Haichuan (Ken) Xu

haichuanxu@gatech.edu
https://haichuanxuken.github.io
https://www.linkedin.com/in/haichuan-ken-xu/

Research Interests

My research focuses on fraud and abuse detection, including forensic techniques for Android malware and Ethereum smart contracts, leveraging program analysis and machine learning for behavior modeling. I'm interested in Android security, banking and blockchain security, large-scale malware analysis, privacy leakage discovery, and system design that secures user privacy.

Education

Ph.D. in Computer Science 08/21 - 12/25
Cyber Forensics Innovation Laboratory
Advisor: Professor Brendan Saltaformaggio
Georgia Institute of Technology Atlanta, GA

Master of Science in Computer Engineering 08/19 - 05/21
Georgia Institute of Technology Atlanta, GA

Bachelor of Science with Honors in Computer Engineering 08/15 - 05/19
University of Illinois at Urbana-Champaign Champaign, IL

Publications

Top-Tier Security Conferences

Xu, H., Yao, M., Zhang, R., Dawoud, M., Park, J., Saltaformaggio, B., "DVa: Extracting Victims and Abuse Vectors from Android Accessibility Malware," In *Proceedings of the 33rd USENIX Security Symposium (Security '24)*, Philadelphia, PA, Aug. 2024. [Open Source]
USENIX Artifact Evaluation Result: 🏅Available, 🏅Functional.

Zhang R., Yao, M., **Xu, H.**, Alrawi, O., Park, J., Saltaformaggio, B., "Hitchhiking Vaccine: Enhancing Botnet Remediation With Remote Code Deployment Reuse," To Appear in *Proceedings of the 2025 Annual Network and Distributed System Security Symposium (NDSS '25)*, San Diego, CA, Feb. 2025. [Open Source]

Yao, M., Zhang R., **Xu, H.**, Chou, R., Paturi, V., Sikder, A., Saltaformaggio, B., "Pulling Off The Mask: Forensic Analysis of the Deceptive Creator Wallets Behind Smart Contract Fraud," In *Proceedings of the 45th IEEE Symposium on Security and Privacy (S&P '24)*, San Francisco, CA, May. 2024. [Open Source]

Fuller, J., Pai Kasturi, R., Sikder, A., **Xu, H.**, Arik, B., Verma, V., Asdar, E., Saltaformaggio, B., "C3PO: Large-Scale Study Of Covert Monitoring of C&C Servers via Over-Permissioned Protocol Infiltration," In *Proceedings of the 28th ACM Conference on Computer and Communications Security (CCS '21)*, Virtual Conference, Nov. 2021. [Open Source]

Work Experience

Security Research Intern 05/24 - 08/24
Bank of America (BofA) Addison, TX

Identified 10K fraud transactions by modeling behaviors of PoC Android malware.
Deployed proactive defense against Android malware in the BofA app by collaborating with development team.
Streamlined BofA's malware response process and improved efficiency by creating a mobile malware defense playbook and operationalizing it with the malware analytics team.

Research Experience

Research Assistant 01/20 - Present
Georgia Institute of Technology Atlanta, GA

1. Digital Wallet Card Binding Fraud Detection. **Work In Progress**
Collaborating with BofA to prevent ATO initiated from digital wallet apps.
Using machine learning to classify fraudulent card binding based on bank logs.
Applying dynamic traffic analysis to extract insecure verification protocols utilized by banks.

2. Android Banking Accessibility Malware Analysis. **Published - USENIX Security '24**
Created a cloud-based solution to help Google Play block on-device monetization malware.
Developed dynamic forced execution techniques to reveal 215 targeted victims of a11y malware.
Applied symbolic execution to attribute a11y malware behaviors to their fine-grained victims.
Detected 59K instances of abuse vector from automated analysis on 9,850 Android a11y malware.

3. Ethereum Fraudulent Smart Contract Forensics. **Published – IEEE S&P '24**
Uncovered 2.6M ETH ($2B) in illicit profit associated with fraud contracts.
Traced 1M contracts linked to 91 creator wallets from 157 confirmed fraud contracts.
Developed symbolic analysis engine to aid Etherscan and FBI to combat fraud contracts.

