Syed Rafiul Hussain

Contact Information

Charles K. Etner Early Career Assistant Professor
Dept. of Computer Science & Engineering
School of Electrical Eng. and Computer Science
The Pennsylvania State University
University Park, PA 16803

W305 Westgate Building
+1 814-865-6454
hussain1@psu.edu
https://syed-rafiul-hussain.github.io
https://synsec-den.github.io

Research Interests

Network and Systems Security, Formal Methods, Automated Reasoning, Program Analysis.

Education

Purdue University — Fall 2018
Ph.D. in Computer Science
Thesis: *A Systematic Framework for Analyzing the Security and Privacy of Cellular Networks.*
Advisor: Elisa Bertino

North Carolina State University — Spring 2013
Master in Computer Science
Supervisor: Peng Ning

Bangladesh University of Engineering and Technology (BUET) — Spring 2009
B.Sc. in Computer Science and Engineering
Supervisor: Ashikur Rahman

Employment

Assistant Professor — Fall 2020 - Present
Computer Science and Engineering, Pennsylvania State University

Postdoctoral Researcher — Spring 2019 - Summer 2020
Purdue University, Hosts: Elisa Bertino and *Ninghui Li*

Research Assistant — Fall 2013 - Fall 2018
Purdue University, Supervisor: Elisa Bertino

Research Associate Intern — Summer 2015, Summer 2016
Hewlett-Packard Labs, Mentors: Shahriar Nirjon, Shruti Sanadhya, Manager: Kyu-Han Kim

Research Assistant — Summer 2012 - Spring 2013
North Carolina State University, Supervisor: Peng Ning

Honors and Awards

2024	Distinguished Paper Award at USENIX Security Symposium 2024
2024	Distinguished Member of INFOCOM 2024 TPC
2023	Charles K. Etner Early Career Professorship by Penn State
2022	National Science Foundation CAREER Award
2022	DARPA Young Faculty Award
2022	Selected as a DARPA Riser
2019-2024	Inducted to the Mobile Security Research Hall of Fame by GSMA for identifying and fixing security and privacy flaws in 4G and 5G networks
2021	Best Paper Award Nomination, ICDCS '21
2019	Best Paper Award, ACSAC '19
2019	Distinguished Paper Award Honorable Mention, NDSS'19
2019	Awarded $10K as research gift by Qualcomm for evaluating their modems
2017	Nominated for the Best Paper Award, ACM SIGBED EWSN'17
2017	Intel Security Research Assistantship award for Spring 2017

Last updated: August 26, 2024

2016 IEEE Symposium on Security & Privacy travel grant award.
2015 CERIAS Symposium Best Poster Award (runner up).

Grants

❍ **A Holistic Cybersecurity Testing Framework for 5G Radio Access Networks**
Sponsor: **National Telecommunications and Information Administration (NTIA)**
Role: PI
Total Amount: $2,000,000
Penn State Amount: $476,375
Duration: 2024-2026

❍ **NSF Convergence Accelerator Track G (Phase 2): Combating Vulnerability and Unawareness in 5G Network Security: Signaling and Full-Stack Approach**
Sponsor: **National Science Foundation (NSF)/Department of Defense (DoD)**
Role: PI
Total Amount: $5,000,000
Penn State Amount: $443,557
Duration: 2023-2025

❍ **NSF Convergence Accelerator Track G (Phase 1): Combating Vulnerability and Unawareness in 5G Network Security: Signaling and Full-Stack Approach**
Sponsor: **National Science Foundation (NSF)/Department of Defense (DoD)**
Role: PI
Total Amount: $750,000
Penn State Amount: $60,000
Duration: 2022-2023

❍ **Collaborative Research: CNS Core: Large: Systems and Verifiable Metrics for Sustainable Data Centers**
Sponsor: **National Science Foundation (NSF) CNS Large**
Role: PI
Total Amount: $666,385
Penn State Amount: $206,598
Duration: 2022-2026

❍ **NSF CAREER: Principled Approaches to Securing Next Generation Cellular Networks**
Sponsor: **National Science Foundation (NSF) SaTC**
Role: PI (Sole)
Total Amount: $557,183
Duration: 2022-2027

❍ **DARPA Young Faculty Award (YFA):Automated Reasoning and Repairing Framework for Systematic Assurance of 5G RAN Systems**
Sponsor: **Defense Advanced Research Projects Agency (DARPA)**
Role: PI (Sole)
Total Amount: $500,000 (Option: $500,000 requested)
Duration: 2022-2024

❍ **Adoption of "Smart" Agricultural Irrigation Systems: Assessing and Mitigating Cybersecurity Threats to U.S. Food, Water, And Energy Reserve**
Sponsor: **Penn State Center for Security Research and Education Fall (CSRE)**
Role: Co-PI
Total Amount: $30,000

My Share: $10,000
Duration: 2022

❍ **Principled Security Analysis of Intel's Bluetooth Implementation**
Sponsor: **Intel Corporation**
Role: PI
My Share: $27,000
Duration: 2020

Conference Publications

[C30] Syed Md Mukit Rashid, Tianwei Wu, Kai Tu, Abdullah Al Ishtiaq, Ridwanul Hasan Tanvir, Yilu Dong, Omar Chowdhury, and Syed Rafiul Hussain, **State Machine Mutation-based Testing Framework for Wireless Communication Protocols**, *The ACM Conference on Computer and Communications Security **(CCS), 2024***.

