Ehsan Koohestani

73 Harmonia Cres
Woodbridge, Ontario, Canada, L4L 3Y2

+1 226 789 5375
koohestani.ehsan@gmail.com

Experience

Firmware Developer/ Team Lead Oct 2018 – Present

Advanced Micro Devices (AMD) - Platform Security Processor (PSP) team *Markham, Ontario, Canada*

- Implemented a dGPU Bootloader boot flow that supports new features with minimal maintenance and overhead in collaboration with PSP internal and external team.
- Led migration and developed firmware to re-architect BootROM, Bootloader, and Trusted 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.).
- Devised and implemented an innovative debugging and benchmarking method for AMD Secure Processor known as Secure Trace Log.
- Presented a system-level proposal for integrating features such as Static/Dynamic RoT measurements (DRTM) into the TEE OS.
- Formulated a comprehensive system-level proposal and integrated Device Identifier Composition Engine (DICE) layering architecture for SPDM applications. This initiative covers BootROM, Bootloader and Trusted OS implementations.
- Design architecture and implement end-to-end DICE Protection Environment scheme for new generation of Server products based on TCG iROT Profile.
- Design and implemented pre-silicon and post-silicon end-to-end test plan for DICE. Including the the mission mode and provisioning FW.
- Integrated 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.
- Customized an AMD X.509 parser for SPDM requirements. Hands on RFC specifications for X.509 standard.
- Represented the PSP team during the pre-silicon phase of successful programs such as Vega20, Mi100, Mi200 and Mi300 and contributed to their bring-up.
- Transferred dGPU exclusive features from amd-tee2.0 (AMD proprietary TEE OS) to amd-tee3.0 projects and verified them in the simulator/emulator.
- Created and implemented a secure register whitelist mechanism to be accessed by an x86 driver via RAS (Reliability, Availability, and Serviceability) Trusted Application.
- Collaborated on the design and implementation of a multi-die control network and memory sharing AMD protocol related to PSP.
- Proposed and implemented a mechanism to minimize boot-up time by utilizing the DMA engine in multi-queue mode.
- 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.
- Created Python scripts to increase the team throughput in using GDB to simplify debugging of RISC-V/ARM MMU blocks.
- Created Python scripts to generate certificate signing request (CSR) from DICE parameters and send it to the AMD Key Signing Distribution (KSD) server in a secure manner.
- 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.

- Mentored numerous newly hired engineers and Co-ops. Acted as one of the first points of contact for the security FW team to provide AMD internal consultations.

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

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

- Contributed as part 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
- Co-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 *Wateloo, 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*

Engineers Australia 2009
Assessed as Professional Engineer

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)*

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)