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*

- Co-designed and implemented dGPU Bootloader boot flow to support new features with minimum maintenance and overhead
- Analyzed security issues reported by third-party auditors and proposed solutions with minimum architectural costs
- Leaded migration and developed FW to re-architecture BootROM (immutable code), Bootloader and Trusted OS to support RISC-V ISA along side with ARM A5 ISA
- Provided architectural proposals to improve TEE OS lower layers for better usage of RISC-V core features (thread scheduling, MMU, cache management, interrupts/ exceptions, etc)
- Developed Python scripts in contact with GDB to facilitate debugging of RISC-V/ ARM MMU block
- Designed and implemented an innovative debugging and bench-marking mechanism, called Trace Log
- Provided system level proposal for porting features, as such Static/ Dynamic RoT measurements (DRTM), into TEE OS
- Provided end-to-end system level proposal and implemented features, such as Device Identifier Composition Engine (DICE) layering architecture for SPDM application
- Represented PSP team during pre-silicon phase of many successful programs such as Mi100, Mi200 and Mi300 and contributed in their bring-up
- Ported dGPU exclusive featured from amd-tee2.0 (AMD proprietary TEE OS) to amd-tee3.0 projects and validate those in the simulator/ emulator
- Designed and implemented a secure register white list mechanism to be accessed by x86 driver via RAS (Reliability, availability and serviceability) Trusted Application
- Co-designed and implemented multi-die control network and memory sharing AMD protocol, related to PSP
- Provided proposal and implemented a mechanism to minimize boot-up time by using DMA engine in multi-queue mode
- Provided feedback to CI/CD team to understand requirements of PSP team FW stacks
- Standing as a reliable team member for debugging critical issues related to Crypto-graphic engine, TEE OS and Bootloader. Discovered multiple HW issues during Pre-Silicon phase (simulation and emulation) and proposed solutions
- Published internal secure coding guidelines and code styles. Committed actively to provide internal system level security audit for FW stacks as well as techniques to keep optimization of FW footprint vs performance
- Mentored many new hired engineers and Co-ops. Standing as one of the first contacts of security FW team to provide AMD internal consults

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

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

- Contributed in a multi-disciplinary team to design a Bluetooth Low-Energy IC for IoT and hearing aid applications
- Implemented audio path for a proprietary protocol between two ICs with a sophisticated audio synchronization mechanism. Used ASRC engine alongside with an auto-correction/ compression algorithm to reach to maximum quality that was required
- Co-designed and implemented audio path for a chip with MFi communication capability: left/ right audio synchronization for hearing aids, techniques for reducing the artifacts effects, etc
- Designed and implemented sample codes for BLE, audio path and ports for a new chip as a team-lead

- Designed and implemented test-plans for verification of several interfaces (UART, I2C, SPI, PCM, PWM, DMA, etc) on ARM-CM3, DSP co-processor (an audio compression algorithm) and audio engines (Asynchronous Sample Rate Converter, synchronizer, etc) during pre/post tape-out
- Designed and co-implemented an automated instrumented testing mechanism to control the embedded software and the measurement tools using Python, GDB and JLink
- Leaded RSL10 Firmware team for over a year. Mentored many new hired engineers and Co-ops. Been in direct contact with costumers to provide engineering consultation and training

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 principals
- Ported a System Generator design Logic System side of Zynq-7000 chips and refined relevant software on Processor System for a complete OFDM based-band design
- Developed software device drivers in C/C++ for a Dual-Core ARM Cortex-A9 processor (EMAC, UART,I2C, etc) and a radio board devices (ADC, DAC, PLL, amplifiers etc)
- Brought-up an embedded Linux on a Zynq-7000 board and mounted the device drivers and application code for the flexible logic

Software/ Hardware Designer Oct, 2013 – Jan, 2014

EnviSens Technologies *Turin, Italy*

- Elected a DSP chip and industrial board based on defined requirements for a meteorological radar application
- Bring-up real-time Embedded Linux on a Spartan-6 Eval board and created customized testing logic

Firmware Developer May, 2011 – Mar, 2012

Omid Technology *Tehran, Iran*

- Corporate in a team to implement an industrial DVB-T, -S and DVB-ASI Decoder Software based on ST Microelectronics products (STi5202 and STi7109)
- Generated software for a RTOS as a multitasking platform and device driver development of various peripherals like I2C, SPI, OSD, UART, GUI, various tuners and higher level application programming to produce a professional video decoder
- Studied various video stream/ DVB standards, STMicroelectronics STB architectures and operating system software layers
- Implemented a SNMP platform to management of the decoder status and alarms focusing on a Lantronix's product to have a Human Monitoring Interface via network
- Implemented a remotely Xilinx configuration mechanism on AVR microprocessor
- Created a program to produce JTAG state machine protocol and Implement FAT32 on a SD Card to file management and SPI Flash

Firmware Developer/ Architect Apr, 2005 – Nov, 2010

Rayan Electronics *Tehran, Iran*

- Designed and implemented electronic part of an array infra-red Camera with remarkable functionality in digital image processing
- Designed several schematic and PCB: analogue (buffers and low-noise amplifiers) and digital signals (synchronizations) and mixed signals (ADC, DAC) to drive an Infra-red detector
- Implemented several innovative algorithms for non-uniformity correction of array sensor on FPGA after simulations and verification in MATLAB
- Designed and implemented a real-time panoramic system for scanning 360° around which elaborated with an Infra-red array and an accurate controlled motor and transmission of image packets to PCI port and synchronization of the imaging data to the spanning position in FPGA
- Redesigned and enhanced a communication card based on TI DSP (firmware, schematic and PCB) for transmission and receive PCM data by McASP port and manage call control commands

Firmware Engineer/ Architect Apr, 2008 – Mar, 2014

Freelancer *Iran/ Italy*

- Designed and fabricated a Media Processor board (schematic and PCB) based on PNX1302
- Designed schematic and PCB, boot loader procedure and device drivers layer of video components
- Innovated an applicable software for a video processor for image stabilization based on multi local motion estimation on a video processor
- Completed application software for MPEG2/4 and JPEG decoding on PNX1005
- Designed hardware based on a TMS320F28335 and CPLD; Implemented device drivers layer for TMS320/Microchip/ Atmel microprocessors for reading rate sensors; and a proposed high performance decision mechanism based on DSP concepts
- Displayed a gyro-stabilized image with video processing functionalities like tracking, software stabilization and OSD after driving a CCD block camera

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)*

Outstanding Performance Recognition RSL10/ E7150SL contribution

Onsemi *2018*

Specialized Skills

Programming Languages: C (advance), ARM/ RISC-V Assembly (intermediate), Python (intermediate), MATLAB (advance), VHDL (advance)
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)