Diego **Zamboni**

IT Security Architect · Computer Scientist · Team and Project Leader

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

Introduction

I am a senior computer security expert, computer scientist, IT architect, team and project leader with 28 years of professional experience, specialized in the areas of Computer Security, Cloud Computing, Self-healing Systems and Configuration management. I possess a strong combination of theoretical and practical knowledge in multiple areas of computing that make me able to analyze complex problems, design and implement elegant and pragmatic solutions. I have ample experience in technical writing, teaching and public speaking. I have a rich background which includes advanced education, scientific research, software architecture, practical technical knowledge, team leadership and customer-facing experience.

Skill and Experience Overview

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.
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.).
Configuration management	CFEngine (Author of *Learning CFEngine 3* published by O'Reilly Media), Ansible, Puppet.
Languages	Spanish (native), English (100%), German (B1/B2 level).
Other skills	Excellent written and spoken communication skills, customer-facing experience, project and product management experience.

Experience

Swisscom

2015 to date *Switzerland*

Enterprise Security Architect — *Apr. 2019 to date*

- As Security Architect for the IT Clouds Large Solution, I participate in the design and definition of security-relevant capabilities, compliance and business goals of cloud platforms built by Swisscom.
- As Enterprise Architect, I participate in the overall design, discussion and proposals regarding the future of the products and solutions offered by Swisscom.

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

- The HSM team has an expanded scope 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, and 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.–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–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 (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*

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.

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

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.

Foundation Certificate in IT-Service Management (ITILv2) *April 2006*

IBM Micro MBA program *March 2003*

Research

(see “Publications” for publication reference details)

Research projects at IBM (selected)

Project Phantom *2008–2009*

- Security for VMware virtual environments using virtual machine introspection (based on the VMware VMsafe API) to provide detection and prevention capabilities with increased security and reliability.
- Publications: [10].

Code instrumentation for intrusion detection *2007*

Exploration of code instrumentation and low-level monitoring mechanisms for efficient and accurate intrusion detection and prevention.

Billy Goat: Active worm detection and capture *2002–2008*

- An active worm-detection system, in wide deployment in the IBM worldwide internal network. Billy Goat listens for connections to unused IP address ranges and actively responds to those connections to accurately detect worm-infected machines, and in many cases capture the worms themselves. Billy Goat is engineered for distributed deployment, with each device containing standalone detection and reporting capabilities, together with data centralization features that allow network-wide data analysis and reporting.
- Publications: [15, 22]

Router-based Billy Goat *2005–2007*

- An active worm-capture device deployed at the network boundary and coupled with the border router, that allows the Billy Goat to effectively and automatically spoof every unused IP address outside the local network. This makes it possible for the Router-based Billy Goat to accurately detect local infected machines and prevent them from establishing connections to the outside, limiting the propagation of the worms to the outside network.
- Publications: [13]

SOC in a Box *2005–2007*

Integrated device containing multiple security tools: intrusion detection, worm detection, vulnerability scanning and network discovery.

Exorcist *2001–2002*

Host-based, behavior-based intrusion detection using sequences of system calls.

Ph.D. Thesis Research

Utilization of internal sensors and embedded detectors for intrusion detection

- Study of data collection methods for intrusion detection systems.
- Implementation of novel methods for data collection in intrusion detection systems.
- Analysis of the properties, advantages and disadvantages of internal sensors and embedded detectors as data collection and analysis elements in intrusion detection systems.
- Publications: [8, 16, 17, 24, 29]

Additional research projects

Using autonomous agents for intrusion detection

- Design and documentation of an architecture (AAFID) to perform distributed monitoring and intrusion detection using autonomous agents.
- Implementation of a prototype according to the architecture. This prototype is published as open source.
- Exploration of research issues in the distributed intrusion detection area.
- Publications: [18, 19, 25, 32, 30, 31].

Analysis of a denial-of-service attack on TCP/IP (Synkill)

- Collaborated in the analysis of the SYN-flooding denial-of-service attack against TCP and in the implementation of a defense tool.
- Publications: [20].

Software Development

Programming languages	C, Perl, Java, AWK, Unix shells (Elvish, Bourne shell, C shell, Korn shell), Python, PHP, Ruby, Objective C, Cocoa (MacOS X), Go, Clojure.
Environments	Unix/Linux, OpenStack, Cloud Foundry, Amazon EC2, Mac OS X.
Other	REST APIs, Riemann (event stream processing), XML and related technologies, network programming, database programming (SQL), kernel programming (OpenBSD and Linux), HTML.

