Haichuan Xu

haichuanxu@gatech.edu
https://haichuanxuken.github.io

Research Interests

Cyber forensics and system security with a focus on Android accessibility (a11y) security, large-scale malware analysis, privacy leakage discovery, and system design that secure user privacy.

Education

Ph.D. in Electrical and Computer Engineering 08/21 - 05/25
Cyber Forensics Innovation Laboratory
Advisor: Professor Brendan Saltaformaggio
Georgia Institute of Technology Atlanta, GA

Master of Science in Electrical and 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

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 Experience

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

1. Android a11y Malware Analysis. **Accepted - USENIX Security '24**
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.
Detected 59K instances of abuse vector from automated analysis on 9,850 Android a11y malware.

2. Android Frontend Botnet Takedown. **In Submission – USENIX Security '24**
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.

3. Android Industrial Control System (ICS) App Vulnerability Analysis.
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.
1 CVE issued, 4 email confirmations from vulnerability disclosure to developers.

4. Windows Botnet Covert C&C Infiltration. **Published – CCS '21**
Identified 62K over-permissioned protocols (FTP, IRC, MySQL, etc.) used by 200k botnets.
Applied backward slicing in angr to extract 443K instances of C&C monitoring capabilities.

Relevant Coursework

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

Technical Skills

Languages: Java, Python, x86 Assembly, Jimple, C/C++, SQL, JS, HTML/CSS, Shell
Security Analysis Tools: Soot, Jadx, Frida, Xposed, IDA Pro, angr, Ghidra, Pin, Drozer, Wireshark, Burp Suite
Development Tools: Linux, Git, AWS, GCP
Binary Analysis Skills: symbolic execution, taint data-flow analysis, sandbox execution, dynamic hooking, forced execution, reverse engineering

Honors & Awards

Research Grants
Bank of America Research Collaboration Funding 2023

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

Teaching Experience

Guest Instructor 02/23
Electrical and Computer Engineering 4117: Introduction to Malware Reverse Engineering
Georgia Institute of Technology Atlanta, GA

Guest Instructor 10/22
Electrical and Computer Engineering 6747: Advanced Topics in Malware Analysis
Georgia Institute of Technology Atlanta, GA

Teaching Assistant 10/18
Electrical and Computer Engineering 385: Digital Systems Laboratory
University of Illinois at Urbana-Champaign Champaign, IL

Teaching Assistant 07/17
Electrical and Computer Engineering 110: Introduction to Electronics (Summer Camp)
University of Illinois at Urbana-Champaign Champaign, IL

Services

Student Assistant
IEEE Secure Development Conference 2021 - 2023

CVE Disclosure
CVE-2022-32530 2022

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