[C29] Rabiah Alnashwan, Yang Yang, Yilu Dong, Prosanta Gope, Behzad Abdolmaleki, and Syed Rafiul Hussain, **Strong Privacy-Preserving Universally Composable AKA Protocol with Seamless Handover Support for Mobile Virtual Network Operator**, *The ACM Conference on Computer and Communications Security **(CCS), 2024***.

[C28] Tianchang Yang, Syed Md Mukit Rashid, Gang Tan, and Syed Rafiul Hussain, **ORANalyst: Systematic Testing Framework for Open RAN Implementations**, *USENIX Security Symposium **(USENIX Security), 2024***.

[C27] Feiyang Yu , Quan Zhou, Syed Rafiul Hussain, Danfeng Zhang, **Athena: Analyzing and Quantifying Side Channels of Transport Layer Protocols**, *USENIX Security Symposium **(USENIX Security), 2024***.

[C26] Kai Tu, Abdullah Al Ishtiaq, Syed Md Mukit Rashid Yilu Dong, Weixuan Wang, Tianwei Wu, and Syed Rafiul Hussain, **Logic Gone Astray: A Security Analysis Framework for the Control Plane Protocols of 5G Basebands**, *USENIX Security Symposium **(USENIX Security), 2024***.
✪ **Distinguished Paper Award**

[C25] Abdullah Al Ishtiaq, Sarkar Snigdha Sarathi Das, Syed Md Mukit Rashid, Ali Ranjbar, Kai Tu Tianwei Wu, Zhezheng Song, Weixuan Wang, Mujtahid Al-Islam Akon Rui Zhang, and Syed Rafiul Hussain. **Hermes: Unlocking Security Analysis Of Cellular Network Protocols By Synthesizing Finite State Machines From Natural Language Specifications**, *USENIX Security Symposium **(USENIX Security), 2024***.

[C24] Raja Hasnain Anwar, Syed Rafiul Hussain, Muhammad Taqi Raza, **In Wallet We Trust: Bypassing the Digital Wallets Payment Security for Free Shopping**, *USENIX Security Symposium **(USENIX Security), 2024***.

[C23] Mujtahid Akon, Tianchang Yang, Yilu Dong, and Syed Rafiul Hussain, **Formal Analysis of Access Control Mechanism of 5G Core Network**, *The ACM Conference on Computer and Communications Security **(CCS), 2023***.

[C22] Imtiaz Karim, Abdullah Ishtiaq, Syed Rafiul Hussain, and Elisa Bertino, **BLEDiff: Scalable and Property-Agnostic Noncompliance Checking for BLE Implementations**, *IEEE Symposium on Security and Privacy **(IEEE S&P), 2023***.

[C21] Yohan Beugin, Quinn Burke, Blaine Hoak, Ryan Sheatsley, Eric Pauley, Gang Tan, Syed Rafiul Hussain, and Patrick McDaniel, **Building a Privacy-Preserving Smart Camera System**, *Privacy Enhancing Technologies **(PETS), 2022***.

[C20] Syed Rafiul Hussain, Imtiaz Karim, Abdullah Ishtiaq, Omar Chowdhury, and Elisa Bertino, **Non-**

compliance as Deviant Behavior: An Automated Black-box Noncompliance Checker for 4G LTE Cellular Devices, *The 28th ACM Conference on Computer and Communications Security **(CCS), 2021***.

[C19] Imtiaz Karim, Syed Rafiul Hussain, and Elisa Bertino, **ProChecker: An Automated Security and Privacy Analysis Framework for Communication Protocol Implementations**, *The 41st IEEE International Conference on Distributed Computing Systems **(ICDCS), 2021***.
✪ **Best Paper Award Nomination**

[C18] Ankush Singla, Rouzbeh Behnia, Syed Rafiul Hussain, Atilla Yavuz, and Elisa Bertino, **Look Before You Leap: Secure Connection Bootstrapping for 5G Networks to Defend Against Fake Base-Stations**, *The 16th ACM ASIA Conference on Computer and Communications Security **(AsiaCCS), 2021***.

[C17] Mitziu Echeverria, Zeeshan Ahmed , Bincheng Wang , M. Fareed Arif , Syed Rafiul Hussain, and Omar Chowdhury, **PHOENIX: Device-Centric Cellular Network Protocol Monitoring using Runtime Verification**, *The 28th Network and Distributed Systems Security **(NDSS), 2021***.

[C16] Moosa Yahyazadeh, Syed Rafiul Hussain, Endadul Hoque, and Omar Chowdhury, **PatrIoT: Policy Assisted Resilient Programmable IoT System**, *20th International Conference on Runtime Verification **(RV), 2020***.

[C15] Weicheng Wang, Fabrizio Cicala, Syed Rafiul Hussain, Ninghui Li, and Elisa Bertino, **Analyzing the Attack Landscape of Zigbee-enabled IoT System sand Reinstating Users' Privacy**, *13th ACM Conference on Security and Privacy in Wireless and Mobile Networks **(WiSec), 2020***.

[C14] Ankush Singla, Syed Rafiul Hussain, Omar Chowdhury, Ninghui Li, and Elisa Bertino, **Protecting the 4G and 5G Cellular Paging Protocols against Security and Privacy Attacks**, *The 20th Privacy Enhancing Technologies Symposium **(PETS), 2020***.

