Runze Zhang

runze.zhang@gatech.edu
runzezhang.me
www.linkedin.com/in/runzezhang1995

Research Interests

My research leverages program analysis, graph theory, and machine learning to tackle large-scale cyber threats. My work spans a broad spectrum of challenges, including global botnet takedowns, mobile malware forensics, smart contract fraud detection, and click fraud mitigation.

Education

Ph.D. in Electrical and Computer Engineering — Jan. 2021 - Present
Georgia Institute of Technology — Atlanta, GA
Cyber Forensics Innovation Laboratory
Advisor: Dr. Brendan Saltaformaggio

M.S. of Cybersecurity — Sep. 2019 - Aug. 2021
Georgia Institute of Technology — Atlanta, GA
GPA: 3.88

B.E. in Electronic and Information Engineering — Sep. 2014 - May 2019
Hong Kong Polytechnic University — Hong Kong SAR, China
Thesis: *Real-time People Detection and Re-identification*
Advisor: Dr. Kin-man Lam
GPA: 3.83

Publications

Peer-Reviewed Top-Tier Security Conferences

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]
NDSS Artifact Evaluation Result: Available, Functional.

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. Acceptance Rate: 17.8% [Open Source]
Media Coverage: [Georgia Tech]

Xu, H., Yao, M., **Zhang, R.**, Moustafa, 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. Acceptance Rate: 18.3% [Open Source]
USENIX Artifact Evaluation Result: Available, Functional.
Media Coverage: [TechRadar][NY Breaking][MSN] [Hypepotamus] [hackerdose] [TechXplore][Sensi Tech Hub] [Georgia Tech][Science of Security] [WizCase] [Hackread] [xatakaen]

Internship Experience

Research Sciences Intern
May. 2023 – Aug. 2023
Microsoft Corporation Redmond, WA

- Designed a deep learning model to detect search requests linked to click fraud for Bing.com.
- Prototyped session-level telemetry data from billions of daily searches and developed a *BERT-LSTM model* to detect click fraud from sessions' query-based semantic and temporal features.
- Analyzed JavaScript click-fraud malware binaries and integrated findings with *TF-IDF* and *entropy-based metrics* to build ground-truth datasets for model training and evaluation.
- Trained and benchmarked the prototype model with SOTA models, achieving 94% accuracy.
- Assessed the system's robustness to adaptive fraud strategies and documented the outcomes.

Application Developer
Jul. 2017 – Jun. 2018
Application Technology Co. Ltd. Hong Kong SAR, China

- Developed a business card scanning IOS app, which combines *OCR* and *NLP* techniques to serialize contact information from card photos and sync with IOS built-in contacts.
- Implemented a *MongoDB-based* business card management system with RSA encryption.
- Built the *facial recognition* feature for a check-in IOS app and launched it to the Apple store.

Research Experience

Graduate Research Assistant
Jan. 2020 - Present
Georgia Institute of Technology Atlanta, GA

Residential Proxy Detection via Network Activity Graphs | *Work In Progress* 2024

- Designed a *Graph Neural Network-based* model to identify residential proxy's IP for click fraud.
- Combined an IP probing framework with statistical analysis methods for ground truth datasets.
- Prototyped undirected graphs to link IPs with different types of network requests, including searches and clicks, and prepared the graph-based features for GNN models.
- Currently aim to perform real-time inference of residential proxy IPs for proactive click fraud detection on search engines. The prototype will be evaluated using Bing.com's real-world data.

Botnet Remediation Via Remote Code Deployment Reuse | *Accepted - NDSS'25* 2024

- Developed a botnet remediation system that utilizes the frontend bot as input, extracting and repurposing its internal remote code deployment routines to run remediation code within bots.
- Developed a formal *graph-based modeling* with *hybrid program analysis* techniques to analyze payload deployment patterns and used *automated code generation* to build remediation code.
- Collaborated with *Netskope* on large-scale testing, successfully removing 523 real-world malware.

Creator Wallets Forensic Behind Smart Contract Fraud | *Published - S&P'24* 2023

- Built a forensic tool to trace fraud networks by analyzing behaviors of deceptive creator wallets.
- Developed a *graph-based model* integrating *symbolic analysis* to identify fraudulent contracts, achieving a 91% accuracy, uncovering 1M+ contracts responsible for 2.6M+ ETH illicit profits.
- Collaborated with *Etherscan*, showing the system's capability in proactively mitigating fraud.

Android Banking Accessibility Malware Analysis. | *Published - USENIX Sec' 24* 2023

- Systematically detecting and modeling the malicious behavior of Android malware abusing accessibility service to steal money from victims' banking apps for illicit profits.
- Utilized *symbolic execution* and *dyanmic force execution* approaches for malware sample forensic, revealing their targetted victims, infection vectors, and anti-analysis techniques.
- Deployed the pipeline on 9,850 malware samples, identifying 59K abuses and 215 targeted apps.

Undergraduate Research Assistant Jun. 2018 - May 2019
Hong Kong Polytechnic University Hong Kong SAR, China

Computer Vision and Image Processing-Related Research Projects. 2019

- Designed an image segmentation algorithm using the *U-Net CNN model* for detecting lung tumors in CT scans, achieving a *top-6 ranking* in the 2018 IEEE Video & Image Processing Cup.
- Built a HOG and CNN-based people detection and re-identification system as my honors project.

Honors & Awards

The Cisco Snort Scholarship 2021
Awarded $10,000 for The 2021 Snort Scholarship.

First Class Honours for Bachelor of Engineering 2019
Awarded First-Class Honours for outstanding Bachelor academic performance.

Hong Kong Polytechnic University Reaching-out Scholarship 2017
Awarded HK $19,000 to support exchange-scholar education at McGill University.

Technical Skill

Machine Learning: Transformers, Sequence Models, Graph Models, Tree-based Models.

Binary Reverse Engineering: Android Apps, JavaScript Web code, and Assembly Binaries.

Program Analysis: FlowDroid, Jadx, Ghidra, Angr, Frida, Wireshark, and IDA Pro.

Programming Languages: Python, Java, JavaScript, C#, C++, and SQL.

Development Tools and Frameworks: PyTorch, TensorFlow, pandas, MongoDB, Cosmos Bigdata platform, Docker, K8s, Kafka, Linux, Git, AWS.

Invited Talks

SkyWalker: Targets the Analysis of Command and Control Services of Botnets
TPCP Software Security Summer School, West Lafayette, IN 2020

Professional Service

Student Assistant
IEEE Secure Development Conference 2023

External Reviewer (Total = 20)

Network and Distributed System Security Symposium (NDSS)	2021 - 2025
IEEE Symposium on Security and Privacy (S&P)	2021 - 2024
USENIX Security Symposium(USENIX)	2021 - 2023
Annual Computer Security Applications Conference (ACSAC)	2020 - 2021
Digital Forensics Research Workshop (DFRWS)	2021-2023
ACM Conference on Computer and Communications Security (CCS)	2020
European Symposium on Research in Computer Security (ESORICS)	2020
International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)	2020

References

Professor Brendan Saltaformaggio
Director of Cyber Forensics Innovation Laboratory
Georgia Institute of Technology
Department of Electrical and Computer Engineering
North Ave NW
Atlanta, GA 30332
(404) 894-8362
brendan@ece.gatech.edu