Muhammad Hammad Bashir

Ph.D. Student, Computer Science
PSecLab, The Pennsylvania State University
Website ◇ GitHub ◇ LinkedIn ◇ hammad.bashir543@gmail.com ◇ +1 (814) 280-5551

Research Interests

Firmware and embedded-system security, firmware rehosting and emulation, binary analysis, hardware and software security, and side-channel analysis.

Research & Professional Experience

The Pennsylvania State University — Pennsylvania, USA
Ph.D. Student, PSecLab; Advisor: Prof. Arslan Khan — *Aug 2025 – Present*

- **BoardRunner (ACM CCS 2026):** Developed a framework for LLM-assisted firmware rehosting using high-fidelity compositional device models, enabling scalable execution and analysis across 5+ MCU platforms (STM32, NXP).
- Ported *HALucinator* to an in-house QEMU execution backend, replacing its avatar^2/GDB debugger-in-the-loop architecture; up to 12× faster rehosted execution on its bundled example targets.
- **Agent-Orchestrated Firmware Rehosting:** Building an automated workflow that coordinates firmware analysis, execution diagnostics, peripheral/model resolution, and iterative emulation refinement; rehosted production-scale ArduPilot ArduRover on ChibiOS.
- **µLEAK:** Investigated cache-timing leakage across MPU isolation boundaries on ARM Cortex-M7; evaluated software mitigation effectiveness and overhead.

10xEngineers — Lahore, Pakistan
RISC-V Compliance Verification Engineer – Open Source Contributor — *Mar 2023 – Jul 2025*

- Led a three-person effort building the platform-level verification environment and test suite for replacing ARM Cortex-A5 with the RISC-V CVA6/Ariane core in the SSE-500 subsystem.
- Developed directed tests verifying the RISC-V platform-level interrupt controller (PLIC) and core-level interrupt controller (CLINT) in that subsystem.
- Authored assembly architecture tests and covergroups in the official RISC-V Architecture Tests for Physical Memory Protection (PMP), virtual memory (SV32/SV39), interrupts, and atomic extensions.
- Extended RISC-V Privileged Architecture support in RISCOF with Allen Baum (Vice-Chair, RISC-V ISA Infrastructure HC), implementing static signature embedding for self-verifying compliance tests; upstreamed to RISC-V Arch Tests, RISCOF, and the RISC-V Sail model.

Publications

Peer-Reviewed Conference Publication

- Muhammad Hammad Bashir, Michael Rooney, Colin Smith, Dongyan Xu, Arslan Khan. BoardRunner: Automatic Firmware Rehosting using High-Fidelity Compositional Device Models. In *the 33rd ACM Conference on Computer and Communications Security (CCS)*, 2026. **Accepted; to appear.**

Extended Abstracts

- Muhammad Hammad Bashir, Taegyu Kim, Arslan Khan, Kyungtae Kim. µLEAK: Bypassing MPU Isolation on Cortex-M7 via Cache-Timing Attacks. In *the Non-Volatile Memories Workshop (NVMW)*, Santa Clara, 2026.
- Muhammad Hammad Bashir, Umer Shahid, Muhammad Tahir, Yazan Hussnain, Fatima Saleem. Verification of CoreSwap: Replacing ARM Cortex-A5 with RISC-V CVA6 in ARM SoC Environment. In *the RISC-V Summit Europe*, Paris, France, 2025.
- Muhammad Hammad Bashir, Umer Shahid, Allen Baum, James Shi. Static Signature Embedding: Self-Verifying RISC-V Architecture Compliance Tests. In *the RISC-V Summit China*, Hangzhou, China, 2025.

Education

The Pennsylvania State University — Pennsylvania, USA
Ph.D. in Computer Science; GPA: 4.00/4.00; Advisor: Prof. Arslan Khan — *Aug 2025 – Expected 2030*

University of Engineering and Technology, Lahore — Lahore, Pakistan
B.S. in Electrical Engineering; GPA: 3.41/4.00 — *Oct 2020 – May 2024*

Security Experience & Competitions

DARPA FIRE Hackathon 2026

Faithful Integrated Reverse-engineering and Exploitation

- Reverse-engineered 100 corrupted and obfuscated embedded binaries to recover processor architecture, vendor/platform, and firmware family, including ArduPilot and Betaflight identification.
- Built a Capstone-based disassembly and classification pipeline on-site, prototyped with LLM assistance, that returned correct identifications for 70–75% of targets.
- Cross-validated pipeline output against teammates' Binary Ninja analyses to confirm attributions; the seven-person team's submission won the competition.

MITRE Embedded Capture the Flag (eCTF) 2026

- Led Penn State's five-person team and designed the security architecture for a hardware security module (HSM) providing secure file storage and transfer on the MSPM0L2228 board.
- Coordinated system design, implementation, and security analysis across the defensive design and offensive evaluation phases; the team placed 22nd of 119 teams.

CyberAuto Challenge 2026

- Conducted authorized security analysis of EV charging infrastructure and identified multiple security-relevant weaknesses across embedded/Linux system components and configuration boundaries.
- Validated findings through proof-of-concept testing and reported them under NDA.

Technical Skills

Programming: C/C++, Python, Bash, RISC-V Assembly
Firmware & Embedded Security: Firmware rehosting, peripheral/MMIO modeling, binary analysis and reverse engineering, fuzzing, side-channel analysis, JTAG/SWD debugging
Emulation, Debugging & Analysis: QEMU/TCG, FastDyn/BoardRunner, HALucinator, avatar^2, GDB, OpenOCD, ST-Link, execution tracing, coverage analysis
Embedded Systems & ISA Tooling: ARM Cortex-M, RISC-V, STM32, ChibiOS/RTOS, SPI, I2C, UART, DMA, GPIO, interrupts, RISCOF, RISC-V Architecture Tests, Sail, Spike, SystemVerilog

Academic Service

- **Artifact Evaluation Committee, USENIX WOOT 2026** — Evaluated research artifacts for functionality, reproducibility, and validation of reported results.

Honors & Awards

- **Student Travel Grant** — RISC-V Summit North America, 2025.
- **CodeMaster Coding Competition** — 1st position among 100 participants, UET Lahore, 2023.

Talks & Tutorials

- **Tutorial:** *"Embedded Systems with RISC-V: Bare-Metal Firmware Development for CH32V003 Microcontrollers"*, RISC-V Community Event, Lahore, Pakistan, November 2024.