[C13] Elisa Bertino, Syed Rafiul Hussain, and Omar Chowdhury, **5G Security and Privacy: A Research Roadmap**, *Computing Community Consortium **(CCC), 2020***.

[C12] Syed Rafiul Hussain, Mitziu Echeverria, Imtiaz Karim, Omar Chowdhury, and Elisa Bertino, **5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol**, *The 26th ACM Conference on Computer and Communications Security ((**CCS), 2019***.

[C11] Imtiaz Karim, Fabrizio Cicala, Syed Rafiul Hussain, Omar Chowdhury, and Elisa Bertino, **Opening Pandora's Box through ATFuzzer: Dynamic Analysis of AT Interface for Android Smartphones**, *The 35th Annual Computer Security Applications Conference **(ACSAC), 2019***.
✪ **Distinguished Paper Award**

[C10] Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, and Elisa Bertino, **Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information**, *The 26th Network and Distributed Systems Security **(NDSS), 2019***.
✪ **Distinguished Paper Award Honorable Mention**

[C9] Syed Rafiul Hussain, Mitziu Echeverria, Ankush Singla, Omar Chowdhury, and Elisa Bertino, **Insecure Connection Bootstrapping in Cellular Networks: The Root of All Evil**, *The 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks **(WiSec), 2019***. (This work has been discussed by FCC in the *Managing Security Risk in the Transition to 5G* working group.)

[C8] Syed Rafiul Hussain, Shahriar Nirjon, and Elisa Bertino, **Securing the Insecure Link of Internet-of-Things Using Next-Generation Smart Gateways**, *The 15th IEEE International Conference on Distributed Computing in Sensor Systems **(DCOSS), 2019***.

[C7] Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino, **LTEInspector:**

A Systematic Approach for Adversarial Testing of 4G LTE, *The 25th Network and Distributed Systems Security* ***(NDSS), 2018***. (This work has been discussed by FCC in the *Managing Security Risk in the Transition to 5G* working group

[C6] Syed Rafiul Hussain, Shagufta Mehnaz, Shahriar Nirjon, and Elisa Bertino, **SeamBlue: Seamless Bluetooth Low Energy Connection Migration for Unmodified IoT Devices**, *The 14th ACM SIGBED International Conference on Embedded Wireless Systems and Networks* ***(EWSN), 2017***. **(✪ Nominated for the Best Paper Award)**

[C5] Syed Rafiul Hussain, Asmaa Sallam, and Elisa Bertino, **DetAnom: Detecting Anomalous Database Transactions by Insiders**, *The 5th ACM Conference on Data and Application Security and Privacy* ***(CODASPY), 2015***.

[C4] Syed Rafiul Hussain, Changda Wang, Salmin Sultana, and Elisa Bertino, Secure Data Provenance Compression Using Arithmetic Coding in Wireless Sensor Networks, *The 33rd IEEE International Performance Computing and Communications Conference* ***(IPCCC), 2014***.

[C3] Syed Rafiul Hussain, Ala Odeh, Amrut Shivakumar, Shalini Chauhan, and Khaled Harfoush. **Real-time Traffic Congestion Management and Deadlock Avoidance for Vehicular Ad Hoc Networks**, *The 10th IEEE High Capacity Optical Networks and Emerging/Enabling Tech.* ***(HONET-CNS), 2013***.

[C2] Subrata Saha, Syed Rafiul Hussain, and Ashikur Rahman, **RBP: Reliable Broadcasting Protocol in Large Scale Mobile Ad Hoc Networks**, *The 24th IEEE International Conference on Advanced Information Networking and Applications* ***(AINA), 2010***.

[C1] Syed Rafiul Hussain, Subrata Saha, and Ashikur Rahman, **An Efficient and Scalable Address Autoconfiguration in Mobile Ad Hoc Networks**, *The 8th International Conference on Ad Hoc Networks and Wireless* ***(ADHOC-NOW), 2009***.

Industrial Conference

[I4] Kai Tu, Abdullah Al Ishtiaq, Syed Md Mukit Rashid Yilu Dong, Weixuan Wang, Tianwei Wu, and Syed Rafiul Hussain, **Cracking the 5G Fortress: Peering Into 5G's Vulnerability Abyss**, ***Black-Hat USA 2024***.

[I3] Syed Rafiul Hussain BaseDiff: Differential Security Analysis of Cellular Basebands ***Qualcomm Security Summit 2022***.

[I2] Syed Rafiul Hussain, Side Channel Attacks in 4G and 5G Cellular Networks, ***The Black Hat Europe, London, UK, 2019***.

[I1] Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino, LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE, ***Qualcomm Security Summit 2018***.

Journal Publications

[J7] Anshul Gandhi, Kanad Ghose, Kartik Gopalan, Syed Rafiul Hussain, Dongyoon Lee, David Liu, Zhenhua Liu, Patrick McDaniel, Shuai Mu and Erez Zadok, **Metrics for Sustainability in Data Centers**, *ACM SIGEnergy Energy Informatics Review*, Volume 3, Issue 3, pp 40–46, 2023.

