Diego **Zamboni**

diego@zzamboni.org | zzamboni.org | Zurich | zzamboni | zzamboni | zzamboni | zzamboni.org

CISO • Organizational Leader • Security Expert • Computer Scientist

Summary

I am a senior computer scientist, computer security expert, IT architect, organization and team leader with 30 years of professional experience, and much longer of being fascinated and passionate about science, computing and education. I specialize in the areas of Computer Security, Cloud Computing, Self-healing Systems and Configuration Management.

I possess a strong combination of leadership, conceptual and technical skills that enable me to help organizations and teams reach their goals. I have excellent 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 extensive experience in both academic and business environments.

Professional Highlights

Management and leadership, IT security, cloud computing

- Chief Information Security Officer for Governance at Avaloq, defining and managing Avaloq's global ISO27001-certified Information Security Management System
- Managed security architecture at the Stellantis *Virtual Engineering Workbench* project. Worked with Stellantis CISO and business stakeholders to define governance, establish security best practices and drive risk analysis, threat modeling and mitigation.
- Established scalable and durable mechanisms to enable partners to work securely in the Volkswagen Digital Production Platform (DPP) program.
- Managed security architecture, risk management, data governance and compliance (ISO27001, ISAE3402/3000, etc.) for Swisscom's Cloud platforms.
- Established and led the Swisscom IT Clouds security community of practice.
- Established and led the *Health and State Management* team at Swisscom to design, implement and operate a framework for scalable monitoring, logging and alerting for Swisscom's Cloud platforms.
- Established and led the first computer security organization at UNAM, which has grown into the university's Information Security Coordination (UNAM-CERT).
- Managed IT security customer relationships at HP Enterprise Services, including overseeing the activities of operational and engineering teams, risk and compliance management, requirements discussion and reporting.

Research, architecture and design

- Designed the *Orchard* monitoring framework for Swisscom's *Application Cloud* platform, and led the team that implemented it and brought it into production.
- Designed and implemented the *Billy Goat* malware capture and analysis system at IBM.

Communications and community

- Author of multiple books including *Learning CFEngine*, *Learning Hammerspoon* and *Literate Configuration*.
- Program chair and program committee member for multiple conferences including the RAID symposium, DIMVA conference, the *Computer Security Day* and *Computer Security* conference at UNAM, and others.
- Former member of the Editorial Board of the Computers & Security Journal.

Experience

Avaloq — *Switzerland*

CISO Governance — *Jan 2024 - Present*

I lead the global CISO Governance team, focusing on establishing robust security policies and monitoring compliance. I am in charge of defining and monitoring Avaloq's global Information Security Management System. My role involves defining requirements and ensuring effective oversight of first-line security functions, which is essential for maintaining a secure and compliant environment in the financial technology sector.

Amazon Web Services — *Switzerland*

Senior Global Security Architect — *Oct 2022 - Dec 2023*

I worked with customers and within AWS to increase security awareness, design and build secure solutions, mentor and develop colleagues and customers in security best practices. I was Lead Security Architect in the Stellantis Virtual Engineering Workbench (VEW) project.

- Established the VEW security workstream to identify customer security requirements and policies, define and promote security best practices and drive activities related to risk analysis, threat modeling and mitigation definition, prioritization and implementation.
- Established in VEW measurement mechanisms for status and metrics for security activities, which provide visibility to both technical and business stakeholders.
- Established the VEW *Security Champions* program to promote and transfer security knowledge.
- Defined and tracked implementation of security features in VEW to fulfill both customer business requirements and AWS best practices.

Global Security Architect

Sep 2021 - Sep 2022

Worked with AWS global customers to improve security posture and promote secure design and implementation practices. I was a member of the security team in the Volkswagen Digital Production Platform (DPP) project.

- Established in DPP scalable and durable mechanisms to enable DPP partners to work securely in the DPP program.
- Created and promoted security learning materials tailored for various roles within the DPP project.
- Increased security awareness and knowledge by promoting a *Security Guardians* initiative across the DPP organization.

Swisscom

Switzerland

Enterprise Architect and IT Clouds Solution Security Architect

Apr 2019 - Sep 2021

As an *Enterprise Architect*, I participated in the design of future products and solutions offered by Swisscom, in collaboration with architects from all other divisions of the company.

As *Solution Security Architect for Swisscom's Cloud Platforms* (including *Enterprise Service Cloud*, *Enterprise Application Cloud*, *Dynamic Computing Services*, *Enterprise Cloud for SAP Applications* and related services) I was responsible for the security, compliance and data governance of those services. I defined, prioritized and drove relevant product features and business goals. I also lead the IT Clouds Security Community of Practice and advised engineering teams on compliance, governance and operational activities.

