Tianchang Yang

✉ tzy5088@psu.edu | ☎ 582-203-0606 | 🔗 tianchang-yang.github.io
📍 101 Banffshire Heights, State College, PA 16803

EDUCATION

The Pennsylvania State University **08/2022 - Present**
Ph.D. Candidate, Computer Science *University Park, PA*
Advisor: Dr. Syed Rafiul Hussain Expected 05/2027

Columbia University **08/2019 - 12/2020**
M.S., Computer Science, Computer Security Track *New York, NY*

University of Richmond **08/2015 - 05/2019**
B.S., Double Major in Computer Science and Mathematics *Richmond, VA*
Minor in Business Administration
Honors: Graduation with **Magna Cum Laude**, All A's (Fall 16, Spring 17), Dean's List (Spring 16, Fall 17, Spring 18, Fall 18, Spring 19)

RESEARCH INTEREST

- Systems and Network Security
- Mobile Network Systems
- Machine Learning Security & Privacy
- Program Analysis
- Formal Methods for Security
- Large Language Model

RESEARCH EXPERIENCE

The Pennsylvania State University **08/2022 - Present**
Ph.D. Research Assistant, School of EECS *University Park, PA*
Thesis Topic (Proposed): *Securing 5G and Open RAN System Implementations*

- Designed and implemented a novel testing methodology for Open Radio Access Network (O-RAN) implementations, combining static and dynamic program analysis techniques. This approach uncovers 19 new vulnerabilities in O-RAN implementations, resulting in system crashes, component DoS, messaging delays, and logical errors, with 15 CVE numbers assigned to these findings.
- Designed a formal analysis framework to evaluate access control mechanisms in the 5G core network, identifying six previously unknown vulnerabilities in the 3GPP 5G Technical Specifications that could enable unauthorized access and DoS attacks. Reported the findings to the GSMA Coordinated Vulnerability Disclosure (CVD) Panel of Experts and collaboratively authored a Liaison Statement (LS), which led to multiple revisions in the 3GPP standards.
- Developed a novel *iterative symbolic analysis* algorithm to automate state space exploration in commercial mobile baseband firmware, effectively mitigating path explosion. This approach leads to the discovery of seven exploitable vulnerabilities in basebands used by Galaxy and Pixel devices, several of which were rated High or Critical by vendors.

AT&T Labs **06/2024 - 08/2024, 06/2025 - Present**
Senior Associate Student Research Intern *Bedminster, NJ*

- Developed Large Language Model (LLM)-powered query, reasoning, and coordination capabilities for outage planning for analyzing and coordinating RAN outages to minimize end-user impact, supporting critical projects such as the Nokia-to-Ericsson network equipment swap.
- Facilitated efficient outage planning across all 12 U.S. markets, benefiting over 1,200 outage submitters and approvers, and coordinating 16,000+ yearly planned outages.

- Analyzed cell site provisioning data from over 1.6 million RAN sites nationwide, applying predictive models to validate cell configurations. The models uncovered misconfigured sites previously undetected by existing rule-based validations, improving network performance and reliability.

University of Richmond **05/2017 - 07/2017**
Summer Research Fellowship, Department of Math and Science *Richmond, VA*

- Received fellowship grant to investigate bird image classification using deep learning techniques (the BirdID Project) with Dr. Lewis Barnett.
- Researched on different image augmentation techniques and neural network designs. The resulting CNN implementation using Lasagne with Theano can achieve an accuracy of 85% - 97%.
- Built an R-based automated tool for the second Virginia Breeding Bird Atlas (VABBA2) project to detect unusual bird breeding activities from large-scale user reports using pattern recognition.

INDUSTRY EXPERIENCE

Tencent Holdings Ltd. **04/2021 - 05/2022**
Backend Engineer, Tencent Video *Shenzhen, CN*

- Provided reliable live streaming services to up to 6 million concurrent viewers and a peak QPS of 100,000 per live stream in Tencent Video, the second largest streaming service provider in China.
- Led the development of data management, live stream creation/deletion, stream audition, and monitoring systems on Tencent Video's new iteration of live-stream management system.
- Engaged in iterative and incremental development of new features, participated in maintaining and monitoring large-scale live streams like the LoL S11 finals, NBA games, Tokyo Olympics, etc.

Wangsu Science & Technology **05/2018 - 07/2018**
Security R&D Research Intern *Beijing, CN*

- Researched identification and defense techniques against DDoS attacks on the transport layer of network communication in Wangsu, a leading information infrastructure platform service provider.
- Developed automated software to identify DDoS attack patterns by inspecting packets' header and searching for suspicious patterns and known signatures in the payload. The software automatically clusters payload and extracts signatures from known attacking packets.

PUBLICATION

- Yilu Dong, **Tianchang Yang**, Abdullah Al Ishtiaq, Syed Md Mukit Rashid, Ali Ranjbar, Kai Tu, Tianwei Wu, Md Sultan Mahmud, Syed Rafiul Hussain. CoreCrisis: Threat-Guided and Context-Aware Iterative Learning and Fuzzing of 5G Core Networks. *USENIX Security Symposium (USENIX Security), 2025.*
- Ali Ranjbar, **Tianchang Yang**, Kai Tu, Saaman Khalilollahi, Syed Rafiul Hussain. Stateful Analysis and Fuzzing of Commercial Baseband Firmware. *IEEE Symposium on Security and Privacy (SP), 2025.*
- **Tianchang Yang**, Sathiyajith K S, Ashwin Senthil Arumugam, Syed Rafiul Hussain. Feedback-Guided API Fuzzing of 5G Network. *Workshop on Security and Privacy of Next-Generation Networks (FutureG), 2025.*
- **Tianchang Yang**, Syed Md Mukit Rashid, Ali Ranjbar, Gang Tan, Syed Rafiul Hussain. ORANalyst: Systematic Testing Framework for Open RAN Implementations. *USENIX Security Symposium (USENIX Security), 2024.*
- Mujtahid Akon, **Tianchang Yang**, Yilu Dong, Syed Rafiul Hussain. Formal Analysis of Access Control Mechanism of 5G Core Network. *The ACM Conference on Computer and Communications Security (CCS), 2023*