[J6] Imtiaz Karim, Fabrizio Cicala, Syed Rafiul Hussain, Omar Chowdhury, and Elisa Bertino, **AT-Fuzzer: Dynamic Analysis Framework of AT Interface for Android Smartphones**, *ACM Digital Threats: Research and Practice (****DTRAP****), 2020.*

[J5] Syed Rafiul Hussain, Shagufta Mehnaz, Shahriar Nirjon, and Elisa Bertino, **Secure Seamless Bluetooth Low Energy Connection Migration for Unmodified IoT Devices**, *IEEE Transaction on Mobile Computing* ***(TMC)****, 2018.*

[J4] Lorenzo Bossi, Elisa Bertino, Syed Rafiul Hussain, **A System for Profiling and Monitoring Database Access Patterns by Application Programs for Anomaly Detection**, *IEEE Transaction on Software Engineering (**TSE**), 2017.*

[J3] Asmaa Sallam, Elisa Bertino, Syed Rafiul Hussain, David Landers, R. Michael Lefler, and Donal Steiner, **DBSAFE - An Anomaly Detection System to Protect Databases from Exfiltration Attempts**, *IEEE Systems Journal, 2015.*

[J2] Syed Rafiul Hussain[†], Changda Wang[†], and Elisa Bertino, **Dictionary Based Secure Provenance Compression for Wireless Sensor Networks**, *IEEE Transaction on Parallel and Distributed Systems (**TPDS**), 2014.* ([†] indicates equal contribution)

[J1] Syed Rafiul Hussain, Subrata Saha, and Ashikur Rahman, **SAAMAN: Scalable Address Autoconfiguration in Mobile Ad Hoc Networks**, *Journal of Network and System Management (**JNSM**), Springer, 2011.*

Patents

[PA2] Syed Rafiul Hussain, and Kyu-Han Kim, **Mobile Virtual Private Network Configuration**, *US Patent App. 16/070,948, 2019.*

[PA1] Syed Rafiul Hussain, Shruti Sanadhya, and Kyu-Han Kim, **Deterrence of User Equipment Device Location Tracking**, *US Patent App. 15/369,508 and 10/154,369, 2018.*

Magazine Publications

[M1] Syed Rafiul Hussain, Patrick McDaniel, Anshul Gandhi, Kanad Ghose, Kartik Gopalan, , Dongyoon Lee, David Liu, Zhenhua Liu, Shuai Mu and Erez Zadok, **Verifiable Sustainability in Data Centers**, *IEEE Security & Privacy, 2024.*

Workshop Publications

[W1] Anshul Gandhi, Kanad Ghose, Kartik Gopalan, Syed Rafiul Hussain, Dongyoon Lee, David Liu, Zhenhua Liu, Patrick McDaniel, Shuai Mu and Erez Zadok, **Metrics for Sustainability in Data Centers**, *Proceedings of the 1st Workshop on Sustainable Computer Systems Design and Implementation (**HotCarbon'22**).*

Posters

[PS2] Syed Rafiul Hussain, Shagufta Mehnaz, Shahriar Nirjon, and Elisa Bertino, **Seamless and Secure Bluetooth LE Connection Migration**, *Seventh ACM on Conference on Data and Application Security and Privacy (CODASPY)*, 2017.

[PS1] Elisa Bertino, L. Bossi, Syed Rafiul Hussain, Asmaa Sallam, **Monitoring DBMS Activity for Detecting Data Exfiltration by Insiders**, *The 16th Annual Information Security Symposium*, 2015. **(✪ Best Poster Award Runner-up)**

Software Artifacts from Research

❍ **5GBaseChecker (2024):** An automated and scalable security testing framework for 5G basebands. : https://github.com/SyNSec-den/5GBaseChecker

❍ **HERMES (2024):** An end-to-end framework to automatically generate formal representations from natural language cellular specifications. : https://github.com/SyNSec-den/hermes-spec-to-fsm

❍ **5GCVerif (2023):** A model-based testing framework designed to formally analyze the access control framework of the 5G Core. : https://github.com/SyNSec-den/5GCVerif

❍ **BLEDiff (2023):** Scalable and property-agnostic non-compliance analysis framework for BLE implementations that identifies potential deviations in the BLE implementations from the standard. : https://github.com/BLEDiff/BLEDiff

❍ **DIKEUE (2021):** A black-box non-compliance checker for 4G LTE device's control plane protocol implementations. : https://github.com/SyNSec-den/DIKEUE

❍ **5GReasoner (2019):** Formal verification framework for 5G control-plane protocols.
: https://github.com/relentless-warrior/5GReasoner (20+ stars)

❍ **ATFuzzer (2019):** A grammar-guided, evolutionary fuzzing framework for testing the AT interface in Android phones. : https://github.com/Imtiazkarimik23/ATFuzzer (90+ stars)

❍ **LTEInspector (2018):** Formal verification framework for 4G NAS layer protocols.
: https://github.com/relentless-warrior/LTEInspector (115+ stars)

Reported Vulnerabilities

❍ **19 new vulnerabilities in ORAN-SC and SDRAN implementations of Open RAN, 2024**
- CVE-2024-25377, CVE-2024-29420, CVE-2024-34043, CVE-2024-34044, CVE-2024-34045, CVE-2024-34046, 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.

