IMTIAZ KARIM

Postdoctoral Research Associate, Purdue University
Lawson Computer Science Building, 305 N University St, West Lafayette, IN 47907
(463) · 204 · 8034 ⋄ karim7@purdue.edu ⋄ https://www.imtiazkarim.net/

RESEARCH INTEREST

My research interests lie in analyzing the security and privacy of wireless communication protocols (e.g., *4G, 5G, Bluetooth, VoWiFi, vehicular, WiFi, and IoT*), their implementations, networked systems, and mobile computing. My research aim is to develop tools that systematically analyze real-world systems and widely used protocols using formal verification, program analysis, machine learning, natural language processing, and software testing techniques. Furthermore, with the advent of the next generation of networks (6G and beyond), my future goal is to ensure the *resilience (reliability, adaptability, and security)* of future network generations and develop systems that are secure by design.

EDUCATION

Purdue University, West Lafayette, IN *Fall 2018 - Spring 2023*
Ph.D. in Computer Science, GPA: 4.00/4.00
Thesis: A Systematic Framework for Analyzing The Security And Privacy of Wireless Communication Protocol Implementations.
Advisor: Dr. Elisa Bertino
Advisory Committee: Dr. Ninghui Li, Dr. Sonia Fahmy, and Dr. Dave Tian

Bangladesh University of Engineering and Technology *February 2013 - September 2017*
B.Sc. in Computer Science & Engineering
Thesis: Heterogeneous Coverage in Visual Sensors Networks
Advisor: Dr. A.K.M. Ashikur Rahman

RESEARCH POSITIONS

Purdue University West Lafayette, IN
Postdoctoral Research Associate *Summer 2023 - Present*

Purdue University West Lafayette, IN
Graduate Research Assistant *Fall 2019 - Summer 2023*

Amazon
Applied Scientist Intern *Summer 2021*

- Retrofitting Domain-Specific Languages with type inference and type checking
- *Manager:* Dr. Vaibhav Sharma; *Mentor:* Dr. Saswat Padhi

Intel Corporation Hillsboro, OR
Security Researcher Intern *Summer 2020*

- Utilizing symbolic execution for property-guided security and privacy testing in communication protocol implementations
- *Manager:* Jason M. Fung; *Mentors:* Dr. Sayak Ray, Dr. Arun Kanuparthi, and Dr. Stephan Heuser

Intel Corporation Hillsboro, OR
Security Researcher Intern *Summer 2019*

- Security and privacy analysis framework for communication protocol implementations
- *Manager:* Jason M. Fung; *Mentors:* Dr. Sayak Ray and Dr. Arun Kanuparthi

AWARDS & HONORS

2022-2023	Bilsland Dissertation Fellowship award from Purdue University Graduate School
2021	Best paper award nomination, ICDCS
2021, 2019	Inducted three times in the Mobile Security Research Hall of Fame by GSMA for identifying security & privacy flaws and coordinating mitigation in the 4G LTE/5G cellular network standards and implementations.
2020	Maurice H. Halstead Memorial Award for outstanding research in Software Engineering, Purdue University
2019	Distinguished Paper Award, ACSAC
2019	ACM CCS Student Travel Grant Award
2016-2017	Dean's List Award during B.Sc.

PUBLICATIONS

Peer-Reviewed Conference:

[**C9**] **Imtiaz Karim**, Kazi Samin Mubasshir, Mirza Masfiqur Rahman, and Elisa Bertino, SPEC5G: A Dataset for 5G Cellular Network Protocol Analysis *(under review)*.

[**C8**] **Imtiaz Karim***, Hyunwoo Lee*, and Elisa Bertino, VWAttacker: A Systematic and Automated Security Testing Framework for Voice over WiFi Implementations, *(under review)*.

[**C7**] **Imtiaz Karim**, Abdullah Al Ishtiaq, Syed Rafiul Hussain, and Elisa Bertino, BLEDiff: Scalable and Property-Agnostic Noncompliance Checking for BLE Implementations, 44th IEEE Symposium on Security and Privacy (**IEEE S&P**), 2023.

[**C6**] Hyunwoo Lee, **Imtiaz Karim**, Ninghui Li, and Elisa Bertino, VWAnalyzer: A Systematic Security Analysis Framework for the Voice over WiFi Protocol, 17th ACM ASIA Conference on Computer and Communications Security (**ASIACCS**), 2022.

[**C5**] Elisa Bertino and **Imtiaz Karim**, AI-powered Network Security: Approaches and Research Directions, 8th International Conference on Networking, Systems, and Security **(NSysS)**, 2021. (Invited research directional paper)

[**C4**] **Imtiaz Karim***, Syed Rafiul Hussain*, Abdullah Al Ishtiaq, Omar Chowdhury, and Elisa Bertino, Noncompliance as Deviant Behavior: An Automated Black-box Noncompliance Checker for 4G LTE Cellular Devices, 28th ACM Conference on Computer and Communications Security (**CCS**), 2021.

