Shariful Alam, Ph.D.

Santa Clara, CA, USA | 409-466-9596 | alam.shariful@hotmail.com | linkedin.com/in/shariful-alam-162267114/

PROFESSIONAL SUMMARY

Senior Security and Crypto Engineer with a Ph.D. in Cyber Security and 5+ years of experience building software for hardware-backed security, data privacy, and applied cryptography. Specializes in firmware development and Trusted Execution Environments (TEEs). Experienced in launching secure products, executing vulnerability assessments, and managing security initiatives across complex hardware architectures.

TECHNICAL SKILLS

Languages: C, C++, Python, Java, x86 Assembly, Shell Scripting.

Hardware & Firmware Security: Trusted Execution Environments (TEEs), Secure Boot, Hardware Root of Trust, Zephyr RTOS, Cloud HSM, Compute Express Link (CXL).

Cryptography: OpenSSL, MbedTLS, PKI, Symmetric/Asymmetric Cryptography, Threat Modeling, Firmware Signing.

Tools & Frameworks: Linux Kernel Internals, GDB, Docker, Git, CMake, Unit Testing, Synopsys Virtualizer Development Kits (VDKs).

WORK EXPERIENCE

Marvell Semiconductor, Inc — **Santa Clara, CA, USA**
Senior Security and Crypto Engineer — *August 2022 - Present*

- Designed and implemented firmware signing and provisioning flows for internal chip bring-up. This included defining how firmware images are verified before execution on early silicon.
- Worked on firmware for CXL-based systems, focusing on secure handling of CXL as well as vendor-specific requests, and implemented Zephyr-based IPC for secure core-to-core communication.
- Validated CXL device performance by executing comprehensive hardware benchmarks using the Memory Latency Checker (MLC) tool.
- Worked closely with hardware and validation teams to debug system-level issues using logs, GDB, and targeted experiments on pre-production hardware.
- Supported early silicon bring-up by building a VDK-based firmware testing framework, utilizing gtest unit testing framework to detect and resolve code quality issues.
- Supported the agile release cycle for Cloud HSM manufacturing kits to maintain and launch critical software products.

Boise State University — **Boise, Idaho, USA**
Cyber Security Researcher / Graduate Assistant — *January 2019 - May 2022*

- Developed a novel virtualization-based architecture for kernel and userspace system hardening, mitigating targeted kernel-level exploits.
- Debugged C-based OpenSSL source code using GDB to isolate memory leaks and improve the stability of secure communication protocols.
- Deployed an Apache web server with HTTPS and digital certificates to enforce robust Public-Key Infrastructure (PKI) standards.
- Developed custom kernel rootkits and device drivers to secure the system call table against unauthorized hooking techniques.

PROJECTS

Virtualization-Based Trusted Execution Environments (TEEs)

- Developed a secure OpenSSL engine using C, MbedTLS, multithreading, and KVM source modifications to establish hardware-backed security features and prevent physical memory extraction attacks.

EDUCATION

Ph.D. in Computing (Cyber Security) | *Boise State University, Boise, Idaho* — *May 2025*
Master of Science in Computer Science | *Lamar University, Beaumont, Texas* — *December 2018*

PUBLICATIONS

- **CAUSEC: Cache-based Secure Key Computation with (Mostly) Deprivileged Execution** – 2023 IEEE 43rd International Conference on Distributed Computing Systems (ICDCS '23).