- Ensured cloud platform and service compliance with internal, contractual and regulatory standards, including ISO27001, ISAE3402/3000 and GDPR.
- Established and led a community of around 30 /Security Champions/ from different teams, who drove security initiatives and promote the security culture within the Swisscom IT Clouds organization.
- Coordinated threat modeling, audits, penetration tests and security compliance reporting.
- Coordinated organization- and team-wide processes for risk and vulnerability management.
- Development of the Swisscom Platforms vision for 2025.

Team Lead & Product Owner for Health & State Management

Mar 2016 - Apr 2019

I built and led a team which evolved on par with Swisscom cloud platforms to provide their monitoring and logging capabilities. My responsibilities included people management (up to 16 people), definition and prioritization of requirements and roadmaps (in collaboration with Product Managers and other stakeholders), technical architecture, and managing the planning and execution of team activities.

- Led the transition of the *Enterprise Cloud* LEMM (Logging, Event Management and Monitoring) and Access & Inventory frameworks into maintenance mode as the platform was retired.
- Defined the scope and mission of the Health and State Management (HSM) team as part of the new *Enterprise Service Cloud* project, and later of other platforms as the *IT Clouds* scope expanded to *Application Cloud*, *Enterprise Cloud for SAP Solutions* and *Dynamic Computing Services*.
- Defined the logging and monitoring architecture for the *Enterprise Service Cloud* platform based on VMware vRealize Operations and vRealize Log Insight.
- Led the transition of the *Application Cloud* platform monitoring from the Orchard framework to a TICK-based framework.
- Defined architecture and oversaw implementation of the Customer Log Forwarding service.
- Managed business relationship and technical implementation of OpsGenie for alert management in IT Clouds.
- Main technologies involved: VMware vSphere (ESX, vCenter, NSX), VMware vRealize Operations Manager and Log Insight, Ansible (configuration management), OpsGenie (alert management).

Cloud Architect and Orchard Project Lead

Aug 2015 - Mar 2016

Managed a team of three people and led the *Orchard* project through its implementation, production release and further improvements and development.

Cloud Lab Senior Platform Architect

Aug 2014 - Jul 2015

- Designed the architecture and implemented the initial prototype for the *Orchard* health-management and self-healing framework for Swisscom's *Application Cloud* Platform-as-a-Service service.
- Main technologies involved: OpenStack (cloud computing infrastructure), Cloud Foundry (application platform), Consul (health management and service discovery), RabbitMQ (message bus), Riemann (event analysis).

CFEngine AS

Norway/U.S.A. (remote)

Product Manager

Aug 2013 - Jun 2014

- Managed the CFEngine language roadmap.
- Created and led the CFEngine Design Center project, which was the foundation for the current CFEngine Build service.
- Coordinated the work on CFEngine third-party integration (e.g. AWS EC2, VMware, Docker and OpenStack).
- Developed code for both the Design Center core and its integrations.

Senior Security Advisor — *Oct 2011 - Jun 2014*

- CFEngine Advocate, with a special focus on security.
- Wrote the book *Learning CFEngine 3*, published by O'Reilly Media, which became the de facto introductory text to CFEngine.
- Gave talks, wrote articles and blog posts, taught classes, and in general spread the word about CFEngine.
- Developed and implemented the strategy for CFEngine as a security component.

Boundless Innovation and Technology

Mexico

Cofounder, Head of Research and Training — *Jul 2012 - Jul 2014*

I advised and coordinated teams working on teaching- and security-related products, consulting and services.

HP Enterprise Services

Mexico

Account Security Officer — *Oct 2010 - Oct 2011*

- Acted as first point of contact for all security-related issues for five HP enterprise customers in Mexico.
- 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*

- Helped multidisciplinary customer teams (software engineering, IT management, networking, sales and support) 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

Switzerland

Research Staff Member — *Oct 2001 - Oct 2009*

I was a member of the *Global Security Analysis Laboratory* (GSAL), where I worked in intrusion detection, malware detection and containment, and virtualization security research projects. See Research for details of my research.

Sun Microsystems

U.S.A.

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

- Developer for 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)

Mexico

Founder and lead of Computer Security Area — *Aug 1995 - Aug 1996*

- Established UNAM's *Computer Security Area*, the University's first team dedicated to computer security, which has evolved into the *Information Security Coordination (UNAM-CERT)*.
- Managed up to nine people working on different projects related to computer security.
- Managed security monitoring for 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 evolved into the *Computer Security Day* and the *Computer Security Congress*.
- Designed and headed development of an audit-analysis tool for Unix systems (SAINT).