Major publicly-available software projects

CopperExport *2005–2008*

An export plugin for iPhoto.

mailer *1999-2000*

An email alias and list manager, for use at CERIAS (Center for Education and Research in Information Assurance and Security) in Purdue University.

AAFID2 prototype *1997-1999*

A distributed intrusion detection system, based on the AAFID intrusion detection architecture developed at CERIAS, in Purdue University.

Other software projects (not publicly available)

Pilatus *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 *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 *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) *2000-2001*

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.

Other IT technologies

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.

Teaching and Advising

Students

Daniele Sgandurra, University of Pisa, Italy *Internship advisor* *2009*

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

Martin Carbone, Georgia Institute of Technology, U.S.A. — *Internship advisor* — *2007*

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

Urko Zurutuza Ortega, Mondragon University, Spain — *Ph.D. co-advisor* — *2005–2008*

Thesis: Data Mining Approaches for Analysis of Worm Activity Towards Automatic Signature Generation.

Milton Yates, ENST Bretagne, France — *External Diploma Thesis advisor* — *2005*

Thesis: The Router-based Billy Goat Project.

Candid Wüest, ETH Zurich, Switzerland — *Diploma Thesis tutor* — *2002–2003*

Thesis: Desktop Firewalls and Intrusion Detection.

Teaching

CFEngine one-day training class (8 hour class)	*Multiple venues*	*2011–2013*
"Virtualization" lecture (2 hours), Systems Security class, Computer Science Dept.	*ETH Zürich*	*2008*
"Intrusion detection: Basic concepts and current research at IBM" class (3 hours), Information Technology Security Spring School	*University of Lausanne*	*2005*
"Introduction to Computer Security" class (40 hours)	*ITESM, Mexico*	*2003*
EE495 (*Information Extraction, Retrieval and Security*) course	*Purdue University, U.S.A.*	*2000*

- Collaborated in the design of eight security-related lectures and taught two of them.
- Participated in the design of the class project.

"SSH: Achieving secure communication over insecure channels" class	*CSI NetSec conference, U.S.A.*	*2000*
"Protecting your computing system" class	*Schlumberger, U.S.A.*	*1997*
Supercomputing Internship Program Courses	*UNAM, Mexico*	*1991–1996*

- Participated in the design and teaching of the syllabus, structure and contents of multiple courses 10–40 hours long, including the following topics:
  - Introduction to Unix
  - Unix utilities
  - Unix security
  - Basic Unix administration
  - Advanced Unix administration
  - UNICOS system administration on Cray supercomputers

Honors & Awards

2010	**CFEngine Champion,** awarded by CFEngine AS	*Norway*
Jul. 2001	**Josef Raviv Memorial Postdoctoral Fellowship,** awarded by IBM	*U.S.A.*
Apr. 2001	**Member of Phi Beta Delta,** honor society recognizing scholarly achievement.	*U.S.A.*
Sep. 2000	**UPE Microsoft Scholarship Award,** awarded for academic record and activities.	*U.S.A.*
Apr. 1998	**Member of Upsilon Pi Epsilon,** the ACM Computer Sciences honor society	*U.S.A.*
May 1996	**Fulbright Scholarship,** for pursuing Ph.D. studies at Purdue University	*Mexico*

Other Professional Activities

1998–	**Member,** The Association for Computing Machinery (ACM)	
2000	**Founder,** Purdue.pm, the Purdue Perl Users Group	*U.S.A.*
1999–2000	**President,** Purdue University Chapter of Upsilon Pi Epsilon	*U.S.A.*
1998–1999	**Secretary,** Purdue University Chapter of Upsilon Pi Epsilon	*U.S.A.*

Program Committees and Boards

2011–2013	**Editorial Board,** Computers & Security Journal	
2007–2012	**Steering Committee,** Intl. Symposium on Recent Advances in Intrusion Detection (RAID)	
2006	**Program chair,** 9th Intl. Symposium on Recent Advances in Intrusion Detection (RAID)	*Germany*
2001–2005	**Program Committee,** Intl. Symposium on Recent Advances in Intrusion Detection (RAID)	
2009	**Program co-chair,** IBM Academy of Technology Security and Privacy Symposium	
2009	**Program chair,** ZISC Workshop on Security in Virtualized Environments and Cloud Computing	*Switzerland*
2008	**Program chair,** Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)	*France*
2007	**Program Committee,** IEEE Security and Privacy Symposium	*U.S.A.*
2003–2007	**Program Committee,** Annual Computer Security Applications Conference (ACSAC)	
1994–2000	**Program Committee,** International Computer Security Day Conference	*Mexico*
1994–1995	**Organizer,** International Computer Security Day Conference	*Mexico*

Selected publications

Books

[2] Diego Zamboni. *Learning CFEngine 3*. O'Reilly Media, Inc. 2012–2017, self-published since 2017. ISBN: 9781449312206. URL: http://cf-learn.info/.