4. Android Frontend Botnet Takedown. **Accepted – NDSS '25**
Created app sandbox to capture dynamic code loading (DCL), e.g. JAR, DEX, APK, JS.
Applied taint analysis to classify 5 DCL routine capabilities, e.g. command execution, toast msg.
Generated remediation payload to notify frontend user and automatically remove frontend botnet.
Successful remediation payload generated for 523 / 702 Android botnet.

5. Android Industrial Control System (ICS) App Vulnerability Analysis. **In Submission – EuroS&P '25**
Discovered 1 CVE, received 4 email confirmations from vulnerability disclosure to developers.
Identified 52 instances of vulnerabilities from 139 ICS apps by developing a static scanner that identifies unauthorized access, command injection, DoS, and UI modification vulnerabilities.

Media Coverage

Researchers develop new tool for spotting Android malware. [TechRadar][NY Breaking][MSN]
New Open-Source Tool From Georgia Tech Can Help Protect Your Android From Malware. [Hypepotamus]
Newly Developed Tool Helps Researchers Spot Android Malware. [hackerdose]
New tool can detect malware on Android phones. [TechXplore][Sensi Tech Hub]
Georgia Tech's New Tool Can Detect Malware on Android Phones. [Georgia Tech][Science of Security]
New Tool Detects Malware Exploiting Smartphone Accessibility Features. [WizCase]
New Tool DVa Detects and Removes Android Malware. [Hackread]
Malware Is Exploiting This Android Feature on Millions of Smartphones. Researchers Say They Know How to Detect It. [xatakaen]

Technical Skills

Languages: Java, Python, x86 Assembly, Jimple, C, C++, SQL, JavaScript, HTML/CSS, Shell
Machine Learning: PyTorch, TensorFlow, OpenNN, scikit-learn, numpy, pandas, LangChain
Security Analysis Tools: Soot, Jadx, Appium, Frida, Xposed, IDA Pro, angr, Ghidra, Pin, Drozer, Wireshark, Burp Suite
Program/Binary Analysis: symbolic analysis, data-flow analysis, sandbox, dynamic hooking, forced execution, reverse engineering
Development Tools: Linux, Git, AWS, GCP

Honors & Awards

Research Grants
Bank of America Research Collaboration Funding — 2023

Travel Grants
30th USENIX Security Symposium (Security '21) — 2021

Teaching

Guest Instructor — 02/23 & 02/24
ECE 4117: Introduction to Malware Reverse Engineering
Georgia Institute of Technology — Atlanta, GA

Guest Instructor — 10/22
ECE 6747: Advanced Topics in Malware Analysis
Georgia Institute of Technology — Atlanta, GA

Teaching Assistant — 10/18
ECE 385: Digital Systems Laboratory
University of Illinois at Urbana-Champaign — Champaign, IL

Teaching Assistant — 07/17
ECE 110: Introduction to Electronics (Summer Camp)
University of Illinois at Urbana-Champaign — Champaign, IL

Services

Artifact Evaluation Committee
ACM Computer and Communications Security (CCS) — 2024

CVE Disclosure
CVE-2022-32530 — 2022

Student Assistant
IEEE Secure Development Conference — 2021 - 2023

External Reviewer (Total = 27)

IEEE Symposium on Security and Privacy (S&P)	2021 - 2024
Network and Distributed System Security Symposium (NDSS)	2021, 2023 - 2024
USENIX Security Symposium (USENIX)	2021 - 2023
ACM Computer and Communications Security (CCS)	2020, 2023
European Symposium on Research in Computer Security (ESORICS)	2020, 2023
Annual Computer Security Applications Conference (ACSAC)	2020, 2022 - 2023
Computers & Security Journal (COSE)	2020, 2022
Language-Theoretic Security (LangSec)	2022
IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS)	2022
Research in Attacks, Intrusions, and Defenses (RAID)	2020 - 2021
Transactions on Information Forensics and Security (TIFS)	2020 - 2021
IEEE European Symposium on Security and Privacy (Euro S&P)	2021
Digital Forensics Research Workshop (DFRWS)	2021

Relevant Coursework

Advanced Malware Analysis, Computer Network Security, Secure Computer Systems, Machine Learning, Empirical Computer Security, Information Security CTF Lab, Advanced Programming Techniques, Data Structures, Algorithms and Models of Computing