[**C3**] **Imtiaz Karim**, Syed Rafiul Hussain, and Elisa Bertino, ProChecker: An Automated Security and Privacy Analysis Framework for 4G LTE Protocol Implementations, The 41st IEEE International Conference on Distributed Computing Systems (**ICDCS**), 2021.
Best paper award nomination

[**C2**] **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, 35th Annual Computer Security Applications Conference (**ACSAC**), 2019.
Distinguished paper award

[**C1**] Syed Raiful Hussain, Mitziu Echeverria, **Imtiaz Karim**, Omar Chowdhury, and Elisa Bertino, 5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol, 26th ACM Conference on Computer and Communications Security (**CCS**), 2019.

Peer-Reviewed Journal:

[**J2**]: **Imtiaz Karim**, Fabrizio Cicala, Syed Rafiul Hussain, Omar Chowdhury, and Elisa Bertino. ATFuzzer: Dynamic Analysis Framework of AT Interface for Android Smartphones. Digital Threats: Research and Practice, **(DTRAP)**, 2020.

[J1]: Abdullah Al Zishan, **Imtiaz Karim**, Sudipta Saha Shubha, Ashikur Rahman, Maximizing Heterogeneous Coverage in Over and Under Provisioned Visual Sensor Networks, The Journal of Network and Computer Applications, Elsevier (**JNCA**), Volume 124, 15 December 2018, Pages 44-62.

Book:

[B1]: Imtiaz Karim, et. al., including Elisa Bertino, Machine Learning Techniques for Cybersecurity, Part of the book series: Synthesis Lectures on Information Security, Privacy, and Trust (SLISPT), Springer Nature, May 2023.

Industrial Conference Papers:

[IC2]: Imtiaz Karim, Sayak Ray, Arun Kanuparthi and Jason M. Fung, ProChecker: An Automated Security and Privacy Analysis Framework for Communication Protocol Implementations, Intel SoftWare Practitioners Conference, (Intel SWPC) 2020.

[IC1]: Imtiaz Karim, Sayak Ray, Arun Kanuparthi, Stephan Heuser and Jason M. Fung, Utilizing Symbolic Execution for Property-Guided Security and Privacy Testing in Communication Protocol Implementations, Intel SoftWare Practitioners Conference, (Intel SWPC) 2020.

GRANT APPLICATIONS

1. Author of the proposal - Systematic LLM Based Protocol Analysis, awarded $\$109,372$ by Cisco Research, 2023.

2. Author of the proposal (NSF 2223452) - Detecting fake and compromised base stations using the platforms for Advanced Wireless Research (PAWR). Funded by NSF, 2022.

3. Helped with the write up of thrust 4 : AI-Powered Network Security (NSF 2112471) - AI Institute for Future Edge Networks and Distributed Intelligence. Awarded: $\$19,990,577$, 2021.

4. Author of the proposal - Principled Security Analysis of Intel's Bluetooth implementation through enhanced Symbolic Execution, awarded $\$72,000$ by Intel for 2021.

5. Co-author of the proposal - Principled Security and Privacy Analysis of Intel's Implementation of Bluetooth, Bluetooth Low Energy, and Wi-Fi Protocols, awarded $\$72,000$ by Intel for 2020.

ACADEMIC SERVICE

- **Program Committee Member:**
  - The Network and Distributed System Security Symposium (NDSS) 2024.
  - IEEE International Conference on Distributed Computing Systems (ICDCS) 2023.
  - Research in Attacks, Intrusions and Defenses (RAID) 2023.
- **Artifact Evaluation Committee Member:**
  - Usenix Security 2023, 2022.
  - European chapter of ACM SIGOPS (EuroSys) 2023.
  - ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) 2022.
- **Organizing Committee:**
  - Chair, Committee for AI-EDGE Students/Postdocs Meetings (SPARKS)
- **Journal Review:**
  - ACM Transactions on Privacy and Security (TOPS).
  - The International Journal of Information Security Springer.
  - ACM Computing Surveys, IEEE Transactions on Information Forensics and Security.
  - IEEE Transactions on Dependable and Secure Computing.
- **Conference Review (External):**
  - Annual Computer Security Applications Conference (ACSAC) 2022.
  - The Network and Distributed System Security Symposium (NDSS) 2023, 2022, 2021.
  - Usenix Security 2022, 2021.
  - ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) 2022.
  - IEEE International Conference on Network Protocols 2022, 2021.

– European Symposium on Research in Computer Security (ESORICS) 2022, 2021, 2020.
– ACM Conference on Data and Application Security and Privacy 2023, 2022, 2021.
– ACM Conference on Computer and Communications Security (CCS) 2021, 2019.
– International World Wide Web Conference (WebConf) 2023.
– Annual International Conference On Mobile Computing And Networking (MobiCom) 2021.