System Administrator — *Nov 1991 - Aug 1995*

- System administrator at UNAM's Supercomputing Center, managing a Cray Y-MP Supercomputer and related systems.
- Managed the Network Queuing Subsystem (NQS),
- Managed and provided support for 22 Unix workstations.
- Monitored the security of the Cray supercomputer and related workstations.
- Other responsibilities: user administration, operating system installation, resource management, security policies.

Education

Purdue University

West Lafayette, IN, U.S.A.

Ph.D. in Computer Science — *Aug 1996 - Aug 2001*

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

Purdue University

West Lafayette, IN, U.S.A.

M.S. in Computer Science — *Aug 1996 - May 1998*

Advisor: Eugene H. Spafford

National Autonomous University of Mexico (UNAM) — *Mexico City, Mexico*
Bachelor's degree in Computer Engineering — *Aug 1989 - Jul 1995*

Thesis: 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

Full list available at Credly

AWS Certified Data Analytics – Specialty, Amazon Web Services Training and Certification (May 2023)

Certified Information Systems Security Professional (CISSP), ISC2 (Apr 2019)

Research

See Publications for publication details.

Phantom — *2008 - 2009*
IBM Research

- Developed security solution for VMware virtual environments using virtual machine introspection
- Implemented intrusion detection and prevention capabilities based on VMware VMsafe API
- Publications: [13]

Billy Goat: Active worm detection and capture — *2002 - 2008*
IBM Research

- Pioneered active worm-capture technology that became the foundation for modern honeypots and honeynets
- Designed system to simulate thousands of vulnerable hosts to attract and capture propagating worms
- Implemented automated analysis to extract signatures and update intrusion detection/prevention systems
- Publications: [18], [25]

Router-based Billy Goat — *2005 - 2007*
IBM Research

- Deployed active worm-capture at network boundary, coupled with border router infrastructure
- Implemented automatic IP address spoofing to cover entire external address space
- Enabled accurate detection of infected local machines and prevention of outbound worm propagation
- Publications: [17]

SOC in a Box — *2005 - 2007*
IBM Research

- Pioneered integrated security appliance concept, precursor to modern Unified Threat Management systems
- Combined multiple security functions: intrusion detection, worm detection, vulnerability scanning, and network discovery

Exorcist — *2001 - 2002*
IBM Research

- Developed host-based intrusion detection system using behavior analysis
- Implemented system call sequence monitoring for anomaly detection

Ph.D. Thesis: Using internal sensors and embedded detectors for intrusion detection — *1996 - 2001*
Purdue University

- Investigated novel approaches to data collection for intrusion detection systems
- Implemented and evaluated internal sensors and embedded detectors as data collection mechanisms
- Analyzed trade-offs and effectiveness of different sensor placement strategies in IDS architectures
- Publications: [11], [19], [20], [27], [26], [32]

Using autonomous agents for intrusion detection — *1997 - 1999*
Purdue University

- Designed AAFID architecture for distributed monitoring and intrusion detection using autonomous agents
- Implemented and published prototype as open source, contributing to distributed IDS research community
- Explored novel research approaches in distributed intrusion detection
- Publications: [21], [22], [28], [35], [33], [34]

Analysis of a denial-of-service attack on TCP/IP (Synkill) — *1997*
Purdue University

- Analyzed SYN-flooding denial-of-service attack against TCP/IP protocol
- Developed defense tool to mitigate SYN-flooding attacks

- Publications: [23], awarded the 2020 IEEE Security & Privacy Test of Time Award

Software

Open-source software projects

- GitHub: github.com/zzamboni
- GitLab: gitlab.com/zzamboni

Pilatus *Jan 2005 - Dec 2007*

IBM Research (not publicly available)

An automated 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.

Embedded Sensors Project *Jan 1999 - Dec 2001*

Purdue University

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

Honors & Awards

May 2020	**IEEE Security & Privacy Test of Time Award (IEEE S&P page, CERIAS blog post)**, IEEE
2010	**CFEngine Champion**, CFEngine AS
Jul 2001	**Josef Raviv Memorial Postdoctoral Fellowship**, IBM
Sep 2000	**UPE Microsoft Scholarship Award**, UPE and Microsoft
Apr 1998	**Member of Upsilon Pi Epsilon**, Association for Computing Machinery (ACM)
Apr 2001	**Member of Phi Beta Delta**, Phi Beta Delta honor society
May 1996	**Fulbright Scholarship (for pursuing Ph.D. studies at Purdue University)**, Fulbright Program and CONACYT

Program Committees and Boards

Editorial Board Member *2011 - 2013*

Computers & Security Journal, Elsevier

Program Committee (2001-2005), Program Chair (2006), Steering Committee (2007-2017) *2001 - 2017*