❍ **13 new 0-day vulnerabilities in 5G commercial basebands**, 2024
- CVD-2023-0081: GSMA Acknowledgment (known as Mobile Security Research Hall of Fame)
- CVE-2023-52533,CVE-2023-52534, CVE-2023-52341,CVE-2023-52343,CVE-2023-52342,CVE-2023-52344, CVE-2024-28818, CVE-2024-29152, CVE-2023-50803, CVE-2023-49927, CVE-2023-49928, CVE-2023-50804
- Acknowledged by Samsung in Samsung Product Security Update for helping them in identifying and fixing several vulnerabilities in 5G basebands.
- Acknowledged by Unisoc in Unisoc Product Security Acknowledgements for helping them in identifying and fixing vulnerabilities in Unisoc 5G baseband implementations.
- $14,250 bug bounty from Google
- $5,700 bug bounty from Samsung

❍ **7 new 0-day vulnerabilities in BLE devices, 2024**
- Medium and low-severity CVE's: CVE-2024-20890, CVE-2024-20889, CVE-2024-29155.
- Acknowledged by Samsung in Samsung Product Security Update for helping them in identifying and fixing several vulnerabilities in BLE implementations.
- $2,830 bug bounty from Samsung

❍ **3 new 0-day vulnerabilities in 4G LTE devices, 2024**
- CVE-2024-32911, 1 more CVE is yet to be assigned
- $2,850 bug bounty from Samsung

❍ **3 new vulnerabilities the 3GPP's NAS and RRC specifications for 5G networks, 2023**
- CVD-2023-0071: GSMA Acknowledgment (known as Mobile Security Research Hall of Fame)

❍ **6 new vulnerabilities the 3GPP's access control specifications for 5G core networks, 2023**
- CVD-2023-0069: GSMA Acknowledgment (known as Mobile Security Research Hall of Fame)

❍ **10 new vulnerabilities in the Bluetooth Low Energy (BLE) implementations, 2022**
- High and medium-severity CVE's assigned to some of the implementation issues we found in different BLE implementations: CVE-2022-45190, CVE-2022-45189, CVE-2022-40480, CVE-2022-41768, CVE-2022-45191
- Huawei Security bug bounty and acknowledgments: HWPSIRT-2022-56262, HWPSIRT-2022-13244, HWPSIRT-2022-96208
- Security advisory from STMicroelectronics (TN1436-ST-PSIRT).
- Google/Android Security bug bounty reward of $10,000 USD
- Responsible disclosure process

❍ **11 new vulnerabilities in the 14 different 4G LTE basebands, 2021**
- CVD-2021-0050: GSMA Acknowledgment (known as Mobile Security Research Hall of Fame)
- Google Bug Bounty Reward

- Samsung Bug Bounty Reward
- MediaTek Security Acknowledgements
- Qualcomm Security Bulletins
- High-severity CVE's assigned to some of the implementation issues we found in different UE implementations: CVE-2021-25471, CVE-2021-25480, CVE-2021-40148, CVE-2021-30344, SVE-2021-22327, SVE-2021-22324, CVE-2022-25685, CVE-2022-22091

❍ **3 new vulnerabilities in the NAS layer of 4G and 5G networks, 2021**
- CVD-2021-0043: GSMA Acknowledgment (known as Mobile Security Research Hall of Fame)

❍ **11 new vulnerabilities in the NAS and RRC layers of 5G networks, 2019**
- CVD-2019-0029: GSMA Acknowledgment (known as Mobile Security Research Hall of Fame)

❍ **Samsung phones accept AT commands over Bluetooth resulting in DoS attacks and exposure of sensitive information, such as IMSI, IMEI, call status, Internet service status, 2019**
- CVE-2019-16400, CVE-2019-16401

❍ **Static paging occasion of 4G and 5G networks (ToRPEDO), IMSI exposure through paging with IMSI (PIERCER), and IMSI-Cracking in 4G and 5G networks, 2019**
- CVD-2018-0014: GSMA Acknowledgment (known as Mobile Security Research Hall of Fame)

Research Impact

❍ Helped in uncovering and fixing 15 new vulnerabilities in ORAN-SC and SDRAN— the two open-source implementations of Open RAN.

❍ Uncovered 13 new exploitable implementation flaws (0-days) and 2 interoperability issues in 5G baseband devices and helped vendor fix the issues.

❍ Uncovered six new flaws (0-days) in the access control mechanism designed by 3GPP for the 5G core networks and helped 3GPP fix those.

❍ Unveiled three new design-level security flaws in the NAS and RRC layer protocols of 5G networks.

❍ Uncovered 10 new implementation flaws (0-days) in Bluetooth Low Energy devices widely used worldwide and helped vendor fix the issues.

❍ Uncovered 20+ new protocol flaws in 4G and 5G networks affecting billions of cellular devices which resulted in a number of changes in the 4G and 5G cellular standards.

❍ Uncovered 15+ implementation flaws (0-days) of operational networks worldwide and cellular devices, and helped the affected stakeholders to fix the flaws.

❍ Helped Qualcomm and Intel to set up their adversarial test-beds in 2018-19.

❍ Our proposed defense [C9] against fake base stations has been discussed by FCC for protecting users' security and privacy against the Stingray-type attacks.

❍ Since 2018, working with Intel to find vulnerabilities using our formal verification and dynamic analysis frameworks.

Public Media

❍ **5GBaseChecker (USENIX Security '24):** Your Phone's 5G Connection Is Vulnerable to Bypass, DoS Attacks, Dark Reading, 2024.

❍ **NSF/DoD 5G Convergence Accelerator '23:** Penn State partners on NSF grant to improve 5G networks, College of Engineering, Penn State, 2023.

❍ **NSF CNS Large on Sustainability:** Hussain earns NSF grant to make data centers more sustainable, College of Engineering, Penn State, 2023.

❍ **DARPA Young Faculty Award and DARPA Riser '22:** Faculty member receives grant, recognition from the U.S. Department of Defense, College of Engineering, Penn State, 2022.