TEACHING

Purdue University

- Guest Lecturer: CS 59000-DSP Data Security And Privacy *Spring 2022*
- Graduate Teaching Assistant: CS 180: Problem Solving and Object-Oriented Programming (Fall 2018, Spring 2019)

Pennsylvania State University *Spring 2022*
Guest Lecturer: CMPSC 443: Introduction to Computer Security

Daffodil International University, Bangladesh *September 2017 - July 2018*
Lecturer, Department of Computer Science and Engineering

Mentor, Purdue University CSGSA Mentor-Mentee program *Fall 2021 - Spring 2022, Fall 2022 - Spring 2023*

RESEARCH MENTORING

- Mirza Mashfiqur Mim, Ph.D. Student, Purdue University *Summer 2022 - present*
  Research: 5G cellular network protocol, reinforcement learning
  Co-author of SPEC5G
- Kazi Samin Mubasshir, Ph.D. Student, Purdue University *Fall 2022 - present*
  Research: 5G cellular network protocol defense
  Co-author of SPEC5G
- Benjamin Nelson Bond, Ph.D. Student, Purdue University *Spring 2023 - present*
  Research: Firmware re-hosting and analysis
- Zilin Shen, Ph.D. Student, Purdue University *Spring 2023 - present*
  Research: WiFi security
- Mir Imtiaz Mostafiz, Ph.D. Student, Purdue University *Spring 2023 - present*
  Research: Graph neural networks

BUG BOUNTIES AND BUGS

2022, 23 Google Bug Bounty reward of $15,000 for finding high severity vulnerability in 4G LTE and BLE implementations [C4] [C7]

2023 Huawei Bug Bounty reward for finding high severity vulnerability in BLE implementations [C7].

2021, 2019 Samsung Bug Bounty Reward for finding high security vulnerabilities in Samsung Smartphones [C4] [C2]

Discovered CVE/CVD/SVE's: : CVE-2022-40480, CVE-2022-41768, CVE-2021-25471, CVE-2021-25480, CVE-2021-40148, CVE-2021-30344, CVE-2019-16400, CVE-2019-16401, CVE-2021-25471, CVE-2021-25480, CVE-2021-40148, CVD-2019-0029, CVD-2021-0043, CVD-2021-0050, SVE-2021-22327, SVE-2021-22324, CVE-2022-40480, CVE-2022-41768, CVE-2022-45190, CVE-2022-45192, CVE-2022-45191, TN1436-ST-PSIRT, HWPSIRT-2022-56262, HWPSIRT-2022-13244, HWPSIRT-2022-96208, CVE-2022-25685, CVE-2022-22091

MEDIA COVERAGE AND SOFTWARE ARTIFACTS

SPEC5G: (`https://github.com/Imtiazkarimik23/SPEC5G`)

FBS-Detector: Platforms for Advanced Wireless Research, Purdue Computer Science.

BLEDiff: (`https://github.com/BLEDiff/BLEDiff`) Security advisory from STMicroelectronics

VWANALYZER: (`https://github.com/vwanalyzer`)

DIKEUE: (`https://github.com/SyNSec-den/DIKEUE`) College of Engineering- Penstate, Qualcomm Product Security Bulletins, Android Security Acknowledgements, MediaTek Product Security Acknowledgements

ProChecker: College of Engineering- Penstate

ATFuzzer: (`https://github.com/Imtiazkarimik23/ATFuzzer`) (120+ stars) Techcrunch, Xiaomi, Deep Security News, My Digi Tech and 40+ media outlets all over the world.

5GReasoner: (`https://github.com/relentless-warrior/5GReasoner`) (25+ stars) Forbes, MIT Technology Review, Wired, Techcrunch and 70+ media outlets all over the world.

TALKS & PRESENTATIONS

- ML and NLP for Cellular Network Security, NSF AI Institute for Future Edge Networks and Distributed Intelligence, Northeastern University, Boston, 2023.
- BLEDiff: Scalable and Property-Agnostic Noncompliance Checking for BLE Implementations, 44th IEEE Symposium on Security and Privacy (IEEE S&P), 2023.
- A White-box Learning Approach to Generate Formal Models of Communication Protocols , AI-EDGE all hands on workshop, June, 2022.
- Noncompliance as Deviant Behavior: An Automated Black-box Noncompliance Checker for 4G LTE Cellular Devices, CCS 2021, and invited talk to the third Annual Side Channel Academic Program (SCAP) workshop, Intel 2021.
- ProChecker: An Automated Security and Privacy Analysis Framework for 4G LTE Protocol Implementations, ICDCS 2021.
- Automated Security and Privacy Analysis for Communication Protocol Implementation, invited talk to the Second Annual Side Channel Academic Program (SCAP) workshop, Intel 2020.
- Opening Pandora's Box through ATFuzzer: Dynamic Analysis of AT Interface for Android Smartphones, ACSAC 2019.

REFERENCES

Dr. Elisa Bertino
Professor
Department of Computer Science
Purdue University.
Email: bertino@purdue.edu

Dr. Ninghui Li
Professor
Department of Computer Science
Purdue University.
Email: ninghui@purdue.edu

Jason M. Fung
Director of Academic Research Engagement
Offensive Security Research Manager
Intel Corporation.
Email: jason.m.fung@intel.com

Dr. Syed Rafiul Hussain
Assistant Professor
Department of Computer Science and Engineering
Pennsylvania State University.
Email: hussain1@psu.edu