# Jianwei Huang

979-985-1097
435 Nagle St, College Station, TX
cloudz
jianwei.me
hjwcloud@gmail.com
jianwei-huang

Ph.D. student specializing in vulnerability detection using program analysis and LLM-assisted fuzzing
*Darpa AIxCC Final Competitor; DEF CON Speaker; Blackhat Speaker*

## 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

**Amazon** 05/2025 – 08/2025
*Security Engineer Intern* *Austin, TX, USA*

*LLM-Assisted Threat Modeling, LangChain*

- Developing an agentic system for automating threat modeling in GenAI application security reviews, supporting extensibility across varied information sources
- Identified a jailbreak attack on Amazon Nova Models

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

*Android Application Reverse Engineering*

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

## Publications

**Curtain: Keep Your Hosts Away from USB Attacks** ISC 2017
*Windows Kernel Programming, Machine Learning*
- *Jianming Fu, **Jianwei Huang**, and Lanxin Zhang*

**Chaos: An SDN-Based Moving Target Defense System** SCN 2017
*SDN Programming*
- *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
*Java Static Analysis*
- *Feng Xiao, **Jianwei Huang**, Peng Liu*

**Discovering Hidden Properties to Attack the Node.js Ecosystem** Blackhat, 2020
*JavaScript Static/Dynamic Analysis*
- *Feng Xiao, **Jianwei Huang**, Yichang Xiong, Guangliang Yang, Hong Hu, Guofei Gu, Wenke Lee*

**Unexpected Data Dependency Creation and Chaining: A New Attack to SDN** IEEE S&P 2020
*Java Static Analysis*
- *Feng Xiao, Jinquan Zhang, **Jianwei Huang**, Guofei Gu, Dinghao Wu, Peng Liu*

**Abusing Hidden Properties to Attack the Node.js Ecosystem** USENIX Security 2021
*JavaScript Static/Dynamic Analysis*
- *Feng Xiao, **Jianwei Huang**, Yichang Xiong, Guangliang Yang, Hong Hu, Guofei Gu, Wenke Lee*

**Practical Speech Reuse Prevention in Voice-driven Services** RAID 2021
*Voice Signal Processing*
- *Yangyong Zhang, Sunpreet Arora, Maliheh Shirvanian, **Jianwei Huang**, Guofei Gu*

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

# Jianwei Huang

979-985-1097
435 Nagle St, College Station, TX
cloudz
jianwei.me
hjwcloud@gmail.com
jianwei-huang


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

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

*Linux Kernel Programming*

› *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

*Android Reverse Engineering*

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

**LogicWeaver: Stitching Client Clues into Deep Web Fuzzing Paths with LLM assistance** In Submission

*LLM Agent Development, LangChain*

› ***Jianwei Huang**, Guofei Gu*

## Awards

**AIxCC Final Competition 2025 – TBD in August** 2025

› Contributed a fuzzing strategy with static analysis results and LLM assistance

**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

## Skills

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