❍ **NSF CAREER Award '22:** NSF CAREER Award: Syed Rafiul Hussain, College of Engineering, Penn State, 2022.

❍ **DIKEUE (CCS'21):** New technique identifies cell phone vulnerabilities accurately and automatically, Penn State, 2022.

❍ **ProChecker (ICDCS'21):** Researcher named to international Mobile Security Hall of Fame, Penn State, 2021.

❍ **5GReasoner (CCS'19):** Wired, TechCrunch, Forbes, MIT Technology Review, Yahoo Finance, and 70+ other media outlets worldwide.

❍ **ATFuzzer (ACSAC'19):** TechCrunch, Xiaomi, Deep Security News, My Digi Tech, Android Police, and 40+ other media outlets all over the world.

❍ **Bluetooth Security '19:** Wired, Medium, Business Telegraph, and 30+ tech-media worldwide.

❍ **ToRPEDO, PIERCER, and IMSI-Cracking (NDSS'19):** Washington Post, Wired, TechCrunch, MSN News, HackerNews, and 80+ other media outlets worldwide.

❍ **LTEInspector (NDSS'18):** New York Times, Forbes, CNet, ACM Tech News, ZDNet, The Register, Ars Technica and 80+ other media outlets all over the world.

Keynote Talks

❍ Building cellular network's security from the ground up for connected vehicles and IoT devices.
- *IEEE Vehicular Networking Conference (VNC)*, 2020.

Invited Talks

❍ Security-by-Design for Cellular Networks
- *srsRAN Project Workshop*, Washington D.C., 2023

❍ Security by Design for Complex Networks and Cyber-Physical Systems
- *University of North Carolina Chapel Hill*, 2023

❍ Security-by-Design for Cellular Networks
- *Ericsson*, 2022

❍ Building Security and Privacy of Complex Networks and Systems from the Ground Up
- *Dartmouth College*, 2021

❍ Building Principled Security Analysis Frameworks for Cellular Networks
- *Indian Institute of Technology, Delhi*, 2021

❍ Securing Cellular Networks from the Ground Up
- *North Carolina State University*, 2021

❍ Building Security Analysis Techniques for Complex Networks and Cyber-Physical Systems
- *Baidu Research*, 2021

❍ Automated Reasoning of Security and Privacy of 5G Cellular Networks and Cyber-Physical Systems
- *Ohio State University*, Cybersecurity Lecture Series, 2021

❍ Building Security and Privacy from the Ground up for Complex Networks and Systems
- *The 7th International Conference on Networking, Systems and Security (NSysS)*, December, 2020

❍ Automated Reasoning of Security and Privacy of Cellular Networks
- *Intel SCAP Workshop*, 2020

❍ Automated Reasoning of Security and Privacy of Networks and Systems
- *Bangladesh University of Engineering and Technology (BUET)*, 2020

❍ Principled Frameworks for Analyzing Security and Privacy Postures of Cellular Networks
- *University of Iowa*, 2019

❍ Systematic Analysis Frameworks for Cellular Networks
- *Intel SCAP Workshop*, 2019

❍ LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE
- Huawei Midwest IoT Security Summit 2018
- Midewest Verification Workshop 2018
- Intel/NSF Annual Workshop at Intel, 2018

Panels

❍ Security Challenges in 5G Wireless and Beyond.
- CSAW, New York University, 2021.

Conference Talks

❍ BaseDiff: Differential Security Analysis Of Cellular Basebands.
- *Qualcomm Product Security Summit*, 2022.

❍ Side Channel Attacks in 4G and 5G Cellular Networks.
- The BlackHat Europe'19.

❍ 5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol.
- ACM Conference on Communications Security (CCS), 2019.

❍ Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side-Channel Information.
- *Network and Distributed Systems Security (NDSS)*, 2019.

❍ Insecure Connection Bootstrapping in Cellular Networks: The Root of All Evil.
- ACM Conference on Sec. and Priv. in Wireless and Mobile Networks (WiSec), 2019.

❍ LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE.
- *Network and Distributed Systems Security (NDSS)*, 2018.

❍ SeamBlue: Seamless BLE Connection Migration for Unmodified IoT Devices.
- *ACM International Conf. on Embedded Wireless Sys and Net. (EWSN)*, 2017.

❍ DetAnom: Detecting Anomalous Database Transactions by Insiders.
- *ACM Conf. on Data and App. Security and Privacy (CODASPY)*, TX, USA, 2015.

❍ Secure Data Provenance Compression Using Arithmetic Coding in Wireless Sensor Networks.
- *IEEE Int. Perf. Computing and Comm. Conference (IPCCC)*, TX, USA, 2014.

Professional Service

❍ **Chair/Co-Chair:**
- Co-lead of *Network and NextG Security* session, NSF SaTC PI Meeting, Pittsburgh, PA, 2024.
- Publication Co-Chair: IEEE Symposium on Security and Privacy (IEEE S&P): 2025, 2024.
- Co-lead of *NextG and Wireless Security* session, NSF SaTC PI Meeting, Washington D.C., 2022.
- Publication Chair: IEEE Conference on Communications and Network Security: 2022.

