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. Student, Computer Science *University Park, PA*
Advisor: Dr. Syed Rafiul Hussain Expected 05/2026

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
- Software Security
- Formal Methods for Security

RESEARCH EXPERIENCE

The Pennsylvania State University **08/2022 - Present**
Ph.D. Research Assistant, School of EECS *University Park, PA*

- Developed a formal analysis framework to assess the access control mechanisms of the 5G core network, uncovering six new vulnerabilities from 3GPP 5G Technical Specifications, potentially leading to unauthorized access and DoS attacks.
- Reported the identified vulnerabilities to the GSMA CVD Panel of Experts (PoE) and collaboratively drafted a Liaison Statement (LS) proposing revisions to the 3GPP 5G Technical Specifications to mitigate the security flaws.
- Conducted in-depth analysis of Open Radio Access Network (O-RAN) and developed testbeds using open-source implementations, enabling end-to-end testing and verification of O-RAN.
- Designed and implemented a novel testing methodology for O-RAN implementations and similar microservice-architecture systems, combining static and dynamic program analysis techniques.
- This grammar-guided end-to-end stochastic testing approach uncovers 19 new vulnerabilities in O-RAN software, resulting in system crashes, component DoS, messaging delays, and logical errors, with 15 CVE numbers assigned to these findings.

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

- Developed Large Language Model (LLM)-powered functionalities and chatbots for analyzing and coordinating RAN outages to minimize user impact, supporting critical projects such as the Nokia-to-Ericsson network equipment swap.
- Enabled natural language-based query, reasoning, and coordination capabilities for outage planning by integrating data from various sources, including planned outages, cell site coverage, site priority, special events, and traffic profiles.
- 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 and configuration data from over 1.6 million RAN sites nationwide, applying predictive models to verify the accuracy and validity of cell configurations.
- The resulting predictive models identified misconfigured sites previously undetected by rule-based validation checks, enhancing overall 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. Depending on the quantity of images per species and the overall number of categories, my CNN implementation written in Python using Lasagne with Theano can achieve an accuracy between 85% - 97% in differentiating bird images.
- Developed an automated tool in R language for the second Virginia Breeding Bird Atlas (VABBA2) project to identify unusual bird breeding activities from massive user-reported data using pattern recognition techniques.

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, stream audition, stream task creation/deletion, and monitoring systems on Shenzhou Console, 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.
- Contributed to various other systems, including the digital wallet and live feed recommendation.

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 both inspecting the packets' header and searching for suspicious patterns and known signatures in the payload portion based on the underlying packet protocol. The software automatically clusters payload and extracts signatures from known attacking packets.
- The division is still updating and utilizing the tool I developed for the preliminary analysis of suspicious packets.

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 to assess students' performance.
- Graded exams and held weekly office hours 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.

PUBLICATION

- **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*

SOFTWARE ARTIFACT FROM RESEARCH

- **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

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
- **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

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