool to detect hidden properties in Node.js programs.
- Evaluated the tool on over 70 widely used Node.js libraries.
- Code @ xiaofen9/Lynx (Final Release) & cl0udz/HiPar (Development Repository)

Security Analysis of SDN Controllers [3][4]
Keywords: Java Static Analysis, Taint Analysis

- Conducted security analysis of the top open-source SDN controllers.
- Discovered approximately 10 vulnerabilities related to unintended data dependency creation.
- Developed a tool to identify sensitive methods in SDN controllers and generate data dependencies for targeted attacks.

iOS Application Analysis
Keywords: iOS Reverse Engineering, iOS Instrumentation

- Created an automated tool to identify key functions related to specific features in iOS applications.
- Uncovered critical vulnerabilities in WeChat SDK and Meituan.
- Code @ cl0udz/Corgi

Working Experience

SRI International, Menlo Park, CA, USA
Summer Intern 05/2020 - 08/2020

- Student Intern - Covid App Research

Texas A&M University, Texas, USA
Teaching Assistant

- Assisted in class CSCE 465: Computer & Network Security
- Assisted in class CSCE 451/652: Software Reverse Engineering
- Assisted in class CSCE 477/703: Cybersecurity Risk

Awards

- **TAMUCTF 2024 -** Competed individually, Ranked 4 among TAMU teams & 50 overall.
- **BCTF 2015 -** Ranked 1st
- **0CTF 2015 -** Ranked 3rd
- Second Prize of National SDN Developer Contest, 2015

Publications

[1] Jianming Fu, **Jianwei Huang**, and Lanxin Zhang. ”Curtain: Keep Your Hosts Away from USB Attacks.” International Conference on Information Security. Springer, Cham, 2017.

[2] Yuan Shi, Huanguo Zhang, Juan Wang, Feng Xiao, **Jianwei Huang**, Daochen Zha, Hongxin Hu, Fei Yan, Bo Zhao, ”Chaos: an sdn-based moving target defense system.” Security and Communication Networks 2017 (2017).

[3] Feng Xiao, **Jianwei Huang**, Peng Liu, ”Hacking the brain: Customize Evil Protocol to Pwn an SDN Controller”, DEF CON 26, 2018.

[4] Feng Xiao, Jinquan Zhang, **Jianwei Huang**, Guofei Gu, Dinghao Wu, Peng Liu. "Unexpected Data Dependency Creation and Chaining: A New Attack to SDN." In Proc. of the 41st IEEE Symposium on Security and Privacy (S&P'20), 2020

[5] Feng Xiao, **Jianwei Huang**, Yichang Xiong, Guangliang Yang, Hong Hu, Guofei Gu, and Wenke Lee. Abusing Hidden Properties to Attack the Node.js Ecosystem. USENIX 2021

[6] Yangyong Zhang, Sunpreet Arora, Maliheh Shirvanian, **Jianwei Huang**, Guofei Gu. Practical Speech Reuse Prevention in Voice-driven Services. RAID 2021

[7] Phakpoom Chinprutthiwong, **Jianwei Huang**, and Guofei Gu. SWAPP: A New Programmable Playground for Web Application Security. USENIX 2022

[8] Hong Sungmin, Lei Xu, **Jianwei Huang**, Hongda Li, Hongxin Hu, and Guofei Gu. "SysFlow: Towards a Programmable Zero Trust Framework for System Security." IEEE Transactions on Information Forensics and Security (2023).

[9] **Jianwei Huang**, Sridatta Raghavendra Chintapalli, Mengxiao Wang, Guofei Gu. "Beyond Visual Confusion: Understanding How Inconsistencies in ENS Normalization Facilitate Homoglyph Attacks." The Web Conference (WWW) 2025.

Skills

- Programming Languages: C, Python, Java
- Program Analysis: JavaScript(Jalangi, esprima), Java(Soot)
- System Programming: Windows, Linux