

HAICHUAN XU (KEN)

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

RESEARCH INTERESTS I love large-scale malware analysis and privacy leakage discovery in the Android ecosystem. I also love anti-fraud and forensics research in the banking and blockchain industry.

EDUCATION

Ph.D. in Computer Engineering Cyber Forensics Innovation Laboratory Advisor: Professor Brendan Saltaformaggio Georgia Institute of Technology	08/21 - 05/25 Atlanta, GA
Master of Science in Computer Engineering Georgia Institute of Technology	08/19 - 05/21 Atlanta, GA
Bachelor of Science with Honors in Computer Engineering University of Illinois at Urbana-Champaign	08/15 - 05/19 Champaign, IL

PUBLICATIONS **Peer-Reviewed Articles**

Xu, H., Yao, M., Zhang, R., Dawoud, 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.

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,” To Appear In *45th IEEE Symposium on Security and Privacy (S&P '24)*, San Francisco, CA, May. 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 Georgia Institute of Technology	01/20 - Present Atlanta, GA
--	--------------------------------

1. Digital Wallet Card Binding Fraud Detection. Work In Progress
Collaborating with BoA to prevent ATO and card binding 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. 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.

3. *Ethereum Fraudulent Smart Contract Forensics*. **Accepted – IEEE S&P '24**

Uncovered 2,638,752 ETH (\$2,089,504,682) in illicit profit associated with fraud contracts.
Traced 1,283,198 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*. **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.

5. *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.

6. *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, Machine Learning, Empirical Computer Security, Information Security CTF Lab, Advanced Programming Techniques, Data Structures, Algorithms and Models of Computing		
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 EXPERIENCE	Guest Instructor Electrical and Computer Engineering 4117: Introduction to Malware Reverse Engineering Georgia Institute of Technology	02/23 & 02/24	
	Guest Instructor Electrical and Computer Engineering 6747: Advanced Topics in Malware Analysis Georgia Institute of Technology	10/22	
	Teaching Assistant Electrical and Computer Engineering 385: Digital Systems Laboratory University of Illinois at Urbana-Champaign	10/18	
			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