|  |  |  |  |
| --- | --- | --- | --- |
| **SUMMARY** | |  | |
| * Security specialist and Confidential Computing architect for 10+ years. Member of SW team that helped bring industry’s first HW-rooted TEE, SGX, to market. * Liaison to Intel security incident response for security issues affecting SGX/TDX. Responsible for implementing security mitigations in SGX/TDX SW, including mitigations for Spectre and other transient execution (microarchitectural) security issues. * Implemented processes assuring the integrity of Confidential Computing attestation. * Extensive SW design experience working on a wide range of products. Design review and code review leadership and participation. Six years’ engineering management experience. * Solid foundation in cryptography. Responsible for ensuring FIPS 140 compliance of SGX/TDX SW. | | |
|  | | |
| **SKILLS** | | |
|  | | |
| Confidential Computing, C, C++, cryptography, mentoring, computer security, attestation, SDL (Security Development Lifecycle), x86 architecture/microarchitecture/assembly, Python, PowerShell, Docker, GitHub, PCI, chipsets | | |
|  |  | |
| **EXPERIENCE** | |  | |
|  | |  | |
| **Intel, Raleigh, NC** | | **August 2000 – September 2024** | |
|  |  | | |
| **Principal Engineer/SW Architect, Cloud SW Architecture, 2020 – September 2024** | | | |
|  | |  | |
| * **Implemented improvements to SGX/TDX attestation process. The improvements considered the needs of customers, validation requirements and the integrity of attestation.** * **Recognized gaps in validation of Intel updates containing mitigations for SGX or TDX vulnerabilities. Volunteered to address this by writing test plan (100+ pages), working with and mentoring validation engineers and by leading effort to utilize “attestation infrastructure” additions dedicated to validation. The additions allowed system testing to happen 3-4 months earlier.** * Worked with customers, including Microsoft Azure Confidential Computing (CC) engineers, to ensure understanding of how Intel addresses security issues and the implications for attestation. * Part of small team responsible for defining and executing Intel’s Confidential Computing TCB (Trusted Computing Base) Recovery process. The process incorporates the details of how each TCB component (microcode, firmware, etc.) can be updated. * Led response to [SGX.Fail](https://sgx.fail/) research that explored the implications of stale attestation results and where researchers were able to compromise the privacy of a popular block chain. Worked closely with the block chain vendor to utilize additional information in the attestation response to limit the breach. Balanced tradeoffs while addressing the stale attestation result root cause. * Member of task force responsible for facilitating FIPS 140 certification of Intel-provided SGX/TDX SW. * Completed Intel crypto training, level 1, consisting of coursework and paper-reading/discussion. * Designed simple fault injection countermeasures in light of [VoltPillager](https://www.usenix.org/system/files/sec21summer_chen-zitai.pdf)/[PlunderVolt](https://plundervolt.com/) research. * Introduced and specified an attestation library/service, for execution in the TDX Confidential VM, that hides attestation details from SW running in the TD. | | | |
|  |  | | |
| **SW Architect, 2018 - 2020** | | | |
| **Led SGX SW response to Spectre and subsequently discovered microarchitectural/transient execution issues. Led mitigation efforts when mitigations were implemented in SW, for example, for Spectre variant 1 and** [**LVI**](https://lviattack.eu/) **(Load Value Injection).**   * Led the effort to develop tools and to modify existing GCC and Microsoft tool chains to be able to add [LVI](https://lviattack.eu/) mitigations without changing source code, which was not viable for [LVI](https://lviattack.eu/). Defined different [LVI](https://lviattack.eu/) mitigation options, realizing the performance impact of full mitigations. * Proof of concept work related to the [Foreshadow](https://foreshadowattack.eu/)/L1TF speculative execution issue, specifically to address ease of exploit when hyper-threading was enabled, even with Intel’s microcode patch. Developed stack location randomization to make exploit more difficult. | | | |
|  | | | |
| **SW Architect, 2008 - 2018** | | | |
|  | |  | |
