MD Armanuzzaman

Davis Hall 309
University at Buffalo
Buffalo, NY, 14228

E-mail: mdarmanu@buffalo.edu
Homepage: tomal-kuet.github.io
Ph: +15857527756

EDUCATION

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

Ph.D Student, Computing and Information Science — Rochester Institute of Technology, NY, USA
- Advisor: Ziming Zhao — August 2019 - August 2020

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

PROFESSIONAL EXPERIENCE

Graduate Research Assistant, Cacti Lab, University at Buffalo — August 2020 – Present
- 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 2020 - 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
- Built background on embedded systems, TEEs, CTFs, systems security, and FPGA.

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*]

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.*

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.*

PATENT

1 Ziming Zhao, **MD Armanuzzaman**. "Building Your Own Trusted Execution Environments Using FPGA". *USA: Full patent filled in November 2023.*

WORKING-IN-PROGRESS PAPERS

1 **MD Armanuzzaman**, Ziming Zhao. "Enola: Efficient Control-Flow Attestation for Embedded Systems".

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

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

4 Zheyuan Ma, Gaoxiang Liu, Kai Kaufman, Katherine Jesse, Xi Tan, **MD Armanuzzaman**, Robert Walls, Ziming Zhao. "On the Challenges and Pitfalls in Securing Microcontroller-based Systems".

SELECTED AWARDS AND HONORS

- 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

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).

PROFESSIONAL SERVICES

- *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.

PRESENTATIONS

- **Talk** @ *Great Lake Security Day (GLSD)* Spring 2021
  - Building Your Own Trusted Execution Environments Using FPGA.
- **Presentation**: Research-in-progress presentation at SKM. Fall 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 & dynamic analysis
- **Competitive Programming:** UVA OJ(Tomal.kuet): 100+, Codeforces: 180+, Leetcode: 50+

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

INTERESTS

Hiking, camping, sports, traveling, and tech blogs