Intl. Symposium on Recent Advances in Intrusion Detection (RAID)

Program co-chair *Jun 2009*

IBM Academy of Technology Security and Privacy Symposium (internal IBM event)

Program Chair *Sep 2009*

ZISC Workshop on Security in Virtualized Environments and Cloud Computing

Program Chair *Jul 2008*

Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)

Program Committee Member *May 2007*

IEEE Security and Privacy Symposium

Program Committee Member *2003 - 2007*

Annual Computer Security Applications Conference (ACSAC)

Founder and Program Committee Member *1994 - 2000*

Computer Security Day Conference

Student Advising

Urko Zurutuza Ortega (Mondragon University, Spain) *Jan 2005 - Dec 2008*

IBM Research

- Ph.D. co-advisor
- Thesis: Data Mining Approaches for Analysis of Worm Activity Towards Automatic Signature Generation

Milton Yates (ENST Bretagne, France) *Jan 2005 - Dec 2005*

IBM Research

- External Diploma Thesis advisor
- Thesis: The Router-based Billy Goat Project

Candid Wüest (ETH Zurich, Switzerland) *Jan 2002 - Dec 2003*
IBM Research

- Diploma Thesis advisor
- Thesis: Desktop Firewalls and Intrusion Detection

Daniele Sgandurra (University of Pisa, Italy) *Jan 2009 - Dec 2009*
IBM Research

- Internship advisor
- Project: Design and implementation of process injection using virtual machine introspection.

Martin Carbone (Georgia Institute of Technology, U.S.A.) *Jan 2007 - Dec 2007*
IBM Research

- Internship advisor
- Project: Implementation of a proof of concept Hyperjacking attack on Intel platform.

Teaching

CISSP training (30 hours) *2020*
iNetworks, Mexico (remote class)

CFEngine one-day training class (8 hours) *2011 - 2013*
Multiple venues

Virtualization lecture (2 hours), Systems Security class, Computer Science Dept. *2011 - 2013*
ETH Zürich

Intrusion detection: Basic concepts and current research at IBM class (3 hours), Information Technology Security Spring School *2005*
University of Lausanne

Introduction to Computer Security class (40 hours) *2003*
ITESM, Mexico

EE495 (Information Extraction, Retrieval and Security) course *2000*
Purdue University, U.S.A.

- Co-designed eight security-related lectures and taught two of them
- Co-designed the class project

SSH: Achieving secure communication over insecure channels class *2000*
CSI NetSec conference, U.S.A.

Protecting your computing system class *1997*
Schlumberger, U.S.A.

Supercomputing Internship Program Courses *1991 - 1996*
UNAM, Mexico

Designed and taught multiple courses (10-40 hours long) on the following topics:

- Introduction to Unix
- Unix utilities
- Unix security
- Basic Unix administration
- Advanced Unix administration
- UNICOS system administration on Cray supercomputers

Other Professional Activities

The Association for Computing Machinery (ACM) *1998 - Present*
Member

Purdue.pm, the Purdue Perl Users Group *2000*
Founder

Purdue University Chapter of Upsilon Pi Epsilon *1998 - 2000*
Secretary and President

Publications

Full list online

Skills

Leadership	32 years of multidisciplinary team and project leadership experience · IT Enterprise Architecture · Scaled Agile Framework (SAFe)
Communication	Excellent written and spoken communication skills · Extensive public speaking experience · Professional writing and teaching experience
Information and Cyber Security	Enterprise security governance · Enterprise security architecture · Virtualization and cloud computing security · Risk management and compliance · Intrusion detection and prevention · Software security and secure software development · ISO27001
Technology	Broad and deep IT expertise · Cloud computing · Computer security · Operating systems · Networking · Configuration management · Software & services development · Programming languages
Cloud Computing	AWS architecture · AWS security · AWS infrastructure and development · Held multiple AWS Professional- and Associate-level certifications (Security, Solutions Architect, Dev/Sysops) from 2022-2025
Research	Ph.D. in Computer Science · 9 years of experience at IBM Research
Programming Languages	Ruby · Python · C · Perl · Java · LISP family (Clojure, Racket) · Unix shells and tools
Systems & Development	Unix/Linux systems engineering and administration · System health management and monitoring · Cloud platforms · Software development · Configuration management (CFEngine, Puppet, Chef, Ansible)
Development Environments & Technologies	Unix/Linux · Cloud Foundry · Amazon EC2 · macOS · VMware (ESX, vSphere) · OpenStack · Docker · REST APIs · XML and related technologies · Network programming · Database programming (SQL) · Kernel programming (OpenBSD and Linux) · HTML

Languages

Spanish	Native
English	Full proficiency
German	Intermediate proficiency (B2 level)

References

- Available by request