Diego **Zamboni**

IT Enterprise Security Architect · CFEngine Expert · Team and Project Leader

diego@zzamboni.org · zzamboni.org · zzamboni · zzamboni · zzamboni · zzamboni

Introduction

I am a senior computer security expert, IT architect, computer scientist, team and project leader with 29 years of professional experience. I specialize in the areas of Configuration Management, Computer Security, Cloud Computing and Self-healing Systems. I possess a strong combination of leadership, research and technical skills that enable me to lead teams in analyzing complex problems, designing and implementing elegant and pragmatic solutions. I have strong communication abilities, with ample experience in writing, teaching and public speaking. I can interact and work fluently at the strategic, tactical and technical levels. I have a Ph.D. in Computer Science and have experience in both academic and business environments.

Skill and Experience Overview

Configuration management CFEngine (Author of *Learning CFEngine*), Ansible, Puppet.

Computer Security Enterprise Security Architecture, Intrusion detection and prevention (Ph.D. in Computer Science in this area), operating systems security, network security, software security, secure software development, virtualization and cloud computing security, malware detection and containment.

Leadership Technical team and project leadership, Scaled Agile Framework (SAFe) methodology and processes, SAFe Product Owner certification, SAFe Architect training.

Systems and Development Unix/Linux systems engineering and administration, systems health management and monitoring, cloud computing environments and platforms (OpenStack, Amazon EC2, Cloud Foundry) and software development experience (C, Python, Ruby, Perl, Java, etc.).

Communications Excellent written and spoken communication skills, with more than 30 years of written and oral communication and teaching experience in different contexts and topics.

Languages Spanish (native), English (100%), German (B1/B2 level).

Other skills Customer-facing experience, project and product management experience.

Experience

Swisscom

2015 – Present *Switzerland*

Enterprise Security Architect / IT Clouds Security Solution Architect *Apr 2019 – Present*

- As Enterprise Architect, I participate in the design of the future products and solutions offered by Swisscom.
- As Security Architect for the IT Clouds Large Solution, I design and define security-relevant product features, compliance and business goals of the cloud platforms built by Swisscom. I also advise on compliance, governance and operational activities. Selected achievements:

Squad Lead & Product Owner for Health & State Management in the IT Clouds Large Solution *Apr 2018 – Apr 2019*

- I oversaw the requirement definition, planning and execution of the HSM team's mission to design, implement and manage Health Management and Monitoring components for all the IT Clouds platforms, including Enterprise Service Cloud, Application Cloud, Enterprise Cloud 1.x, Enterprise Cloud for SAP applications (EC4SAP), Marketplace Services, and Cloud Connectivity Management.
- Main technologies involved: VMware vSphere (ESX, vCenter, NSX), VMware vRealize Operations Manager and Log Insight, Ansible (configuration management), OpsGenie (alert management).

Squad Lead & Product Owner for Health & State Management in the Enterprise Service Cloud project *Jan 2017 – Mar 2018*

- Worked with Product Management to define the technical features necessary for Health Management and Monitoring in the Enterprise Service Cloud project
- I lead the team which implements, deploys and operates these components.

Head of Health and State Management — *Mar 2016 – Jan 2017*

- Led a team working on multiple projects related to Health Management and Monitoring of the Swisscom cloud offerings, including Application Cloud (CloudFoundry-based PaaS offering), Enterprise Cloud 1.x and Enterprise Service Cloud (IaaS offerings).

LEMM Squad Lead in the Enterprise Cloud project — *Jun 2016 – Dec 2016*

- Led the architecture and delivery of the Logging, Event Management and Monitoring framework (LEMM) of the Swisscom Enterprise Cloud, which handles all the processing, analysis and monitoring of the logging messages, health events, and other relevant infrastructure events.

Cloud Architect and Orchard Project Lead — *Aug 2015 – Mar 2016*

- Continued leading the *Orchard* project through its implementation, release and further improvements and development.

