Yilu Dong

+1-8147317003 | yiludong@psu.edu | yilud.me | Yilu Dong | NaivEPoi
801 Toftrees Ave, 456, State College, PA, 16803

Research Interests

Systems Security, Communication Protocols Security, Software Testing, Applied Cryptography

Education

- **The Pennsylvania State University** *01/2024 - present*
  Ph.D. student in Computer Science and Engineering University Park, PA
  - Advisor: Dr. Syed Rafiul Hussain
- **The Pennsylvania State University** *08/2021 - 08/2023*
  M.S. in Computer Science and Engineering University Park, PA
  - Advisor: Dr. Syed Rafiul Hussain
  - Thesis: Deviant Behavior Analysis of 5G Core Network Implementations
- **The Pennsylvania State University** *08/2017 - 05/2021*
  B.S. in Computer Science University Park, PA
  Minor in Cybersecurity Computational Foundations, Computer Engineering, Statistics, and Mathematics Application
  - Dean's List (Fall 18, Spring 19, Fall 19, Spring 20, Fall 20, Spring 21)

Teaching Experience

- **The Pennsylvania State University** *08/2022 - 05/2023, 01/2024 - 05/2024*
  Teaching Assistant (CMPSC 461: Programming Language Concepts) University Park, PA
  - Prepared questions for assignments and exams for a class of over 250 students.
  - Held weekly office hours to help students with concepts and assignments.
- **The Pennsylvania State University** *01/2022 - 05/2022*
  Learning Assistant (CSE 543: Computer Security) University Park, PA
  - Designed graduate-level course projects, including cryptography and web security topics.
  - Held weekly office hours and graded assignments.
- **The Pennsylvania State University** *08/2020 - 12/2020*
  Grader (CMPSC 465: Data Structures and Algorithms) University Park, PA
  - Graded assignments and exams for a class of over 200 students.

Industry Experience

- **CableLabs** *05/2022 - 08/2022*
  5G Security Intern Louisville, CO
  - Deployed a test 5G SA network in the lab using SDRs (USRP B210, N310) and open-source implementation.
  - Modified the OpenAirInterface code to develop a demo PKI solution to prevent fake base station attacks.
  - Built a SIB message relay to evaluate our solution against potential relay attacks.
- **GE Healthcare** *05/2019 - 08/2019*
  Intern Engineer Shanghai, China
  - Designed a program to provide production data to the new Kanban system.
  - Developed a web-based document management system using Spring and MySQL.

Publications

C=Conference, J=Journal

[C6] Yilu Dong, Tao Wan, Tianwei Wu, Syed Rafiul Hussain. **Evaluating Time-Bounded Defense Against RRC Relay in 5G Broadcast Messages**. In *the 18th ACM Conference on Security and Privacy in Wireless and Mobile Networks* ***(WiSec)***, 2025.

[C5] 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**. In *the 34th USENIX Security Symposium* ***(USENIX Security)***, 2025.

[C4] Syed Md Mukit Rashid, Tianwei Wu, Kai Tu, Abdullah Al Ishtiaq, Ridwanul Hasan Tanvir, Yilu Dong, Omar Chowdhury, Syed Rafiul Hussain. **State Machine Mutation-based Testing Framework for Wireless Communication Protocols**. In *the 2024 ACM SIGSAC Conference on Computer and Communications Security* ***(CCS)***, 2024.

[C3] Rabiah Alnashwan, Yang Yang, Yilu Dong, Prosanta Gope, Behzad Abdolmaleki, Syed Rafiul Hussain. **Strong Privacy-Preserving Universally Composable AKA Protocol with Seamless Handover Support for Mobile Virtual Network Operator**. In *the 2024 ACM SIGSAC Conference on Computer and Communications Security **(CCS)***, 2024.

[C2] Kai Tu, Abdullah Al Ishtiaq, Syed Md Mukit Rashid, Yilu Dong, Weixuan Wang, Tianwei Wu, Syed Rafiul Hussain. **Logic Gone Astray: A Security Analysis Framework for the Control Plane Protocols of 5G Basebands**. In *the 33rd USENIX Security Symposium **(USENIX Security)***, 2024. Distinguished Paper Award

[C1] Mujtahid Akon, Tianchang Yang, Yilu Dong, Syed Rafiul Hussain. **Formal Analysis of Access Control Mechanism of 5G Core Network**. In *the 2023 ACM SIGSAC Conference on Computer and Communications Security **(CCS)***, 2023.

