MD Armanuzzaman

498 Minnesota Ave, Buffalo, NY 14215

5857527756 mdarmanu@buffalo.edu linkedin.com/in/armanuzzaman-tomal/ github.com/Tomal-kuet

Education

University at Buffalo **Aug. 2020 – Present**
Ph.D. in Computing Science and Engineering *Buffalo, NY*

Rochester Institute of Technology **Aug. 2019 – Aug. 2020**
Ph.D. in Computing and Information Science *Rochester, NY*

Khulna University of Engineering & Technology **Mar. 2013 – April. 2017**
Bachelor of Science in Computer Science and Engineering *Khulna, Bangladesh*

Research Area

- Cybersecurity
- Systems Security
- Software Security
- OS Security
- Embedded Architecture
- Information Security
- Fuzzing
- Network Security

Professional Experience

Cactilab **Aug. 2019 – Present**
Research Assistant *UB, RIT*

- Research assistant with a focus on embedded systems security, software security, OS security, etc.

University at Buffalo **Aug. 2021 - May 2023**
Teaching Assistant: Developed own CTF platform & challenges (100) *University at Buffalo*

- Teaching assistant for Software Security (Class size 60)
- Teaching assistant for Computer Security(Class size 110)

BJIT Group **July 2017 – August 2019**
Software Developer (Full-stack) *Dhaka, Bangladesh*

- Assisted in developing an ERP system for the Finnish company Valmet.
- Worked on Java frameworks: Spring Boot, Spring MVC, Struts for back-end development

Publications

BYOTee: Towards Building Your Own Trusted Execution Environments Using FPGA. | *ASIACCS, Code repository*

- **MD Armanuzzaman**, Ziming Zhao
- Accept in ASIA Conference on Computer and Communications Security (ASIACCS) 2024

Is the Canary Dead? On the Effectiveness of Stack Canaries on Microcontroller Systems.

- Xi Tan, **MD Armanuzzaman**, Sagar Mohan, Zheyuan Ma, Gaoxiang Liu, Alex Eastman, Hongxin Hu, Ziming Zhao
- Accepted in ACM/SIGAPP Symposium on Applied Computing (SAC) 2024

A secure and efficient data transmission technique using quantum key distribution. | *NSysS'17*

- **MD Armanuzzaman**, Kazi Md. Rokibul Alam, Md. Mehadi Hassan
- International Conference on Networking, Systems and Security (NSysS), 2017

Efficient Hardware Assisted Control Flow Attestation. | *Work-In-Progress*

- **MD Armanuzzaman**, Ziming Zhao

Research Projects

BYOTee: Towards Building Your Own Trusted Execution Environments Using FPGA. | *Code repository*

- **Research question:** Open-sourced and proprietary TEEs such as ARM TrustZone or Intel SGX suffer from various drawbacks: single TEE (TrustZone), software TCB bloating, high context switching overhead, no trusted paths for peripherals, cache side-channel, and cold boot attacks, etc. Can we design a hardware configurable TEE framework with minimal software TCB, no resource sharing, and multiple enclave support?
- **Solution:** Designed BOTee applicable to cloud & SoCs, a TEE framework where the enclaves are hardware configurable, supports multiple enclaves, minimum software TCB, concurrent execution TEE and REE apps, reduced switching overhead, etc. BYOTee uses FPGA resources to construct multiple enclaves, while the REE applications execute in traditional hardcore processors. Hardware isolation and carefully designed software implementation resolves the mentioned issues of current TEEs.

Efficient Hardware Assisted Control Flow Attestation. | *Work-In-Progress*

- **Research question:** Current CFA approaches utilize software-based attestation reports, which are neither efficient nor practical solutions for embedded systems. Frequent interaction with TrustZone hampers the performance a lot. Can we design a more efficient and deployable CFA for embedded systems?
- **Solution:** We utilize ARM hardware security extension Pointer Authentication (PA), which provides a hardware trusted module to compute cryptographic hashes on instruction or data pointers. Also, developing LLVM passes to generate runtime control flow measurements of a user application and its outputs, reduces the context switching overhead.

Is the Canary Dead? On the Effectiveness of Stack Canaries on Microcontroller Systems. | *SAC'24*

- **Research question:** Most embedded systems do not support stack canaries or use fixed canary values due to resource constraints, resulting in either no stack smashing detection or low entropy in the canary value.
- **Solution:** Evaluate the current security state of stack canaries for microcontrollers accross RTOSs, libraries, compilers, and system layers, and lastly propose probable solutions.

Open-sourced project repositories

MITRE eCTF competition | *Embedded capture the flag competition* **Spring 2020-2023**

- Secure car key fob system development and hacking: Fourth place - code
- Designing a secure bootloader for firmware and hacking: Fifth place - code
- Secure UAV communication system design and hacking: Sixth Place - code
- Ensuring digital rights management for music player and hacking: Ninth Place - code

Image reconstruction | *Matlab* **Nov. 2020**

- Implementation of reconstructing images with significant eigenfaces: code

Esho_Shikhi | *Java* **Mar. 2014**

- A desktop application that makes children's education more interesting: code

Wireless PC Controller | *Android* **June 2016**

- An android application to operate various functions of a computer through Wi-Fi network: code

File-share | *ASP* **Oct. 2014**

- A website to share files with group members and to avoid unwanted access: code

Technical Skills

Languages: C, C++, Assembly, Shell, Python, Java, JavaScript, SQL, VHDL, Verilog
Technologies/Frameworks: Linux, Docker, 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, SQL Injection, Cross-site scripting, DOM-based faults, Access control, and Web cache poisoning.
Competitive Programming: UVA OJ(Tomal.kuet): 100+, Codeforces: 180+, Leetcode: 50+

External Paper Reviewer & Talks

- Sub-reviewer at IEEE International Conference on Cloud Computing Technology and Science (CloudCom). **2022**
- Conference on Data and Application Security and Privacy (CODASPY). **2020, 2022**
- IEEE Workshop on the Internet of Safe Things. **2023**
- International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). **2023**
- BYOTee: Building Your Own Trusted Execution Environments Using FPGA at Great Lakes Security Day (GLSD) **2021**

Awards & Achievements

- Best write-up award in MITE eCTF 2021.
- Travel grant for NDSS 2021, SKM 2021
- University Faculty Dean Award in the session 2015-16

Team participation / Extracurricular

Cactilab hacking group **Fall 2019 – Present**

University at Buffalo

- Manage a hacking group to work on binary, web CTF challenges (Graduate & Undergraduate)
- Participate in MITRE embedded CTF competition: involves secure system development and hacking phase