MD Armanuzzaman

Postdoctoral Research Associate
Khoury College of Computer Science
Northeastern University
Email: m.armanuzzaman@northeastern.edu
Personal Webpage: https://tomal-kuet.github.io/armanuzzaman/
Github: https://github.com/Tomal-kuet
Google Scholar: https://scholar.google.com/citations?user=TSEtWiUAAAAJ&hl
Address: 177 Huntington Ave, Boston, MA

RESEARCH INTERESTS

- Cybersecurity
  - **Systems and Software Security**
  - Security of **Embedded**, **IoT**, **FPGA**, and GPU Systems
  - **Trusted Execution Environments**, **Control-Flow Attestation**, **Control-Flow Integrity**, and Program analysis

EDUCATION

Ph.D. in Computer Science and Engineering 2024
- University at Buffalo, NY, USA
- Advisor: Ziming Zhao

B.S. in Computer Science and Engineering 2017
- Khulna University of Engineering & Technology, Khulna, Bangladesh

PROFESSIONAL EXPERIENCE

Postdoctoral Research Associate, CactiLab, Northeastern University Sep 2024 – Present
- Embedded Systems Security; LLM in Cybersecurity; GPU Security; Security of ML.

Graduate Research Assistant, CactiLab, University at Buffalo Aug 2020 – Aug 2024
- Trusted Execution Environments for FPGA SoCs; Control Flow Attestation for Embedded Systems; Systems Security; Software Security; Program Analysis; Security of FPGA HLS.

Teaching Assistant, Department of Computer Science and Engineering, University at Buffalo
- CSE 510 Software Security (class size 60): Contribute to course material design with 130+ challenges and CTF platform development. Aug 2021 - Dec 2022
- CSE 565 Computer Security (class size 110) Jan 2023 - May 2023

Graduate Research Assistant, CactiLab, Rochester Institute of Technology Aug 2019 – Aug 2020
- Embedded systems; CTFs; Ethical Hacking; Binary Analysis; FPGA.

Software Engineer, Full Stack, BJIT, Bangladesh Jul 2017 – Aug 2019
- Spring MVC; Spring Boot; MySQL; JavaScript.

PUBLICATIONS

ASIACCS'24 **MD Armanuzzaman**, Ahmad-Reza Sadeghi, Ziming Zhao. "Building Your Own Trusted Execution Environments Using FPGA". *In Proceedings of the ASIA Conference on Computer and Communications Security (ASIACCS), 2024*. [*code*] (129/585 = 22.1% acceptance rate)

SEED'24 Ziming Zhao, **MD Armanuzzaman**, Xi Tan, Zheyuan Ma. "Trusted Execution Environments in Embedded and IoT Systems: A Perspective". *In Proceedings of IEEE International Symposium on Secure and Private Execution Environment Design (SEED), 2024*.

SAC'24 Xi Tan, Sagar Mohan, **MD Armanuzzaman**, Zheyuan Ma, Gaoxiang Liu, Alex Eastman, Hongxin Hu, and Ziming Zhao. "The Canary is Dead: On the Effectiveness of Stack Canaries on Microcontroller-based Systems". *In Proceedings of ACM/SIGAPP Symposium On Applied Computing (SAC) 2024*. (180/773 = 23.3% acceptance rate)

NDSS'25 Jing Shang, Jian Wang, Kailun Wang, Jiqiang Liu, Nan Jiang, **MD Armanuzzaman**, and Ziming Zhao. "Defending Against Membership Inference Attacks for Iteratively Pruned Deep Neural Networks". *In Proceedings of Network and Distributed System Security Symposium (NDSS), 2025*.

INFOCOM'25 Jingjing Guan, Hui Li, Xiangdong Li, Xiaolei Wang, Binghan Wang, Qiuye Wang, Shengchao Qin, Mengda He, **MD Armanuzzaman**, and Ziming Zhao, "Formally Verifying the State Machine of TLS 1.3 Handshake in OpenSSL". *In Proceedings of IEEE International Conference on Computer Communications (INFOCOM), 2025*.

NSysS'17 **MD Armanuzzaman**, Kazi Md. Rokibul Alam, Md. Mehadi Hassan. "A secure and efficient data transmission technique using quantum key distribution". *In Proceedings of International Conference on Networking, Systems and Security (NSysS) 2017*.

WORKING-IN-PROGRESS PAPERS

- ❑ **MD Armanuzzaman**, Engin Kirda, Ziming Zhao. "Enola: Efficient Control-Flow Attestation for Embedded Systems". Under review in USENIX Security Symposium 2025.
- ❑ Zheyuan Ma, Alex Eastman, Gaoxiang Liu, Kai Kaufman, **MD Armanuzzaman**, Xi Tan, Katherine Jesse, Robert Walls, Ziming Zhao. "We just did not have that on the embedded system: Insights and Challenges for Securing Microcontroller Systems from the Embedded CTF Competitions". Completed work and being submitted in CCS 2025.
- ❑ **MD Armanuzzaman**, Ahmad-Reza Sadeghi, and Ziming Zhao. "BYOTee: Towards Building Your Own Trusted Execution Environments Using FPGA" – Journal Version.
- ❑ Rui Zhang, Jian Wang, Nan Jiang*, **MD Armanuzzaman**, and Ziming Zhao, "Quantum Federated Learning Based on Multi-qubit Quantum Broadcast Protocol (MQBP-QFL)". Under review in IEEE Transactions on Information Forensics & Security (TIFS) 2025.
- ❑ **MD Armanuzzaman**, Ziming Zhao. "HLSSec: FPGA High-Level Synthesis Security".