Swisscom Cloud Lab — *2014 – 2015* — *U.S.A. (remote)*

Senior Platform Architect — *Aug 2014 – Jul 2015*

- I designed the architecture for the *Orchard* health-management and self-healing components of Swisscom's *Application Cloud* Platform-as-a-Service Offering. This system performs self-monitoring and self-healing of the infrastructure and platform components. In addition to designing the architecture, I worked on its implementation together with a team of three people managed by me.
- Main technologies involved: OpenStack (cloud computing infrastructure), Plumgrid (SDN), Cloud Foundry (application platform), Consul (health management and service discovery), RabbitMQ (message bus), Riemann (event stream analysis).

CFEngine AS — *2011 – 2014* — *Norway/U.S.A. (remote)*

Product Manager — *Aug 2013 – Jun 2014*

- Coordinated the CFEngine Design Center project.
- Participated in the development of the CFEngine language roadmap.
- Coordinated the work on CFEngine third-party integration (e.g. AWS EC2, VMware, Docker and OpenStack).
- Developed code for both the Design Center and some of the integrations.

Senior Security Advisor — *Oct 2011 – Jun 2014*

- Overall advocate and fanatic for CFEngine, with a special focus on security.
- Gave talks, wrote articles and blog posts, taught classes, and in general spread the word about CFEngine.
- Worked on developing and implementing the strategy for CFEngine in security.

HP Enterprise Services — *2009 – 2011* — *Mexico*

Account Security Officer — *Oct 2010 – Oct 2011*

- I was the first point of contact for all security-related issues for five HP enterprise customers in Mexico, some of them with international presence.
- Initiated, advised and managed security-related projects.
- Handled communication and coordination between technical teams involved in security initiatives.
- Involved in all security-related decisions at the sales, design, implementation, delivery and ongoing maintenance stages of IT Outsourcing projects.

IT Outsourcing Service Delivery Consultant — *Nov 2009 – Oct 2010*

- I helped customer teams by solving complex problems in customer environments.
- Performed analysis, design and implementation of solutions in multiple areas of expertise, including system automation, configuration management, system administration, system design, virtualization, performance and security.

IBM Zurich Research Lab — *2001 – 2009* — *Switzerland*

Research Staff Member — *Oct 2001 – Oct 2009*

- I worked in intrusion detection, malware detection and containment, and virtualization security research projects. See *Research activities* for details of my research.

Sun Microsystems — *1997* — *U.S.A.*

Developer (Intern) — *May 1997 – Aug 1997*

- Participated in the development of the *Bruce* host vulnerability scanner, later released as the Sun Enterprise Network Security Service (SENSS).
- Designed and implemented the first version of the network-based components of *Bruce*, which allowed it to operate on several hosts in a network, controlled from a central location.

National Autonomous University of Mexico (UNAM) *1991 – 1996* *Mexico*

HEAD OF COMPUTER SECURITY AREA *Aug 1995 – Aug 1996*

- Founded UNAM's Computer Security Area, the University's first team dedicated to computer security, which has since evolved into a much larger organization.
- Supervised up to nine people working on different projects related to computer security.
- Supervised and participated in the direct monitoring of the security of a Cray supercomputer and 22 Unix workstations.
- Provided security services to the whole University, including incident response, security information, auditing and teaching.
- Established the celebration of the *International Computer Security Day* (sponsored by the Association for Computing Machinery) at UNAM. Acted as the main organizer of the event for two years (1994 and 1995). This event has grown and divided into the *Computer Security Day* (a one-day event) and the *Seguridad en Cómputo* (Computer Security) conference (a multi-day event).
- Designed and headed development of an audit-analysis tool for Unix systems (SAINT).

SYSTEM ADMINISTRATOR *Nov 1991 – Aug 1995*

- Part of the system administration team at the University's Supercomputing Center, managing UNAM's Cray Y-MP Supercomputer (the first supercomputer in Latin America) and related systems.
- Managed the Network Queuing Subsystem (NQS).
- Collaborated in other aspects of the supercomputer administration, including user administration, operating system installation, resource management, and policy making and implementation.
- Directly managed three Unix workstations, provided support for 19 more.
- Monitored the security of the Cray supercomputer and related workstations.