Presentations

- **Cracking the 5G Fortress: Peering Into 5G's Vulnerability Abyss** *08/2024*
  BlackHat USA Briefing Las Vegas, NV

Reported Vulnerabilities

- **8 Vulnerabilities in 5G Core Implementations:** CVE-2024-31838, CVE-2024-22728, CVE-2024-33232, CVE-2024-33233, CVE-2024-33236, CVE-2024-33241, CVE-2024-34475, CVE-2024-34476
- **1 Vulnerability in LTE Device:** CVE-2024-32911
- **3 Vulnerabilities in BLE devices:** CVE-2024-20889, CVE-2024-20890, CVE-2024-291554
- **12 Vulnerabilities in 5G commercial baseband:** CVE-2024-28818, CVE-2024-29152, CVE-2023-49927, CVE-2023-49928, CVE-2023-50803, CVE-2023-50804, CVE-2023-52341, CVE-2023-52342, CVE-2023-52343,CVE-2023-52344, CVE-2023-52533, CVE-2023-52534
- **GSMA CVDs:** CVD-2023-0069, CVD-2023-0081

Honors and Awards

- **Best AI Application Built with Cloudflare** *2024*
  HackPSU Fall 2024
  - Used LLM to provide interest points of a city specified by a user.
  - Built the web application using Flask and React with TypeScript.
- **Distinguished Paper Award** *2024*
  the 33rd USENIX Security Symposium
  - Logic Gone Astray: A Security Analysis Framework for the Control Plane Protocols of 5G Basebands **[C2]**.
- **Bug Bounty Reward** *2024*
  Samsung
  - $5,700 for reporting several vulnerabilities in 5G implementation **[C2]**.
  - $2,800 for reporting moderate severity vulnerabilities in BLE **[C4]**.
  - Inducted 6 times in Samsung Product Security Update.
- **Bug Bounty Reward** *2024*
  Google
  - $14,250 for high severity vulnerabilities in 5G implementation **[C2]**.
- **Product Security Acknowledgments** *2024*
  Unisoc
  - Inducted 2 times for identifying security issues in 5G Implementations **[C2]**.
- **Mobile Security Research Acknowledgments** *2023, 2024*
  GSMA
  - Inducted 2 times in the GSMA Mobile Security Research Acknowledgements (formerly known as Hall of Fame) for identifying security and privacy issues in 5G networks **[C1, C2]**.
- **KCF - Hack the Waiting Room Challenge** *2018*
  HackPSU Fall 2018
  - Composed sensor data to measure how many people are in a room. Built from scratch in 24 hours.
  - Acted as a major contributor in a 4-person team with no previous experience with Arduino.

Professional Services

- **Program Committee Member**
  - USENIX Security Symposium Artifact Evaluation **(USENIX Security AE)**: 2025
- **Journal Review**
  - IEEE Transactions on Information Forensics and Security **(TIFS)**
- **External Reviewer**
  - IEEE Symposium on Security and Privacy **(SP)**: 2025
  - IEEE International Conference on Distributed Computing Systems **(ICDCS)**: 2025

Software Artifacts from Research

- **CoreCrisis (2025):** A stateful and grammar-aware fuzzing framework for 5G core network.
- **5GBaseChecker (2024):** An automated and scalable security testing framework for 5G basebands.
- **5GCVerif (2023):** A model-based testing framework designed to formally analyze the access control framework of the 5G Core.

Contributions to Open-Source Projects

- **Open5GS**
  - Report a few vulnerabilities that cause AMF or SMF to crash.
- **free5GC**
  - Report and fix a few vulnerabilities that cause AMF or SMF to crash.
- **UERANSIM**
  - Report and fix a vulnerability that causes UE to crash.
- **Magma**
  - Report and fix a few vulnerabilities that cause AMF to crash.
- **OpenAirInterface CN5G**
  - Report a few vulnerabilities that cause AMF to crash.

Skills

- **Programming Languages:** C, C++, Python, Java, Kotlin, R, Go, Scheme, Rust
- **Web Technologies:** Flask, React.js, Nginx, REST API, JavaScript, TypeScript
- **Other Software and Tools:** Docker, Git, Bash, Wireshark, GDB, OpenSSL, SQL, MongoDB, NumPy, Pandas, protobuf
- **5G-Related Software Stack:** srsRAN, OpenAirInterface, free5GC, Open5GS, UERANSIM, Magma, asn1c
- **Languages:** English (professional), Chinese (native), Japanese (Elementary)