❍ **Program Committee Member:**
- IEEE Symposium on Security and Privacy (IEEE S&P): 2025, 2023.
- ACM Conference on Computer and Communications Security (CCS): 2024, 2023, 2022.
- USENIX Security Symposium: 2024, 2023, 2024, 2022, 2021.
- The Network and Distributed System Security Symposium (NDSS): 2025, 2024, 2023, 2022.
- International Symposium on Research in Attacks, Intrusions and Defenses (RAID): 2024.
- The WebConf (formerly known as WWW): 2021.
- ACM ASIA Conference on Computer and Communications Security (ASIACCS): 2021.
- ACM Conf. on Security and Privacy in Wireless and Mobile Net. (WiSec): 2023, 2022.
- ACM Symposium on Access Control Models and Technologies (SACMAT): 2021, 2022.

- IEEE International Conference on Computer Communications (INFOCOM): 2024, 2023
- European Symposium on Research in Computer Security (ESORICS): 2021, 2020.
- The 29th IEEE International Conference on Network Protocols (ICNP): 2022, 2021.
- International Workshop on Mobile and Pervasive Internet of Things (PerIoT): 2019, 2020.
- International Conference on Networking, Systems and Security (NSysS): 2020, 2021.

❍ **Journal Review:**

- ACM Transactions on Privacy and Security (TOPS).
- Transactions on Dependable and Secure Computing (TDSC)
- Transactions on Mobile Computing (TMC)
- IEEE Communications Magazine.
- ACM Transactions on Sensor Networks.
- IEEE/ACM Transactions on Networking (TON).
- Transactions on Information Forensics & Security (TIFS).
- IEEE Transactions on Dependable and Secure Computing (TDSC).
- ACM Transactions on Internet Technology (TOIT).
- IEEE Internet Computing.
- Sensors.

❍ **Conference (External) Review:**

- IEEE Symposium on Security and Privacy (Oakland): 2019, 2020.
- ACM Conference on Computer and Communication Security: 2019.
- The WebConf (WWW) 2019.
- International Conference on Privacy, Security and Trust (PST): 2019.
- ACM Conference on Data and Application Security and Privacy (CODASPY): 2017.
- ACM ASIA Conference on Computer and Communications Security (ASIACCS): 2015.
- COMPSAC 2015.

❍ **Other Activities:**

- NSF SaTC panelist: 2024, 2022
- NSF SaTC Town Hall attendee: 2022
- Participated the Leonhard Center workshop for CAREER Proposal: 2021.
- NSF CISE CAREER Workshop attendee: 2021.

Teaching Experience

❍ **Pennsylvania State University**

- CSE 543: Computer Security (Fall'24, Fall'22, Fall'21, Fall'20).
- CMPSC 443: Introduction to Computer Security (Spring'22).
- CMPSC 311: Systems Programming (Fall'23).
- CSE 597: Security of Emerging Technologies (Spring'21).
- Security Reading Group/Seminar (Fall'21).

❍ **Purdue University (Guest Lecturer)**

- CS 528: Network Security, Purdue University (Spring 2019 and Spring 2020).
- CS 590: Data Security and Privacy, Purdue University (Spring 2019).
- CS 541: Database Management, Purdue University (Spring 2018, Fall 2019).

❍ **Purdue University (Teaching Assistant)**

- CS 307: Software Engineering (Fall 2017, Spring 2018).
- CS 180: Problem Solving and Object-Oriented Programming (Fall 2015, Spring 2016).

❍ **NC State University (Teaching Assistant)**

- Operating Systems (Fall 2011).
- Internet Protocols (Spring 2012).

Ph.D. Students Advising

- ❍ **Abdullah Al Ishtiaq**: Fall '21 - Present, Area: Network and Systems Security, NLP for Security.
- ❍ **Ali Ranjbar**: Spring '22 - Present, Area: Systems and Software Security, and Binary Analysis.
- ❍ **Mujtahid Akon**: Spring '22 - Present, Area: Automated Reasoning, and Formal methods.
- ❍ **Tianchang Wang**: Fall '22 - Present, Area: Systems security, Program Analysis, Fuzzing.
- ❍ **Syed Md Mukit Rashid**: Fall '22 - Present, Area: Program Analysis and Security.
- ❍ **Tianwei Wu**: Spring '23 - Present, Area: Wireless Security.
- ❍ **Kai Tu**: Spring '24 - Present, Area: Network Security.
- ❍ **Yilu Dong**, Spring '24 - Present, Area: Systems security.
- ❍ **Ridwan Hasan Tanvir**: Spring '24 - Present, Area: NLP for Security.
- ❍ **Md. Sultan Mahmud**: Spring '24 - Present, Area: Wireless Security.
- ❍ **Md Toufikuzzaman**: Fall '24 - Present, Area: Software Security.
- ❍ **Himashveta Kumar**: Fall '24 - Present, Area: Software Security.
- ❍ **Bokai Zhang (co-advised with Gary Tan)**: Fall '24 - Present, Area: Software Security.
- ❍ **Ananna Rahman (co-advised with Shagufta Mehnaz)**: Fall '24 - Present, Area: TBD.

MS Students Advising

- ❍ **Xiaotian Zhou**, Area: Security and Programming Languages.
- ❍ **Weixuan Wang**, Area: Software Security.
- ❍ **Abhijith Krishnan**, Area: Security and Applied Cryptography.

Undergrads Advising

- ❍ **Parth Agarwal**, Area: Software Security and AI.

