Jianwei Huang

979-985-1097 | cloudz | jwhuang@tamu.edu
College Station, TX | jianwei.me | jianwei-huang

PhD student specializing in vulnerability detection through program analysis.

Education

Texas A&M University 09/2019 – 12/2025(Expected)
Ph.D., Computer Science *College Station, TX*

Wuhan University 09/2014 – 06/2018
Bachelor of Engineering, Computer Science *Wuhan, China*

Work Experience

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

Android Application Analysis, Data Analysis

- Identified two vulnerabilities in the design of popular COVID tracking apps
- Assessed the risks posed by two vulnerabilities in 10+ popular COVID tracking apps

Texas A&M University Ongoing
Teaching Assistant *Texas, USA*

Computer Security, Reverse Engineering, Risk Analysis

- CSCE 465: Computer & Network Security, Assisted the professor in teaching
- CSCE 451/652: Software Reverse Engineering, Assisted students in solving CTF challenges
- CSCE 477/703: Cybersecurity Risk, Set up class CTF

Projects

Blackbox Fuzzing on Web Application with LLM Assistance Ongoing

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) 2024

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.
- **Identified security risks in 200+ widely used dApps** and collaborated with vendors to mitigate them.

Security Analysis of One-Time Tokens in Web Applications In Submission

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 2023

Linux Kernel, System Programming, Software-Defined, Intrusion Detection

- Developed *sysflow* Controller Dataplane, a Zero Trust Framework. Implemented the telemetry in Linux Kernel and communication channel between the dataplane and the controller.
- Implemented an application with *sysflow* to provide context-aware access control in web applications by applying privileges defined application-level to files.

Security Framework Based on Service Worker 2022

Web Security, Client-side Defenses

- Contributed to the development of a Service Worker-based security framework SWAPP. Designed and implemented the storage management pipeline the communication channel between DOM and service worker

Jianwei Huang

979-985-1097 | cloudz | jwhuang@tamu.edu
College Station, TX | jianwei.me | jianwei-huang

- Designed and implemented two security applications within the framework to defend against information leakage and MITM attacks on the client-side

Hidden Property Abusing in the Node.js Ecosystem 2021

JavaScript Static/Dynamic Analysis, Taint Analysis

- Developed an automated tool Final Release Development Repository to detect hidden properties in Node.js programs with a combination of static and dynamic taint analysis.
- Evaluated the tool on over 70 widely used Node.js libraries and **identified 15+ vulnerabilities**.

Security Analysis of SDN Controllers 2018-2020

Java Static Analysis, Taint Analysis

- Conducted security analysis of the top open-source SDN controllers.
- **Discovered 18 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 2017

iOS Reverse Engineering, iOS Instrumentation

- Developed an automated tool Corgi to identify key functions of specific features in iOS applications.
- Uncovered critical vulnerabilities in WeChat SDK and Meituan.

Awards

TAMUCTF 2024 – 4th (TAMU), 50th Overall 2024

- Competed individually and solved **all Web challenges.**

BCTF 2015 - 1st Place 2015

- Focused on Web challenges

0CTF 2015 - 3rd Place 2015

- Focused on Web challenges

Software-Defined Networking (SDN) Development Competition - 2nd Prize 2015, China

- Designed a moving target defense mechanism with OpenDayLight, which rotates IP addresses in the network to obfusacte the topology

Publications

Curtain: Keep Your Hosts Away from USB Attacks ISC 2017

- *Jianming Fu, **Jianwei Huang**, and Lanxin Zhang*

Chaos: An SDN-Based Moving Target Defense System SCN 2017

- *Yuan Shi, Huanguo Zhang, Juan Wang, Feng Xiao, **Jianwei Huang**, Daochen Zha, Hongxin Hu, Fei Yan, Bo Zhao*

Hacking the Brain: Customize Evil Protocol to Pwn an SDN Controller DEF CON 26, 2018

- *Feng Xiao, **Jianwei Huang**, Peng Liu*

Unexpected Data Dependency Creation and Chaining: A New Attack to SDN IEEE S&P 2020

- *Feng Xiao, Jinquan Zhang, **Jianwei Huang**, Guofei Gu, Dinghao Wu, Peng Liu*

Abusing Hidden Properties to Attack the Node.js Ecosystem USENIX Security 2021

- *Feng Xiao, **Jianwei Huang**, Yichang Xiong, Guangliang Yang, Hong Hu, Guofei Gu, Wenke Lee*

Practical Speech Reuse Prevention in Voice-driven Services RAID 2021

- *Yangyong Zhang, Sunpreet Arora, Maliheh Shirvanian, **Jianwei Huang**, Guofei Gu*

SWAPP: A New Programmable Playground for Web Application Security USENIX Security 2022

- *Phakpoom Chinprutthiwong, **Jianwei Huang**, and Guofei Gu*

SysFlow: Towards a Programmable Zero Trust Framework for System Security IEEE TIFS 2023

- *Hong Sungmin, Lei Xu, **Jianwei Huang**, Hongda Li, Hongxin Hu, and Guofei Gu*

Beyond Visual Confusion: Understanding How Inconsistencies in ENS Normalization Facilitate Homoglyph Attacks WWW 2025

- ***Jianwei Huang**, Sridatta Raghavendra Chintapalli, Mengxiao Wang, Guofei Gu*

Skills

Languages C, Python, Java
Program Analysis Static(Soot, esprima), Dynamic(Jalangi, ExpoSE)
GenAI Agent Development