Haichuan 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 Large Language Models, leveraging program analysis and machine learning for behavior modeling. I'm interested in Android security, large-scale malware analysis, banking and blockchain security, and privacy leakage discovery.

Education

Ph.D. in Computer Science 08/21 - 05/26
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

Work Experience

Software Engineer Intern 05/25 - 08/25
Meta Menlo Park, CA

Built an end-to-end full-stack pipeline to ingest and query VirusTotal malware behavioral data.
Developed a PHP backend to handle report ingestion, parsing, storage, and LiveHunt rule matching.
Crafted a React UI to display VirusTotal report data, author LiveHunt rules, and visualize matched results.

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.

Selected Publications

Top-Tier Security Conferences

Xu, Haichuan, 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.

Xu, Haichuan, Zhang, R., Yao, M., Oygenblik, D., Huang, Y., Park, J., Saltaformaggio, B.
"Lock the Door But Keep the Window Open: Extracting App-Protected Accessibility Information from Browser-Rendered Websites," In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (**CCS '25**)*, Taipei, Taiwan, Oct. 2025. [Open Source] CCS Artifact Evaluation Result: Available, Functional.

Zhang, R., Sridhar, R.P., Yao, M., Yang, Z., Oygenblik, D., **Xu, Haichuan**, Dave, V., Herley, C., England, P., Saltaformaggio, B.
"Identifying Incoherent Search Sessions: Search Click Fraud Remediation Under Real-World Constraints," In *Proceedings of the 46th IEEE Symposium on Security and Privacy (**S&P '25**)*, San Francisco, CA, May. 2025.

Zhang, R., Yao, M., **Xu, Haichuan**, Alrawi, O., Park, J., Saltaformaggio, B.
"Hitchhiking Vaccine: Enhancing Botnet Remediation With Remote Code Deployment Reuse," 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, Haichuan**, 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]

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, PHP, 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

Services

CVE Discovery
CVE-2022-32530 2022

Artifact Evaluation Committee
USENIX Security Symposium (Security) 2025
ACM Computer and Communications Security (CCS) 2024