MD Armanuzzaman

177 Huntington Ave
Northeastern University
Boston, MA, 02115

E-mail: m.armanuzzaman@northeastern.edu
Homepage: tomal-kuet.github.io
Ph: +15857527756

RESEARCH INTERESTS

- Systems and Software Security of Embedded, IoT, Desktop, and FPGA Systems
- Program analysis, Fuzzing
- Security and Privacy of Machine Learning
- Cyber-Physical Systems Security

EDUCATION

Ph.D, Computer Science and Engineering — University at Buffalo, Buffalo, NY, USA
- Advisor: Zimng Zhao — August 2020 - August 2024

B.S., Computer Science and Engineering — KUET, Khulna, Bangladesh — March 2017

PROFESSIONAL EXPERIENCE

Postdoctoral Research Associate Cacti Lab, Northeastern University — September 2024 – present
- Systems security; software security; embedded systems security; FPGA HLS security; LLM in cybersecurity.

Graduate Research Assistant, Cacti Lab, University at Buffalo — August 2020 – August 2024
- Trusted Execution Environments for FPGA SoCs; control flow attestation for embedded systems; systems security; software security; analyzing the security of FPGA HLS.

Teaching Assistant, Department of Computer Science and Engineering, University at Buffalo
- CSE 510 Software Security (class size 60): TA and course design with CTF platform development with challenges (100). August 2021 - Dec. 2022
- CSE 565 Computer Security (class size 110): TA and design CTF challenges. Jan. 2023 - May 2023

Graduate Research Assistant, Cacti Lab, Rochester Institute of Technology — August 2019 – August 2020
- Embedded systems, TEEs, CTFs, systems security, and FPGA.

Software Engineer, Full Stack, BJIT, Bangladesh — July 2017 – August 2019
- Spring MVC, Spring Boot, MySQL, and Java Script

PUBLICATIONS

1 **MD Armanuzzaman**, Ahmad-Reza Sadeghi, Ziming Zhao. "Building Your Own Trusted Execution Environments Using FPGA". *ASIA Conference on Computer and Communications Security (ASI-ACCS), 2024.* [*code link*] (129/585 = 22.1% acceptance rate)

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

3 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". *ACM/SIGAPP Symposium On Applied Computing (SAC) 2024.* (180/773 = 23.3% acceptance rate)

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

WORKING-IN-PROGRESS PAPERS

1 **MD Armanuzzaman**, Ziming Zhao. "Enola: Efficient Control-Flow Attestation for Embedded Systems". Being Submitted to USENIX Security Symposium 2025.

2 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". Under review in Network and Distributed System Security (NDSS) Symposium 2025.

3 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". Under review in USENIX Security Symposium 2025.

4 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". Under review in INFOCOM 2025.

5 **MD Armanuzzaman**, Ahmad-Reza Sadeghi, and Ziming Zhao. "BYOTee: Towards Building Your Own Trusted Execution Environments Using FPGA" (Journal Version).

6 Rui Zhang, Jian Wang, Nan Jiang*, **MD Armanuzzaman**, and Ziming Zhao, "Quantum Federated Learning Based on Multi-qubit Quantum Broadcast Protocol (MQBP-QFL)".

7 **MD Armanuzzaman**, Ziming Zhao. "HLSSec: FPGA High-Level Synthesis Security".

PATENT

1 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*

SELECTED AWARDS AND HONORS

- MITRE eCTF, team member of Cacti @ UB 2024
  - Ranked 4 among 100 teams. Medical infrastructure supply chain security solution on Tiva-C board, and hacking other teams. [*code link*]
- MITRE eCTF, team member of 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 link*]
- MITRE eCTF, team captain of 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 link*]
- MITRE eCTF, team captain of Cacti @ UB 2021
  - Ranked 9 at final among 20+ teams in MITRE eCTF. 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 link*]
- MITRE eCTF, team member of Cacti @ RIT 2020
  - Ranked 6 at final 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 link*]
- University faculty dean award, Khulna University of Engineering & Technology 2017

PROFESSIONAL SERVICES

- Artifact Evaluation Committee Member at ACM Conference on Computer and Communications Security (CCS) 2024
- *CTF Training, University at Buffalo/Rochester Institute of Technology* 2019 – 2023
- *External Reviewer*: ACM ASIA Conference on Computer and Communications Security (ASIACCS), Conference on Data and Application Security and Privacy (CODASPY), IEEE International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom), IEEE International Conference on Cloud Computing Technology and Science (CloudCom), IEEE Workshop on the Internet of Safe Things.

TRAVEL GRANTS

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

PRESENTATIONS

- **Paper presentation** at *International Symposium on Secure and Private Execution Environment Design (SEED)* 2024
  - Trusted Execution Environments in Embedded and IoT Systems: A Perspective.
- **Talk** at *Great Lake Security Day (GLSD)* 2021
  - Building Your Own Trusted Execution Environments Using FPGA.
- **Talk** at *International Conference on Secure Knowledge Management (SKM)* 2021
  - Work-in-Progress: Building Your Own Trusted Execution Environments Using FPGA.

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