Haichuan Xu (Ken)

2579 Red Alder Alley, Doraville, GA, 30360
☎ 404-736-4392 ✉ haichuanxu@gatech.edu https://haichuanxuken.github.io

Education

Ph.D. in Electrical and Computer Engineering **August 2021 – May 2025**
Georgia Institute of Technology *Atlanta, GA*

Master of Science in Electrical and Computer Engineering **August 2019 – May 2021**
Georgia Institute of Technology *Atlanta, GA*

Bachelor of Science with Honors in Computer Engineering **August 2015 – May 2019**
University of Illinois at Urbana-Champaign *Champaign, IL*

Technical Skills

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

Publications | *Peer-Reviewed Articles*

- **Xu, H.**, Yao, M., Zhang, R., Moustafa, M., Park, J., Saltaformaggio, B.,"DVa: Extracting Victims and Abuse Vectors from Android Accessibility Malware," To Appear In 33rd USENIX Security Symposium (Security '24), Philadelphia, PA, Aug. 2024.
- 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.

Research Projects

Android Accessibility Malware Analysis | *Accepted – USENIX Security '24* **2023**

- Detected 59K instances of abuse vector from automated analysis on 9,850 Android a11y malware.
- Developed dynamic forced execution techniques to reveal 215 targeted victims of a11y malware.
- Created semantic modeling of 7 a11y abuse vectors and 6 persistence mechanisms.
- Applied symbolic execution to attribute a11y malware behaviors to their fine-grained victims.

Android Frontend Botnet Takedown | *In Submission – ACM CCS '24* **2024**

- 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 messages.
- Generated successful remediation payload for 523 / 702 Android botnets to notify user and automatically remove them.

Android Industrial Control System (ICS) App Vulnerability Analysis **2022**

- 1 CVE discovered, 4 email confirmations from vulnerability disclosure to developers.
- Developed static scanner that identifies unauthorized access, command injection, DoS, and UI modification vulnerabilities in Android ICS apps.
- Identified 52 instances of vulnerabilities from 139 ICS apps.

Windows Botnet Covert C&C Infiltration. | *Published – ACM CCS '21* **2021**

- Identified 62K over-permissioned protocols (FTP, IRC, MySQL, etc.) used by 200k Windows botnets.
- Applied backward slicing in angr to extract 443K instances of C&C monitoring capabilities.

Relevant Coursework

- Malware Analysis
- Network Security
- SE-Linux
- CTF Lab
- Empirical Security
- Data Structures
- Advanced Algorithms
- Machine Learning

Awards & Services

Research Grant | *Bank of America Digital Wallet Anti-Fraud Collaboration Funding* **2023**
CVE Disclosure | *CVE-2022-32530 — CVSS v3.1 Base Score 4.8 — Medium Severity* **2022**
Student Volunteer | *IEEE Secure Developement Conference* **2021 - 2023**