MS Students Graduated

- ❍ **Kai Tu**, CSE, Penn State, 2023
  - *Thesis: Deviant Behavior Analysis of 5g COTS UE Implementations*
  - First Employment: PhD Student, Pennsylvania State University
- ❍ **David Reinoso (Co-advised with Trent Jaeger)**, CSE, Penn State, 2023
  - *Thesis: Analysis of Influential Objects in Smart Home Platforms*
  - First Employment: TBD
- ❍ **Yilu Dong**, CSE, Penn State, 2023
  - *Thesis: Deviant Behaviors of 5G Core Network Implementations*
  - First Employment: PhD Student, Pennsylvania State University
- ❍ **Goutham Anicode**, CSE, Penn State, 2023
  - *Project: Securing REST APIs of Microservices*
  - First Employment: Microsoft
- ❍ **Harshita Coneri**, CSE, Penn State, 2023
  - *Project: Securing REST APIs of Microservices*
  - First Employment: Engineer II - CrowdStrike
- ❍ **Saaman Khalilollahi**, CSE, Penn State, 2023
  - *Project: Symbolic Execution in Baseband Firmware*
  - First Employment: Systems Engineer for Liberty Home Mortgage Corporation
- ❍ **Jill Haffner**, IUG Student, CSE, Penn State, 2022.
  - *Project: Extending the Application of Geneva Censorship Tool Against Campus WiFi Infrastructures*
  - First Employment: SCrossFit Lionheart

❍ **Parth Natu**, CSE, Penn State, 2021.
- *Thesis: Securing 5G Broadcast Messages*
- First Employment: Dematic

❍ **Ankush Palasamudrum**, EE, Penn State, 2021
- *Project: Testing the correctness and robustness of Open5GS*
- First Employment: Qualcomm

❍ **Pranitha Malae**, CSE, Penn State, 2021
- *Project: 5G Core Network Security: A Classification of attacks on modern cellular core network*
- First Employment: Molecula

❍ **Suramya Mishra**, CSE, Penn State, 2021
- *Project: Finite State Machine Extractor*
- First Employment: TBD

Undergrads Graduated

❍ **Ziping Ye**, Schreyer Honors College, CSE, Penn State, 2023
- *Thesis: Dragon Defender: Runtime Threat Detection for Cellular Devices*
- First Employment: MS Student, University of Pennsylvania

❍ **Jill Haffner**, IUG Student, CSE, Penn State, Graduated: Fall 2022
- *Thesis: Applying Geneva Censorship Evasion Tool Against Private-Access WiFi Networks*
- First Employment: SCrossFit Lionheart

❍ **Amey Deotale**, CSE, Penn State, Graduated: 2022
- *Project: Baseband Security*
- First Employment: Microsoft

❍ **Naga Vutukuri**, CSE, Penn State, Graduated: 2022
- *Project: Payment card Security*
- First Employment: Microsoft

PhD Thesis Committee Member

❍ **Yu Tsung (Eddy) Lee**, PhD, CSE, Pennsylvania State University, 2024
- *Thesis: Tackling File Vulnerabilities in Android: A Comprehensive Approach Through Access Control Policy Analysis and Program Analysis*

❍ **Xilun Liu**, PhD, CSE, Pennsylvania State University, 2024
- *Thesis: TBD*

❍ **Michael Alexander Norris**, PhD, CSE, Pennsylvania State University, TBD
- *Thesis: TBD (Working on IoT Security)*

❍ **Suryoday Basak**, PhD, CSE, Pennsylvania State University, TBD
- *Thesis: TBD (Working on wireless security)*

❍ **Jialun Zhang**, PhD, CSE, Pennsylvania State University, TBD
- *Thesis: TBD*

❍ **Quan Zhou**, PhD, CSE, Pennsylvania State University, TBD
Thesis: TBD

❍ **Yuanqing Miao**, PhD, CSE, Pennsylvania State University
Thesis: TBD

MS Thesis/Project Committee Member

❍ **Tianwei Wu**, MS, Pennsylvania State University, 2022.
Project: A Survey of Location Privacy Attacks in LTE Networks.

❍ **Sophia Beyda**, MS, CSE, Pennsylvania State University, 2022.
Thesis: The Impact of the Organizational Structure of Android Third Party Libraries.

❍ **Ryan Guide**, MS, CSE, Pennsylvania State University, 2022.
Project: Characterizing the Modification Space of Signature IDS Rules.

❍ **Connor Geer**, MS, CSE, Pennsylvania State University, 2022.
Thesis: Anomaly Detection of Test-Time Evasion Attacks in the Audio Domain.

❍ **Niranjan Thirusangu**, MS, CSE, Pennsylvania State University, 2021.
Thesis: Segmentation of Lesions from Breast Ultrasound Images using Deep Convolutional Neural Network.

❍ **Yohan Beugin**, MS, CSE, Pennsylvania State University, 2021.
Thesis: Building a Secure and Privacy-Preserving Smart Camera System.

University Service Committee

❍ **Penn State, Computer Science and Engineering Department**

- Fall'22 - Present: Graduate Curriculum Committee
- Fall'21 - Present: Faculty Hiring Committee.
- Fall'23 - Present: ABET/Assessment Committee
- Fall'20 - Present: Graduate Committee.
- Fall'20: Moderated the oral test of PhD qualifying exam.

❍ **Penn State, College of Engineering**

- Fall'22 - Present: Research Assistant Professor Hiring Committee, Dept. of Agricultural and Biological Engineering.
- Fall'21 - Present: Education/New Programs Committee.
- Spring'21 - Summer'21: Academic Integrity Committee.
