**RYAN SAVINO**

510 W 18TH ST APT 106, AUSTIN, TX 78701

610.290.6972 | rksavino@gmail.com

**Software System Design Engineer**

*Multifaceted technical expert with 15+ years proven success in software engineering, architecture and management*

Accomplished software professional with solid design and management experience in the open-source software space related to platform hardware security and confidential computing. Skilled, technical leader capable of developing core product architecture and proficient at implementing modern design techniques.

**Core Competencies:**

Software Engineering | Architecture and Design | Management | [Confidential Containers](https://confidentialcontainers.org) | [Kata Containers](https://katacontainers.io) | Security | Cryptography | Web Service Development | Continuous Integration | DevOps |

Software Development Life Cycle | Software Legal Compliance | Data Center

**TECHNICAL PROFICIENCIES**

|  |  |
| --- | --- |
| ***Platforms:***  ***Languages:***  ***Tools/Skills:*** | Windows, Ubuntu, RHEL, SUSE, VMWare, ESXi, Linux KVM, Citrix XenServer, Docker, Kubernetes  Rust, Golang, Java, Python, C, C++, C#, Bash, Perl  GIT, SVN, GitHub (Actions), GitLab, TeamForge, Jira, Maas, Satellite, Foreman, PXE, Ansible, Semaphore, TeamCity, Jenkins, Maven, Ant, Artifactory, Protex, Code Center, Black Duck Binary Analysis, Klocwork, Checkmarx, GORM, VMWare SDK, MySQL, PostgreSQL, Apache, Tomcat, Glassfish, Jetty, Gorilla, Casbin, REST, CRUD, IPMI, Visual Studio |

**PROFESSIONAL EXPERIENCE**

**Advanced Micro Devices (AMD)** | DEAE Austin, TX 12/2021 – Present

**Software System Design Engineer – Senior Member of Technical Staff (SMTS)**

Experienced open-source contributor and technical leader specializing in confidential computing and virtualization technologies. AMD core representative and developer on the [Kata Containers](https://katacontainers.io) and [Confidential Containers](https://confidentialcontainers.org) ([CNCF](https://www.cncf.io) sandbox) community projects. Led the development and integration of EPYC Secure Encrypted Virtualization-Secure Nested Paging ([SEV-SNP](https://www.amd.com/en/developer/sev.html)) solutions within these projects, collaborating with key industry partners and experts from IBM, Red Hat, Nvidia, Microsoft, Intel, Apple and others.

***Key Achievements and Responsibilities:***

Technical Contributions, Open-Source Leadership & Confidential Computing:

* Served as a Source Code Maintainer for the Kata Containers project and the AMD lead on the Confidential Containers Steering Committee, conducting code reviews, approving and merging pull requests, and contributing to the overall project direction
* Contributed to the development of the SEV-SNP attestation solution in Confidential Containers and Trustee, ensuring compatibility with in-development components like the Linux kernel, OVMF, and QEMU promoting ease of use and adoption with end consumers
* Engaged in discussions with company fellows and senior fellows, driving the direction of AMD’s involvement in the confidential computing space, including strategy on an attestation design implementation, community project involvement, potential improvements, and industry applications
* Enabled and maintained the Confidential Containers CI, training and helping team members address bugs, resolve recurring issues, and support the EPYC offering within the community project
* Supported service providers in enabling SEV-SNP in their cloud offerings and assisted end users with showcasing memory encryption proof of concepts, instigating early research and promoting confidential compute technology adoption by industry key players
* Created and maintained the AMD public facing sev-utils project, providing a SEV-SNP enablement utility with automated host setup, QEMU guest launch, and a sample attestation flow – this project provided a direct boot workflow and was taken through the internal AMD approval process for open-source publishing
* Architected the team's internal CI testing platform, including network infrastructure setup (DHCP and DNS hosting), rack management, PXE boot automated server provisioning (MaaS, Satellite, Foreman), Semaphore (Ansible) automation, and GitHub Actions integration
* Worked with IBM and Nvidia to enable GPU and peripheral device support in Confidential Containers via PCI device passthrough by applying respective QEMU patches in the project, paving the way for artificial intelligence (AI) offerings within secure confidential compute Trusted Execution Environments (TEEs)
* Collaborated with IBM and Red Hat to integrate SEV-SNP and Confidential Containers into OpenShift Container Platform (OCP), promoting adoption in popular flavors of orchestration solutions
* Led the development of a POC demo showcasing bare-metal memory scraping of sensitive user input in standard containers versus SEV-SNP memory encrypted workloads using Confidential Containers, exposing hypervisor security threats and the need for confidential computing solutions
* Virtualization and QEMU veteran, serving as a company-wide reference point for expert consulting
* Validated various Linux OS distribution support for SEV-SNP, identifying issues and collaborating with the AMD kernel development team to fix and apply necessary patches

Performance Analysis & Demonstration:

* Conducted a TPROC-C performance analysis of SEV-SNP Confidential Containers, identifying performance overhead differences as compared to Kata Containers and standard Kubernetes containers, working with AMD kernel team developers and within community projects to increase and enhance confidential compute performance with SEV-SNP

Mentorship & Team Leadership:

* Mentored junior engineers, coordinating their work in community projects, helping them build focused development growth strategies through best known practices, coding expertise and debug training

**Intel Corporation** | DPG Folsom, CA 06/2013 – 12/2021

**Software Architect** 08/2019 – 12/2021

Software designer focused on cloud security architecture in Intel’s Data Platforms Group. Intel Security Libraries for the Data Center (ISecL) implements and manages hardware root of trust technologies for data center platforms, collecting and attesting firmware and configuration measurements that are extended to a Trusted Platform Module (TPM) and other Hardware Security Modules (HSMs). Confidential computing and workload orchestration use cases are built on top of this foundational security.