[1] Diego Zamboni. *Learning Hammerspoon*. Self published, Oct. 2018. URL: https://leanpub.com/learning-hammerspoon.

Editorial Activities

[3] *Computers & Security Journal*. Elsevier. Member of the Editorial Board. 2011–2013.

[4] Deborah Frincke, Andreas Wespi, and Diego Zamboni, eds. *Computer Networks* 51.5 (2007): *From Intrusion Detection to Self-Protection*. ISSN: 1389-1286. URL: http://dx.doi.org/10.1016/j.comnet.2006.10.004.

[5] Diego Zamboni and Christopher Kruegel, eds. Recent Advances in Intrusion Detection (RAID): 9th International Symposium (Hamburg, Germany, Sept. 20–22, 2006). Lecture Notes in Computer Science. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2006. ISBN: 354039723X.

[6] Alfonso Valdes and Diego Zamboni, eds. Recent Advances in Intrusion Detection (RAID): 8th International Symposium (Seattle, WA, U.S.A. Sept. 7–9, 2005). Lecture Notes in Computer Science. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2005. ISBN: 3540317783.

[7] Diego Zamboni, ed. *Software: Practice and Experience* 33.5 (Apr. 2003): *Special issue on "Security Software"*. URL: http://onlinelibrary.wiley.com/doi/10.1002/spe.v33:5/issuetoc.

Theses

[8] Diego Zamboni. "Using Internal Sensors for Computer Intrusion Detection". CERIAS TR 2001-42. PhD thesis. West Lafayette, IN: Purdue University, Aug. 2001. URL: https://zzamboni.org/files/theses/zamboni-phd-thesis.pdf.

[9] Diego Zamboni. "Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix (*UNAM/Cray project for Unix System Security*)". Spanish. B.Sc. Thesis. Universidad Nacional Autonoma de México, June 1995. URL: https://zzamboni.org/files/theses/zamboni-bachelors-thesis.pdf.

Refereed Papers

[10] Mihai Christodorescu et al. "Cloud Security is Not (Just) Virtualization Security: A Short Paper". In: *Proceedings of the 2009 ACM Workshop on Cloud Computing Security*. CCSW '09. Chicago, Illinois, USA: ACM, 2009, pp. 97–102. ISBN: 978-1-60558-784-4. DOI: 10.1145/1655008.1655022. URL: http://doi.acm.org/10.1145/1655008.1655022.

[11] U. Zurutuza et al. "Un marco inteligente para el análisis de tráfico generado por gusanos en Internet (An intelligent framework for analysis of worm-generated Internet traffic)". Spanish. In: *Actas de la X Reunión Española sobre Criptología y Seguridad de la Información (X Spanish Meeting on Cryptology and Information Security)*. Sept. 2008.

[12] Urko Zurutuza, Roberto Uribeetxeberria, and Diego Zamboni. "A data mining approach for analysis of worm activity through automatic signature generation". In: *Proceedings of the 1st ACM workshop on AISec (AISec'08)*. Alexandria, Virginia, USA: Association for Computing Machinery, Oct. 2008, pp. 61–70. ISBN: 978-1-60558-291-7. URL: http://doi.acm.org/10.1145/1456377.1456394.

[13] Diego Zamboni, James Riordan, and Milton Yates. "Boundary detection and containment of local worm infections". In: *Proceedings of the 3rd Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI'07)*. Usenix. June 2007. URL: http://www.usenix.org/events/sruti07/tech/full_papers/zamboni/zamboni.pdf.

[14] Urko Zurutuza, Roberto Uribetxeberria, and Diego Zamboni. “Anàlisis de datos procedentes de un sistema de detección de gusanos mediante técnicas de clustering (Analysis of data from a worm-detection system using clustering techniques)”. In: *Actas del II Simposio sobre Seguridad Informática (SSI’2007), II Congreso Español de Informática (CEDI 2007) (Proceedings of the II Symposium on Computer Security, II Spanish Conference on Informatics)*. Sept. 2007, pp. 87–94.

