Errol Pascua

Chandler, AZ · (480) 252-4571 · errol.pascua99@gmail.com
linkedin.com/in/errol-pascua · errolpascua.com

SUMMARY

Embedded security engineer with **4+ years** of experience designing, validating, and automating hardware-accelerated cryptographic systems for production microcontrollers. Expertise spans secure boot, key provisioning, HSM/HSM-Lite architectures, and compliance-driven development (MISRA-C, ASPICE, ISO-21434).

CORE SKILLS

Embedded Security: Secure Boot, Key Provisioning, Trust Anchors, ROM-backed Keys, HSM/HSM-Lite
Cryptography: AES, SHA-1/2, CMAC, HMAC, GMAC, ECDH, ECDSA, RSA, ChaCha20, TRNG, PKE
Standards: ACVP, MISRA-C, ASPICE SWE1–SWE3, ISO-21434
Languages: C, C++, Python, Assembly

EXPERIENCE

Microchip Technology Inc. — Chandler, AZ

Embedded Software Engineer, Cryptography & Security · Jan 2022 – Present

Embedded Security & Cryptographic Systems

- Designed and maintained low-level cryptographic hardware drivers across multiple microcontroller families.
- Implemented and validated hardware-accelerated AES, SHA-1/2, CMAC, HMAC, GMAC, RSA, ECDH, ECDSA, ChaCha20, TRNG, and PKE primitives.
- Architected wrapper layers aligning device-specific implementations with Microchip Crypto v4 APIs, supporting HSM-backed and WolfSSL software fallbacks.
- Strengthened secure boot and key provisioning by migrating sensitive keys from volatile RAM to non-volatile, ROM-backed trust anchors.
- Debugged cryptographic state machines, DMA interactions, and ISR paths using register-level analysis.

Verification, Compliance, & Automation

- Built host-executed, hardware-mocked unit testing frameworks using Unity, CMake, GCC/MinGW, and Python.
- Implemented GCOV-based coverage reporting and automated regression testing to support ASPICE and ISO-21434.
- Authored ASPICE SWE1–SWE3 artifacts including requirements, architecture, design, and verification matrices.
- Ensured MISRA-C compliance via automated static analysis using Cppcheck Premium and MPLAB X MISRA tooling.
- Developed Python-based tooling to automate builds, device configuration, and static library generation.

Southwest Engineering Concepts — Chandler, AZ

Engineering Intern · Sep 2021 – Jan 2022

- Developed embedded sensor systems using accelerometer and gyroscope data for real-time event detection.
- Designed and prototyped inductive measurement and monitoring systems, performing full hardware bring-up and validation.
- Implemented embedded firmware in C for STM32 and Microchip microcontrollers using datasheets and reference manuals.

EDUCATION

Arizona State University, Tempe, AZ — B.S.E. Computer Systems Engineering (Cybersecurity), May 2021