REPORTED VULNERABILITY

- **19 new vulnerabilities in O-RAN-SC and SD-RAN implementations of Open RAN.** CVE-2024-25377, CVE-2024-29420, CVE-2024-34043, CVE-2024-34044, CVE-2024-34045, CVE2024-34046, CVE-2024-34047, CVE-2024-34048, CVE-2023-52724, CVE-2023-52725, CVE-2023-52726, CVE-2023-52727, CVE-2023-52728, CVE-2024-34049, CVE-2024-34050
- **Vulnerabilities discovered in commercial 5G basebands.** CVE-2024-52923, CVE-2024-52924, CVE-2025-26784, CVE-2025-26785, CVE-2025-27891. Acknowledgements:`https://semiconductor.samsung.com/support/quality-support/product-security-updates/`.
  Awarded $29,250 for reporting 1 Critical- and 2 High-severity vulnerabilities in Pixel phones, Google Bug Bounty (2025). Awarded $10,712 for reporting 2 High- and 3 Medium-severity vulnerabilities in Galaxy phones, Samsung Bug Bounty (2025).
- **6 new vulnerabilities in the access control mechanism of the 5G core network in 3GPP Technical Specifications.** CVD-2023-0069: GSMA Mobile security research acknowledgment. `https://www.gsma.com/solutions-and-impact/technologies/security/gsma-mobile-security-research-acknowledgements/`. These discoveries resulted in several critical changes (totaling 279 words in TS 33.501) in the 5G standards: `https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_116_Jeju/Docs/S3-242453.zip`.
- **14 new vulnerabilities in 5G Core Network implementations (Open5GS, free5GC, OpenAirInterface 5G).** CVE-2024-34476, CVE-2024-34475, CVE-2024-33232, CVE-2024-22728, CVE-2024-31838, CVE-2024-33236, CVE-2024-33241, CVE-2024-33233
- **4 new vulnerabilities in 5G Core Network Discovered Through API Fuzzing (free5GC, Aether SD-Core).** CVE-2024-41233, CVE-2024-42866
- **Vulnerabilities in the implementation of functionally split open 5G RAN (OpenAirInterface).** CVE-2024-57330, CVE-2024-57331, CVE-2024-57332, CVE-2024-57333, CVE-2024-57334, CVE-2025-45420, CVE-2025-45421

TALK

- Uncovering 'NASty' 5G Baseband Vulnerabilities through Dependency-Aware Fuzzing
  ▷ *Black Hat USA 2025*
- Feedback-Guided API Fuzzing of 5G Network
  ▷ *Workshop on Security and Privacy of Next-Generation Networks (FutureG) 2025*
- ORANalyst: Systematic Testing Framework for Open RAN Implementations
  ▷ *USENIX Security Symposium 2024*

SOFTWARE ARTIFACT FROM RESEARCH

- **Loris (2025):** Stateful fuzz testing and emulation framework designed to explore and analyze commercial 5G baseband firmware.
  https://github.com/SyNSec-den/Loris
- **ORANalyst (2024):** Systematic testing framework designed for O-RAN's RAN Intelligent Controller (RIC) implementations, combining program analysis with dynamic program testing.
  https://github.com/SyNSec-den/ORANalyst
- **5GCVerif (2023):** Model-based testing framework devised from 3GPP 5G Technical Specifications Release 17 to formally analyze the design of access control framework of the 5G Core.
  https://github.com/SyNSec-den/5GCVerif

TEACHING EXPERIENCE

The Pennsylvania State University **08/2022 - 12/2022**
Teaching Assistant, School of EECS (Discrete Math for Comp-Sci) *University Park, PA*

- Developed and conducted weekly recitations for a group of over 50 students.
- Designed course materials such as quizzes and exams for a class of over 200 students.

University of Richmond **09/2017 - 05/2019**
Peer Tutor, Academic Skills Center *Richmond, VA*

- Assisted over 30 tutees in grasping concepts and gaining skills in Computer Science (Algorithms, Data Structure), Math (Linear Algebra, Real Analysis, Statistics), and Accounting.
- Evaluated each tutee's academic profile, pinpointing strengths and areas for improvement. Provided tailored guidance to foster tutees' independent study habits and critical thinking skills.

ACTIVITY

ICPC North America Regional 2018 **11/2018**

- Received honorable mention at 2018 ACM-ICPC Mid-Atlantic Region Christopher Newport site.

Intramural Basketball **09/2015 - 05/2019**

- Competed in in-school and inter-school matches, finished top four in intramural tournament.

SKILL

Programming:	C/C++, Python, Go, Java, R, SQL, MATLAB, Wolfram Mathematica
Languages:	English (fluent), Chinese (native)

RELEVANT COURSE

- Computer Communication Networks
- Program Analysis
- Malware Analysis & Reverse Engineer
- Intrusion Detection Systems
- Analysis of Algorithms
- Natural Language Processing
- Design/Implementation Prog. Lang.
- Wireless/Mobile Sensing IoT