Ehsan Koohestani

Toronto area, Ontario, Canada 2267895375
koohestani.ehsan@gmail.com

Experience

Firmware Developer/ Team Lead Oct 2018 – Present
Advanced Micro Devices (AMD) - Platform Security Processor (PSP) team *Markham, Ontario, Canada*

- Led migration and developed firmware to re-architect BootROM, Bootloader, and TEE OS (AMD Runtime OS) to support RISC-V ISA, in addition to ARM A5 ISA.
- Proposed and implemented architectural enhancement for lower layers of the TEE OS to optimize the use of RISC-V core features (such as thread scheduling, MMU, cache management, interrupts/exceptions, etc.).
- Implemented a dGPU Bootloader boot flow for AMD Security Processor which supports new features with minimal maintenance and overhead in collaboration with PSP internal and external teams.
- Devised and implemented an innovative debugging and benchmarking method for AMD Secure Processor known as Secure Trace Log.
- Formulated a comprehensive system-level proposal and integrated Device Identifier Composition Engine (DICE) layering architecture for SPDM applications. This initiative covers BootROM, Bootloader and TEE OS implementations. Materialized the proposal in a Server product that covers FW/ HW implementations and a successful end-to-end automated validations for both Provisioning mode and mission mode.
- Designed architecture and led an implementation team for DICE Protection Environment (DPE) for modern generation of Server products based on TCG iROT Profile. The architecture impacts AMD RoT as well as AMD Security Processor and x86 driver.
- Scaled Caliptra DPE (TCG reference code) implementation from Rust code into C with a wrapper. Designed test cases, validated DPE commands based on AMD use-cases and reported many bugs/ improvements to the Caliptra WG.
- Initiated Rust code transition in AMD TEE by design and implementing a Trusted Application for DPE with minimum overhead. It involves full functionality of driver which cohabited with C code, interoperability with Kernel/ OS and other TAs and bench-marking (code size, stack/ heap usage, performance, etc). Teamed up Rust Committee and delegated other Rust-based TAs to new owners.
- Threat modeling and analyzed few critical features that require X.509 certificate as remote/ local identifications (link encryption, multi-client DPE services, etc). Ultimately, provided proposal to improve the security level of Server and GPU products by mitigating vulnerabilities.
- Integrated FWs to use AMD Crypto engine based on TEE APIs for EC-DSA, EC-DH, RSA-PSS, AES-GCM, etc operations for SPDM Open Source project. Designed and implemented creative test units with and without Hyperprovisor donated memory for SEV-TIO use-case.
- Identified security vulnerabilites in SEV-TIO FW code for EPYC family (DMTF SPDM usage, X.509 parser, PCIe topology discovery in multi-node cases, etc) and proposed optimized solutions. Removed many redundant source codes to promote the security quality.
- Executed SEV-TIO attestation from requirements discovery to implementations for modern EPYC products including TCG DICE/DPE, TCB selections, Ownership authorization and transfer, uCode authentications, multi-node link encryptions, etc. This execution includes 6 engineers from 4 teams.
- Identified security issues related to AMD RoT hitless Firmware Update in fusion with the attestation requirements. Proposed a solution with minimum impact on AMD hardware, BootROM changes and Firmware.
- Represented the PSP team during the pre-silicon phase of successful programs such as Vega20, Mi100, Mi200, Mi300/ Mi350, Turin, Venice and contributed to their bring-up.
- Created and implemented a secure register whitelist mechanism to be accessed by an x86 driver via RAS (Reliability, Availability, and Serviceability) Trusted Application.
- Proposed and implemented a mechanism to minimize boot-up time by utilizing the DMA engine in multi-queue mode. Improvement of 15 percent in total.

- Identified security issues flagged by third-party auditors, suggested potential solutions with minimal architectural costs.
- Provided feedback to the CI/CD team to understand the requirements of the PSP team FW stacks.
- Served as a dependable team member for debugging critical issues associated with cryptographic engines, TEE OS, and Bootloader. Identified multiple HW issues during Pre-Silicon phase (simulation and emulation) and recommended solutions.
- Published internal secure coding guidelines and code styles. Actively engaged in conducting an internal system-level security audit of FW stacks and recommended techniques for optimizing FW footprint vs. performance.
- Demonstrated measurable leadership by mentoring a wide range of newly hired engineers while driving key security firmware initiatives. Acted as a primary point of contact for the security firmware team, offering strategic guidance and cross-functional consultation across AMD. Spearheaded the development and integration of security technologies such as DICE/ DPE, SPDM, and Trusted Execution Environments (TEEs), ensuring robust platform integrity and alignment with industry standards.