TEACHING AND MENTORSHIP

- ❑ Mentor Undergraduate Students for Research Projects at Northeastern University 2024
- ❑ Teaching Assistant, University at Buffalo Aug 2021 – May 2023
- ❑ Develop CTF platform and Course Material for CSE 410/510 Software Security Course, UB
  - Over 350 Student Users
- ❑ Supervise four undergraduate students for independent study Fall 2023
- ❑ Mentor Summer Intern (Kayla Yan) from UB CSTEP Summer 2024
- ❑ Advisor for Team Cacti in MITRE eCTF Competitions 2023 – 2024
- ❑ CTF Training: University at Buffalo/Rochester Institute of Technology 2019 – 2023

PATENTS

- ❑ Ziming Zhao, **MD Armanuzzaman**. "System and Method for Building Customized Trusted Execution Environments with a System-On-Chip Field Programming Gate Array". *US 2024/0152601A1, 05/09/24*

DISSERTATION

- **MD Armanuzzaman**. "Augmenting and Utilizing Trusted Execution Environments for Embedded System Security". Doctoral Dissertation, Computer Science and Engineering, University at Buffalo. 2024

SELECTED AWARDS AND HONORS

- Distinguished Artifact Reviewer Award at ACM Conference on Computer and Communications Security (CCS) 2024
- MITRE eCTF, Advisor of Team Cacti, UB 2024
  - **Ranked 4 among 100 teams**. Medical infrastructure supply chain security solution on Tiva-C board, and hacking other teams. [*code*]
- MITRE eCTF, Advisor of Team Cacti, UB 2023
  - **Ranked 4 among 60 teams**. Created a robust key fob system for car door locks, mitigating risks of unauthorized access, replay attacks, key fob duplication, and hacking other teams. [*code*]
- MITRE eCTF, Captain of Team Cacti, UB 2022
  - **Ranked 5 among 28 teams**. Designed a resilient bootloader for firmware updates in an avionic device, ensuring the security of intellectual property, mission data, supply-chain threats including hardware trojans, and hacking other teams. [*code*]
- MITRE eCTF, Member of Team Cacti, UB 2021
  - **Ranked 9 among 20+ teams (Best write-up award)**. Implemented a secure communication system for a UAV package delivery system, protecting against unauthorized network access, disruptions, and hacking other teams. [*code*]
- MITRE eCTF, Member of Team Cacti, RIT 2020
  - **Ranked 6 among 20+ teams**. Developed a secure audio digital rights management module for a digilent Cora Z7 multimedia player, ensuring protection against privacy, region restrictions, and hacking other teams. [*code*]
- University Faculty Dean Award, Khulna University of Engineering & Technology 2017

PROFESSIONAL SERVICES

- Artifact Evaluation Committee Member at USENIX Security Symposium 2025
- Reviewer at ACM Transactions on Cyber-Physical Systems 2025
- Artifact Evaluation Committee Member at ACM Conference on Computer and Communications Security (CCS) 2024
- External Reviewer: IEEE Security & Privacy (S&P), USENIX Security Symposium, ACM Conference on Computer and Communications Security (CCS), ACM ASIA Conference on Computer and Communications Security (ASIACCS), Annual Computer Security Applications Conference (ACSAC), Conference on Data and Application Security and Privacy (CODASPY), Design Automation Conference (DAC), Security and Privacy in Communication Networks (SecureComm), IEEE International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom), International Conference on Information and Communications Security (ICICS), IEEE Conference on Communications and Network Security (CNS), IEEE International Conference on Cloud Computing Technology and Science (CloudCom), IEEE Workshop on the Internet of Safe Things.

TRAVEL GRANTS

- ❑ Travel Grants at NDSS 2021 (Feb 21-25, Virtual). 2021
- ❑ Travel Grants at SKM 2021 (Oct 8-9, Virtual). 2020
- ❑ Travel Grants at USENIX Security 2020 (Aug 12-14, Virtual). 2020

PRESENTATIONS

- ❑ **Trusted Execution Environments in Embedded and IoT Systems: A Perspective** at *International Symposium on Secure and Private Execution Environment Design (SEED)*, University of Central Florida, Orlando, Florida, USA 2024
- ❑ **Building Your Own Trusted Execution Environments Using FPGA** at *Great Lake Security Day (GLSD)*, Virtual 2021
- ❑ **Work-in-Progress: Building Your Own Trusted Execution Environments Using FPGA** at *International Conference on Secure Knowledge Management (SKM)*, Virtual 2021

TECHNICAL SKILLS

- ❑ **Languages**: C, C++, Assembly, Shell, Python, Java, JavaScript, SQL, VHDL, Verilog
- ❑ **Technologies/Frameworks**: Linux, Docker, LLVM, IDA pro, ghidra, Binary ninja, gdb, GitHub, Spring MVC, Spring boot
- ❑ **Ethical Hacking:** Binary Reverse Engineering, Control Flow Hijacking, Cryptography, Side-channel Leakage, Static and Dynamic Analysis

OPEN-SOURCED PROJECTS

- ❑ **Pyelftools** Contribution for Cortex-m85 and ARM-LLVM toolchain binary: [git issue] 2024
- ❑ **BYOTee** Building Your Own Trusted Execution Environments Using FPGAs: [code] 2020 - 2022
- ❑ **Image reconstruction** with significant eigenfaces: [code] 2020
- ❑ **Wireless PC Controller** an android application to control desktop functions: [code] 2016
- ❑ **Esho_Shikhi** a desktop application for children's education: [code] 2014
- ❑ **File-share** a platform for file sharing with access permissions: [code] 2014