***Key Achievements and Responsibilities:***

* Main contributing author from Intel on NIST IR 8320 – “Hardware-Enabled Security for Server Platforms: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases”
* Designed and submitted a proposal for tracking data center servers and assets with GPS and RFID hardware utilizing a platform server OOB mechanism for provisioning location data
* Contributed to cloud native POC on optimizing key exchange/management for Software Guard Extensions (SGX) Trusted Execution Environments (TEEs) to enhance crypto performance for virtualized workloads
* Investigated product integration with the Linux kernel Integrity Measurement Architecture (IMA) and proposed a runtime attestation solution for bare-metal file systems
* Designed a product component to associate security trust evaluations and identifying labels with server nodes in orchestration engines, utilizing OpenStack traits and Kubernetes node affinity features; node labels were used to appropriately filter orchestration scheduling decisions and the product was designed to support a multi-tenant environment
* Drove existing code migration from java to golang and oversaw conversion to a microservice architecture with a common authentication, authorization and certificate management solution
* Overhauled architecture documentation converting to markdown format and consolidating to an organized central location within a design source code repository
* Proposed product improvement strategies and created a venue through Confluence for maintaining continual updates and cultivating new innovative ideas

**Software Engineering Manager** 04/2018 – 08/2019

Development manager for the Intel Server Security Technologies team, overseeing ISecL product development. Responsible for mentoring the development team and maintaining modern industry standards and practices.

***Key Achievements and Responsibilities:***

* Championed agile methodologies, responsible for running daily scrum, coordinating development sprint schedule planning, feature/bug dispositioning, and performing code reviews for development teams across multiple geos
* Conducted employee hiring, performance and career development while mentoring an environment of self-accountability and developer autonomy, emphasizing work quality
* Oversaw and approved developer low level designs including database schemas, REST endpoint definitions, user story specification and application configuration/installation options
* Member of architecture review board responsible for ratifying architectural designs before development low level design commencement
* Interfaced with senior architects to identify important modules and features for product integration and worked with the program management team to integrate these plans into the development schedule
* Enforced secure software guidelines, requiring hashing and encryption algorithm updates and secure cipher suite usage for TLS communication

**Software Engineering Lead** 06/2013 – 04/2018

Senior software developer responsible for producing product low level design, coordinating development tasks across team members, reviewing and approving code merge requests, and mentorship of junior developers.

***Key Achievements and Responsibilities:***

* Completed high and low level architectural designs for next generation of product, producing a complex whitelist matching engine to automatically associate good known values with registered platforms
* Cryptography veteran, well versed in security implementations such as symmetric/asymmetric key encryption, PKI, hashing algorithms, OpenSSL, SSL and TLS communication
* Continuous Integration expert, proficient with tools such as TeamCity and Jenkins, building configurations for automating source code compilation, unit testing, remote artifact deployment, and build delivery notification
* Championed secure Software Development Life Cycle deliverables, including automation of static analysis scanning, scanning for banned functions, 3rd party dependency whitelisting and analysis, and enforcement of intellectual property and license management guidelines
* Developed product extensions for the Kubernetes orchestration engine scheduler to select platforms with specified trust attestation and location values
* Developed and maintained RESTful API interfaces with CRUD operations, providing clear documentation in Javadoc and OpenAPI format
* Maintained open source product release on GitHub

**Comcast Converged Products (CCP)** | Philadelphia, PA 01/2012 – 06/2013

**Software Quality Assurance Engineer**

Specialized in QA systems and stability analysis for the Comcast Xcalibur product, a tru2way cloud-based software platform. At the time, Xcalibur was the next generation Comcast television experience, utilized on a range of devices (QAM and IPTV STBs, PCs, tablets, mobile devices, etc.) for both linear and OnDemand content, as well as third party applications.

**Communications Test Design, Inc.** | Carlsbad, CA 03/2010 – 01/2012

**Headend, Set-top Box Engineer**

Provided onsite engineering support for COX Communications and Verizon Set-Top Box test and repair facility. Day to day operations included administrating cable headend and infrastructure equipment and assisting repair facility with product troubleshooting. Designed and developed set-top box test and repair applications, and documented operational procedures.

**Electrical Engineering Department, University of Notre Dame** | Notre Dame, IN 01/2007 – 08/2009

**Researcher**

Performed research on Quilt Packaging, a microelectronic fabrication technique that produces package interconnects on chip, yielding low loss microwave measurements for wide bandwidths with multiple substrate compatibility. Contributed to multiple publications.

**EDUCATION University of Notre Dame |** Notre Dame, IN May 09

**Bachelor of Science,** Electrical Engineering

**SELECTED COURSEWORK**

Electronics (II) Lab, Semiconductors (II), Electromagnetic Fields and Waves (II), Signals and Systems, Microwave Circuit Design Lab, IC Fabrication Lab, Photonics Lab