MUSTAKIMUR RAHMAN KHANDAKER

Email: mustakcsecuet@gmail.com — Phone: (850) 999-3635 — Milpitas, CA 95035
Website: mustakim.info — GitHub: github.com/mustakimur — LinkedIn: linkedin.com/in/mrk15e

TECHNICAL SKILLS

Coding:	C/C++, Rust, Java, Android/Kotlin, Python, JavaScript, Bash
Architectures:	x86-64, ARM64, RISC-V, MIPS
Systems & Virtualization:	Linux Kernel, AOSP, QEMU, Docker
Security Assessment:	AFL++/LibFuzzer, Cargo-Fuzz/afl.rs, Syzkaller/OSS-Fuzz, Metasploit
Binary Analysis:	Ghidra/Radare2, Capstone/Unicorn/Dyninst, Angr/Triton, ADB/GDB/LLDB
Platform Security:	Intel SGX/MPK/CET/TSX, ARM TrustZone/PAC/MTE
Frameworks & Tooling:	Clang/LLVM, eBPF/SELinux, Qiling/Frida/Scapy, SQLite, Rocket, Git, CI/CD
AI Agents & Security:	LangGraph/PyTorch, PromptFuzz/FuzzIntrospector, ARTKIT/Garak/Promptfoo

WORK EXPERIENCE

Staff Security Research Engineer — Jun 2025 – Present
Enterprise and Security Innovation Lab, Samsung Research America

- **Knox Zero Trust Framework:** Architected the framework's telemetry engine and defined threat metric scopes mapped directly to MITRE ATT&CK. Designed lightweight, on-device threat detection for resource-constrained environments, authored incident response playbooks, and led code reviews to scale production performance.
- **Knox Ultra (Android OS):** Hardened network and browser subsystems to block web- and network-level exploits. Reduced driver and application attack surfaces. Proposed RKP (Real-time Kernel Protection) extension with MTE (Memory Tagging Extensions) to enhance kernel-level memory protection.
- **Knox Secure Agent:** Designed a hardened multi-agent AI orchestration architecture for Android. Prototyped a SELinux-enforced IPC reference monitor to eliminate tool-routing vulnerabilities and developed PoCs for non-human identity & credential management.
- **AI Red Teaming:** Identified a new class of multi-agent cascading exploits to exfiltrate cross-app data. Developed indirect prompt injection exploits across Calendar, SMS, and Web interfaces.
- **Enterprise Security Initiatives:** Designed a sensor data provenance engine, developed real-time shellcode exploit detector, and directed university research collaborations.

Assistant Professor of Cybersecurity — Aug 2020 – May 2025
School of Computing, University of Georgia

- **Research:** Directed an independent systems security lab, publishing peer-reviewed research. Advised and mentored 2 Ph.D. and 4 M.Sc. students. Served as a proposal and journal reviewer for NSF-SaTC-TTP, TDSC, and ACSAC.
- **Teaching:** Taught graduate and undergraduate courses in Secure Programming, Cybersecurity, and Computer Networks. Served on the Graduate Admissions and Curriculum Committees.

Security Research Intern — May 2019 – Aug 2019
X-Lab, Baidu USA

- **Intel SGX Security:** Introduced "COIN Attacks," a novel class of interface vulnerabilities targeting Intel SGX secure enclaves. Developed an LLVM/Clang-based analysis tool to dynamically detect multi-turn execution and input manipulation flaws at untrusted boundaries.

Graduate Research & Teaching Assistant — Aug 2015 – Jun 2020
Department of Computer Science, Florida State University

- **Compiler-Enforced Software Defense:** Researched Control Flow Integrity (CFI) and automated binary analysis. Developed compiler-driven software defenses to mitigate systems vulnerabilities, resulting in top-tier publications.

Senior Android Software Engineer — Dec 2012 – Jun 2015
Samsung Research & Development Institute, Bangladesh

- **Architecture Draw, Sketch, Paint:** Developed the drawing canvas UI with layer management, multi-touch scaling/zooming, an undo/redo engine, and local file storage and image export features.
- **PIMS Applications:** Implemented drag-and-drop event creation, SNote stylus integration, and chat features for calendar app; triaged and resolved over 500 bugs across the Samsung Calendar, Clock, and Calculator codebases.
- **Team Development:** Led technical training sessions and conducted regular code reviews for team members.

EDUCATION

Ph.D. in Computer Science — **Jun 2020**
Florida State University, United States — Research Focus: System & Software Security

B.Sc. in Computer Science & Engineering — **Oct 2012**
Chittagong University of Engineering & Technology, Bangladesh — Thesis: Android Development

SELECTED PUBLICATIONS

[1] "RustLIVE: Reducing the Learning Barriers of Rust Through Visualization," *IEEE Frontiers in Education Conference (FIE)*, **2024**.

[2] "Understanding the Challenges in Detecting Vulnerabilities of Rust Apps," *IEEE Secure Development Conference (SecDev)*, **2024**.

[3] "COIN Attacks: On Insecurity of Enclave Untrusted Interfaces in SGX," *International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, **2020**.

[4] "Origin-sensitive Control Flow Integrity," *USENIX Security Symposium*, **2019**.

[5] "Adaptive Call-site Sensitive Control Flow Integrity," *IEEE European Symposium on Security and Privacy (EuroS&P)*, **2019**. **[Best Paper Award]**

[6] "Pinpointing Vulnerabilities," *ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, **2017**.

[7] "Location based early disaster warning and evacuation system on mobile phones using OpenStreetMap," *IEEE International Conference on Open Systems (ICOS)*, **2012**.

SELECTED TECHNICAL PROJECTS

PTOPlanner: Privacy-First Paid Time Off Application — **2026**
Android Application (Open-source)

- Built an open-source Android application with interactive PTO tracking and balance forecasting. Implemented a local RAG pipeline powered by an on-device LLM to provide secure, offline schedule intelligence.

Ponjika: A Rust crate for Bengali Calendar — **2024**
Rust (Open-source Crate)

- Implemented a Bengali calendar library in Rust, providing precise epoch date conversions and flexible calendar handling configurations.

Graduate Admission & Review System — **2019**
Full-Stack Web Application (Open-source)

- Developed a memory-safe web application to support the graduate admission review pipeline at FSU, incorporating defense-in-depth principles to securely handle sensitive academic profiles.

SELECTED VULNERABILITY DISCLOSURES

[1] **CVE-2024-37824:** A buffer overflow in *md2roff v1.11.*, **2024**.

[2] **Git Issue #1803:** An integer overflow panic error in *Speedy Web Compiler (SWC)*, **2021**.

[3] **Git Issue #456:** A use-after-free on *Intel SGX Confidential Computing* SQLite library, **2019**.

HONORS & AWARDS

2024	Career Development Influencer Award, University of Georgia
2019	**Best Paper Award**, IEEE European Symposium on Security and Privacy (EuroS&P)
2019	Graduate Research Assistant Award, Florida State University
2018	Graduate Teaching Assistant Award, Florida State University
2017–2019	Top Finisher, Competitive Programming League, ACM @ FSU

PROFESSIONAL REFERENCES

Dr. Hayawardh Vijayakumar
Director & Manager
Enterprise & Security Innovation Lab
Samsung Research America

Dr. Roberto Perdisci
Professor & Director
School of Computing
University of Georgia

Dr. David Whalley
Professor & Committee Chair
Department of Computer Science
Florida State University