| * Wrote spec for SGX attestation (200+ pages) including specification of “architectural enclaves” (AEs). (Use of SGX involves the development and use of “enclaves”, essentially user mode libraries that can remain secure even when the OS, VMM, BIOS, etc. are compromised.) To limit SGX HW and microcode complexity, the Intel-provided AEs implement a large portion of the attestation process. * Worked with Intel cryptographers to design a variant of the SIGMA key exchange protocol for use with SGX attestation. * Wrote spec for SGX Platform Services (100+ pages), chipset-provided features complementing native SGX features. Specifically, the chipset provided trusted time and replay-protection through monotonic counters. This work included a novel method for adding the attestation of these complementary features to attestation of the rest of the SGX TCB. * Volunteered to be team’s Security Champion, responsible for compliance with Intel SDL, including security review of SGX SDK and SGX Platform SW deliverables. * Early attestation proof of concept characterized by a Windows service where SGX enclaves responsible for attestation-related provisioning and signing ran. The service was a COM server and the PoC included how to communicate with it (using COM). The eventual product adopted this design. | | | |
|  |  | | |
| **SW Architect, 2005 - 2008** | | | |
|  | |  | |
| **Worked on VoIP and “Wake-on-Event” projects. Wake-on-event was a generalization of Wake-on-LAN/Wake-on-ring and utilized a SIP stack running on a microcontroller integrated in the Intel chipset (part of Intel vPro/AMT).**   * Implemented STUN and DNS clients for SIP ThreadX/Posix-based Wake-on-Event project. * Led small team to develop Linux driver for a PCI SLIC card for VoIP project. * Modified HD Audio class driver to work with HD Audio SLIC device. * Wrote HD Audio spec extension for SLIC devices. Worked with chip vendors on their compliant chips. | | | |
|  |  | | |
| **SW Architect/Engineering Manager, August 2000 - 2005** | | | |
|  | |  | |
| **Led HD Audio soft modem project. Modem representative on Intel's HD Audio initiative team and on the Intel/Microsoft HD Audio joint development team.**   * Identified and helped resolve issues in HD Audio bus driver. Ported HD Audio modem driver to x86 64-bit architecture.   **Technical lead on embedded V.92 modem project where the goals were 1) to switch to have Intel manufacture the modem silicon and 2) to have this silicon support both controller-based and controller-less modems.**   * Ported existing modem controller from a Windows driver implementation to an 8051 implementation. Responsible for development of new platform-dependent code for controller-less mode: selected development tools and specified debugging methodology, consisting of In-Circuit Emulator, debug monitor and use of logic analyzer to facilitate offline analysis of program traces. * Worked with design teams on the design of the new modem chip’s programming interface and to ensure evaluation boards for the new modem chip met chip validation and development requirements. Drove evaluation board project to make sure boards were ready as soon as chips were available. * Responsible for design/programming of Lattice FPGAs on evaluation board. * Wrote 8051 code for new modem chip’s boot ROM. * Defined API designed to hide HW-dependent and OS-dependent details. Wrote corresponding code for both bondouts (controller-based and controllerless/PCI) of the new modem chip. * Developed bringup Windows drivers for the new modem chip: read/write registers, read/write chip memory, test DMA, timers, and GPIO, and load DSP and controller code. * Designed automated modem test, including simple network protocol to allow sharing of modem test equipment. | | | |
|  |  | | |
| Hughes Network Systems, Gaithersburg, MD | | August 1999 – August 2000 | |
|  | |  | |
| **Principal Engineer, August 1999 – August 2000** | | | |
|  | |  | |
| * Responsible for video and audio SW development for Hughes's version of the AOLTV settop box, which combined the standard DirecTV box with HW and SW required to browse the web on a TV. * Quickly developed knowledge needed to develop and debug multimedia HW subsystem, including understanding advantages of using synclocked video, how to use the video capture and playback engines on the IGST CyberPro5055-based HW design and implementing closed-captioning feature. * Used Tornado (VxWorks, GNU C/C++) development environment and remote debugging. | | | |
|  |  | | |
| **ADDITIONAL RELEVANT EXPERIENCE** | | | |
|  |  | | |
| **Cirrus Logic Inc., Austin, TX** | |  | |
| Audio SW Manager | Project Lead | Engineer | | | |
|  | |  | |
| **Compaq Computer Corporation, Houston, TX**  Systems Engineer: Graphics Development | | | |
|  |  | | |
| **Research Planning Inc., Arlington, VA**  SW Engineer | | | |
|  |  | | |
| **EDUCATION** | |  | |
|  | |  | |
| **Master of Science (MS), Electrical Engineering**  Georgia Institute of Technology, Atlanta, GA | | | |
|  |  | | |
| **Bachelor of Science (BS), Electrical Engineering**  University of Maryland, College Park, MD | | | |