Vincent Zimmer

5058 231st Ave SE, Issaquah, WA 98029 • (253) 709-3978 • vincent.zimmer@gmail.com
https://www.linkedin.com/in/vzimmer/ https://sites.google.com/site/vincentzimmer/cv Google Scholar

System software engineer - silicon initialization, secure/trusted computing capabilities and networking.

Experience

OCTOBER 2025 – PRESENT
Staff Software Engineer | Anduril Industries | Seattle, WA

EDKII firmware and embedded Linux-based NixOS for edge AI, including Nvidia. Threat modeling and security. Developing in Rust, C, bash, Python, Lean4, TLA, Isabelle/HOL, Rocq, Ocaml, Nix, Latex.

OCTOBER 2024 – SEPTEMBER 2025
Principal Software Engineer | Microsoft Corporation | Redmond, WA

Threat modeling for an upcoming operating system secure launch capability. Design a recovery architecture for this new OS feature. Creation and support of components in Project Mu, a UEFI codebase which is a downstream fork of EDKII written in C and Rust. Design, documentation and coding of an upcoming system firmware framework in Rust.

FEBRUARY 1997 – SEPTEMBER 2024
Senior Principal Engineer | Intel Corporation | Bellevue, WA

Chair of the UEFI security sub-team and component representative to the Trusted Computing Group (TCG). Specification, design and code of the UEFI Platform Initialization (PI) System Management Mode (SMM) and Pre-EFI Initialization (PEI). Led the creation of UEFI IPV6, WIFI & HTTP boot, along with UEFI Secure boot and the UEFI binding of the TCG Trusted Platform Module (TPM) measured boot, from the UEFI 2.3.1 specification through UEFI 2.6. Let the Firmware Support Package (FSP) specification and resultant product support from FSP 2.0 through FSP 2.5 allowing for open source firmware product development from Slimbootloader for embedded, coreboot for Chromebooks, and EDKII for mainstream platforms. Created EDKII advisory process, including making EDKII a CNA.

Skills

C, Rust, Python, Trusted Computing, Cryptography, Networking

Education

Master of Science in Computer Science and Engineering | University of Washington | Seattle, WA

Bachelor of Science in Electrical Engineering | Cornell University | Ithaca, NY

Accomplishments

2 Intel Achievement Awards, over 1100 issued patents (US + rest of world), 11 books/book chapters, 100+ papers and presentations, Senior Member of IEEE, Senior Member of ACM