

Derek D. Miller

5109 Jacobs Creek Ct.
Austin, TX 78749
+1.512.695.7998
derekdelmiller@gmail.com

Qualifications

- Professional experience architecting and implementing security and content protection solutions for software, firmware, and SoC hardware
- Professional experience in Software Development in C, C++, perl, and Python in Windows and Linux (gcc, Visual Studio, gdb, Valgrind)
- Professional experience in logic design and hardware validation (Verilog)

Experience

Security Software Architect July 2014 to present
Amazon Web Services, Austin, TX

- Architected, documented, and began implementation of a secure boot solution for an ARM-based platform that utilized X.509 certificates, with firmware, key, and certificate rollback protection
- Implemented the SHA256 cryptographic hashing algorithm for an ARMv8 platform using C and inline assembly
- Evaluated and selected cryptographic hardware IP from various vendors for inclusion into an SoC
- Architected the hardware that was needed to integrate the selected IP into a custom pipeline, including data flow and key management interfaces and memories
- Architected a hybrid hardware/software implementation of a secure crypto coprocessor
- Filed 6 patents, with several more in the pipeline

Security Software Architect July 2012 to June 2014
Samsung System LSI, Austin, TX

- Architected, documented, and oversaw implementation of a secure boot system for a new ARM-based platform from scratch that implemented ARM's Trusted Board Boot specification
- Implemented cryptographic functions (SHA256 and RSA) and an X.509 decoder for ROM and firmware
- Developed code that interfaced to a proprietary cryptographic accelerator and to key management hardware, including implementing RSA authentication utilizing an accelerator that utilized Montgomery Multiplication
- Architected, documented, and oversaw implementation of a solution for OpenSSL to utilize a proprietary cryptographic accelerator through an OpenSSL engine and a Linux kernel-mode driver
- Architected and documented a solution for TLS private key protection utilizing ARM's TrustZone technology
- Determined hardware requirements and provided consultations to the hardware team regarding design details and overall security strategy

- Participated in specification and benchmark development in several industry consortia, including UEFI, Trusted Computing Group, and EEMBC

Security Architect

September 2010 to June 2012

Intel IDG, Austin, TX

- Designed and oversaw implementation of the security architecture of SoCs for the cellphone, tablet, and netbook markets
- Designed and oversaw implementation of media content protection hardware and software for SoCs in the cellphone, tablet and netbook markets
- Managed relationships between hardware and software teams in various locations (Texas, Oregon, China, India, Finland, Israel, Malaysia)
- Managed IP supplier relationships and deliverables

Graphics Driver Software Developer

March 2008 to August 2010

Intel Visual Computing Group, Austin, TX

- Designed and tested a Windows OpenGL driver for an experimental high-performance discrete graphics chip
- Designed and debugged elements of a high-performance, SIMD-based, software rasterizer
- Designed and debugged firmware for a multiprocessor, multi-threaded SIMD x86 architecture with texture sampling co-processors
 - Code was a mixture of ANSI C and x86 assembly

Component Design Engineering

May 2004 to March 2008

Intel Chipset Group, Austin, TX

- Logic Designer (in Verilog) of cryptographic functions for integrated graphics chips, including OMAC and AES
- Developed functional simulators in C++ for HDCP, HDMI, memory paging systems, and various other graphics and media functions
- Developed an asynchronous interrupt validation methodology for the preemptive multitasking of a 3D graphics pipeline

CAD Engineer

December 2000 to May 2004

Intel Desktop Platforms Group, Austin, TX

- Developed RTL simulators (C/C++, Verilog)
- Developed front-end design tools for semiconductor design (C/C++, perl, Verilog) utilizing both internal and vendor APIs

Software Developer

April 2000 to December 2000

Motorola Smartcard Solutions Division, Scottsdale, AZ

- Developed encryption software for smartcard manufacturing using the IBM 4758 cryptography board and its API (C/C++)

Systems Engineer

April 1998 to April 2000

Motorola Satellite Communications Division, Chandler, AZ

- Developed support and integration software for the Iridium satellite communications system (perl, C, C++)
- Developed satellite simulation software for a 77 satellite constellation, including calculations of the effects of Doppler shift on call completion rates

Education

Master of Science, Circuit Design, 4.0 GPA
The University of Texas at Austin

December 2006

Bachelor of Science, Engineering Physics, 3.69 GPA
The University of Oklahoma, Norman, OK

December 1997