Education

Ph.D. in Computer Science *West Lafayette, IN, U.S.A.*

PURDUE UNIVERSITY *Aug 1996 – Aug 2001*

- Thesis title: *Using Internal Sensors for Computer Intrusion Detection*.
- Advisor: Eugene H. Spafford.

M.S. in Computer Science *West Lafayette, IN, U.S.A.*

PURDUE UNIVERSITY *Aug 1996 – May 1998*

- Advisor: Eugene H. Spafford.

Bachelor's degree in Computer Engineering *Mexico City, Mexico*

NATIONAL AUTONOMOUS UNIVERSITY OF MEXICO (UNAM) *Aug 1989 – Jul 1995*

- Thesis title: UNAM/Cray Project for Security in the Unix Operating System (in Spanish, original title: *Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix*).

Certifications

Certified Information Systems Security Professional (CISSP) *April 2019*

(ISC)^2, THE INTERNATIONAL INFORMATION SYSTEM SECURITY CERTIFICATION CONSORTIUM

The vendor-neutral CISSP credential confirms technical knowledge and experience to design, engineer, implement, and manage the overall security posture of an organization. Required by the world's most security-conscious organizations, CISSP is the gold-standard information security certification that assures information security leaders possess the breadth and depth of knowledge to establish holistic security programs that protect against threats in an increasingly complex cyber world.

CISSP®

SAFe® 4 Certified Product Owner/Product Manager *July 2017*

SCALED AGILE INC.

A SAFe® 4 Certified Product Owner/Product Manager is a SAFe professional who works with customers and development organizations to identify and write requirements. Key areas of competency include identifying customer needs, writing epics, capabilities, features, stories, and prioritizing work in order to effectively deliver value to the enterprise.

POPM SAFe® 4

System Development and Management

Programming languages	C, Perl, Java, AWK, Unix shells (Elvish shell, Bourne shell, C shell, Korn shell), Python, PHP, Ruby, Objective~C, Cocoa (MacOS X), Go, Clojure.
Development environments	Unix/Linux, OpenStack, Cloud Foundry, Amazon EC2, Mac OS X.
Unix system administration	Linux (experience with multiple distributions including RedHat, Ubuntu, Debian, Gentoo, and others), OpenBSD, FreeBSD, MacOS X, MacOS X Server, Solaris.
Configuration management	CFEngine 3, Puppet, Chef, Ansible.
Virtualization, containers and cloud	VMWare (ESX, vSphere), OpenStack, Amazon EC2, Docker, Cloud Foundry.
Health Management and Monitoring	VMware vRealize Operations Manager, vRealize Log Insight, Nagios, Icinga.
Other	REST APIs, Riemann (event stream processing), XML and related technologies, network programming, database programming (SQL), kernel programming (OpenBSD and Linux), HTML.

Software Development Projects

Publicly-available software projects: see https://github.com/zzamboni/

Other software projects (not publicly available)

Pilatus (IBM) *2005 – 2007*

A system installer that allows arbitrary system installation and configurations, allowing for both proprietary and open source components to be installed in an automated fashion. Open source components can be downloaded directly from their original source to avoid distributing them.

SOC in a Box (IBM) *2005 – 2007*

A specialized Linux distribution containing multiple security services for integrated security monitoring in small and medium networks. Implementation includes also backend infrastructure components for system installation, configuration and upgrade; and data centralization, analysis and reporting.

Billy Goat (IBM) *2002 – 2007*

A specialized Linux distribution containing multiple sensors for detection of large-scale automated attacks. Implementation includes also backend infrastructure components for system configuration and upgrade, data centralization, analysis and reporting.

Embedded Sensors Project (ESP) *1999 – 2001*

A system of sensors for intrusion detection developed in OpenBSD through code instrumentation. Developed as part of my Ph.D. thesis work. Programming done mostly in C.

References

Available by request.