System and Hardware Engineer/ Team Lead Feb, 2015 – Oct, 2018

Onsemi (ON Semiconductor) *Waterloo, Ontario, Canada*

- Contributed as a system level designer of a multi-disciplinary team in the design of a Bluetooth Low-Energy IC for IoT and hearing aid applications.
- Implemented the audio path for a proprietary protocol between two ICs, utilizing an ASRC engine and an auto-correction/compression algorithm to achieve the required level of quality.
- Designed and implemented the audio path for a chip with MFi communication capability, including left/right audio synchronization for hearing aids and techniques to reduce artifact effects.
- Served as team lead in designing and implementing sample codes for BLE, audio path, and ports for a new chip.
- Created test plans for verification of several interfaces, including UART, I2C, SPI, PCM, PWM, DMA, and audio engines such as Asynchronous Sample Rate Converter and synchronizer, on ARM-CM3, DSP co-processor, and during pre/post tape-out.
- Designed and co-implemented an automated, instrumented testing mechanism to control embedded software and measurement tools using Python, GDB, and JLink.
- Led the RSL10 Firmware team for over a year, mentoring new engineers and co-ops, and providing direct engineering consultation and training to customers.

Embedded System Developer Mar, 2014 – Feb, 2015

CST LAB University of Waterloo *Waterloo, Ontario, Canada*

- Contributed to a team to implement a novel wireless protocol based on Full-Duplex principles.
- Ported a System Generator design to the Logic System side of Zynq-7000 chips and optimized relevant software on the Processor System for a complete OFDM-based band design.
- Developed software device drivers in C/C++ for a Dual-Core ARM Cortex-A9 processor, including for EMAC, UART, I2C, etc., and for radio board devices such as ADC, DAC, PLL, amplifiers, etc.
- Performed the bring-up of an embedded Linux on a Zynq-7000 board and integrated the device drivers and application code for the flexible logic.

Software/ Hardware Designer Oct, 2013 – Jan, 2014

EnviSens Technologies *Turin, Italy*

- Conducted an evaluation of DSP chips and industrial boards based on defined requirements for a meteorological radar application and elected a suitable option.
- Performed the bring-up of a real-time Embedded Linux on a Spartan-6 Eval board and developed customized testing logic.

Firmware Developer May, 2011 – Mar, 2012
Omid Technology *Tehran, Iran*

- Worked as a team member to develop software for an industrial decoder supporting DVB-T, -S, and DVB-ASI standards, utilizing ST Microelectronics products, namely STi5202 and STi7109.
- Generated multitasking software for a real-time operating system (RTOS) and developed device drivers for various peripherals such as I2C, SPI, OSD, UART, GUI, various tuners, and higher-level application programming to achieve a professional video decoder.
- Conducted research on various video stream/DVB standards, STMicroelectronics STB architectures, and operating system software layers.
- Implemented a Simple Network Management Protocol (SNMP) platform to manage decoder status and alarms, using a Lantronix product to enable a Human Monitoring Interface via a network.
- Developed a remote Xilinx configuration mechanism for an AVR microprocessor.
- Created a program to produce a JTAG state machine protocol and implement the FAT32 file system on an SD Card for file management and SPI Flash.

Education & Certifications

Politecnico di Torino 2012 – 2015
M.Sc. in Communication Systems Engineering *Turin, Italy*

Azad University 2000 – 2005
B.Sc. in Telecommunications Engineering *Tehran, Iran*

NCC Group 2018
Secure Coding in C and C++ *Markham, Ontario, Canada*

Awards & Honors

Next 5% Award Breaking Exaflop Barriers
AMD *Q2 2022*

Spotlight Award Distinguished among Security team members
AMD *2019 (1 time), 2020 (1 time), 2021 (3 times), 2023 (2 times), 2024 (4 times), 2025 (1 time)*

Selected Main Presenter Annual Canada Innovation Showcase
AMD *2019, 2023, 2024*

Outstanding Performance Recognition RSL10/ E7150SL contribution
Onsemi *2018*

Specialized Skills

Programming Languages: C (advance), ARM/ RISC-V Assembly (intermediate), Python (intermediate), MATLAB (intermediate), VHDL (beginner), Rust (beginner)
Tools: GCC, armcc, GDB, GIT, Perforce, SVN, WireShark
Instruments: Osciloscope, Digital analyzer, Spectrum-analyzer, BLE sniffer
Methodologies: SCRUM, Agile
Languages: Persian (native), English (bilingual), French (advanced), Italian (beginner)