[15] James Riordan, Diego Zamboni, and Yann Duponchel. “Building and deploying Billy Goat, a worm-detection system”. In: *Proceedings of the 18th Annual FIRST Conference*. June 2006.

[16] Florian Kerschbaum, Eugene H. Spafford, and Diego Zamboni. “Using internal sensors and embedded detectors for intrusion detection”. In: *Journal of Computer Security* 10.1,2 (2002), pp. 23–70. URL: http://iospress.metapress.com/content/rkylmv8hepn2p71d/.

[17] Florian Kerschbaum, Eugene H. Spafford, and Diego Zamboni. “Using embedded sensors for detecting network attacks”. In: *Proceedings of the 1st ACM Workshop on Intrusion Detection Systems*. Ed. by Deborah Frincke and Dimitris Gritzalis. CERIAS TR 2000-25. ACM SIGSAC. Nov. 2000. URL: https://www.cerias.purdue.edu/apps/reports_and_papers/view/1641/.

[18] Eugene H. Spafford and Diego Zamboni. “Intrusion Detection using Autonomous Agents”. In: *Computer Networks* 34.4 (Oct. 2000), pp. 547–570. URL: http://dx.doi.org/10.1016/S1389-1286(00)00136-5.

[19] Jai Sundar Balasubramaniyan et al. “An Architecture for Intrusion Detection using Autonomous Agents”. In: *Proceedings of the Fourteenth Annual Computer Security Applications Conference*. IEEE Computer Society, Dec. 1998, pp. 13–24. URL: http://zzamboni.org/diego/pubs/aafid-acsac98.pdf.

[20] Christoph L. Schuba et al. “Analysis of a Denial of Service Attack on TCP”. In: *Proceedings of the 1997 IEEE Symposium on Security and Privacy*. IEEE Computer Society. IEEE Computer Society Press, May 1997, pp. 208–223. URL: http://homes.cerias.purdue.edu/~zamboni/pubs/synkill.pdf.

[21] Diego Zamboni. “SAINT —A Security Analysis Integration Tool”. In: *Proceedings of the 1996 Systems Administration, Networking and Security Conference*. Washington, D.C., May 1996. URL: http://homes.cerias.purdue.edu/~zamboni/pubs/SAINT.pdf.

Tech Reports

[22] James Riordan, Diego Zamboni, and Yann Duponchel. *Billy Goat, an Accurate Worm-Detection System*. Research Report RZ3609. IBM Research, Nov. 2005. URL: http://tinyurl.com/bgtechreport.

[23] Eugene Spafford and Diego Zamboni. *Data Collection mechanisms for intrusion detection systems*. CERIAS Technical Report 2000-08. 1315 Recitation Building, West Lafayette, IN: CERIAS, Purdue University, June 2000. URL: http://homes.cerias.purdue.edu/~zamboni/pubs/2000-08.pdf.

[24] Diego Zamboni. *Doing intrusion detection using embedded sensors— Thesis proposal*. CERIAS Technical Report 2000-21. West Lafayette, IN: CERIAS, Purdue University, Oct. 2000. URL: http://homes.cerias.purdue.edu/~zamboni/pubs/prelim.pdf.

[25] Jai Sundar Balasubramaniyan et al. *An Architecture for Intrusion Detection using Autonomous Agents*. Technical Report 98-05. COAST Laboratory, Purdue University, May 1998. URL: http://homes.cerias.purdue.edu/~zamboni/pubs/tr9805.pdf.

Presentations at Conferences and Workshops

[26] Diego Zamboni and Bill Chapman. *Chaos Heidi vs. Orchard: Self-Disruption and Healing in a Cloud Foundry-Based Service Environment*. Presented at the Cloud Foundry Summit Silicon Valley 2016. May 2016. URL: https://www.youtube.com/watch?v=%20Wr4E--kr_KE.

[27] Diego Zamboni and Mark Burgess. *The Future of In-Container Configuration Management*. Invited talk at the 2014 Usenix Configuration Management Summit (UCMS’14). June 2014. URL: https://www.usenix.org/conference/ucms14/summit-program/presentation/zamboni.

[28] Mike Svoboda and Diego Zamboni. *Leveraging In-Memory Key Value Stores for Large-Scale Operations*. Invited talk at the 27th Large Installation System Administration (LISA) Conference. Nov. 2013. URL: https://www.usenix.org/conference/lisa13/leveraging-memory-key-value-stores-large-scale-operations.

[29] Eugene H. Spafford and Diego Zamboni. *Design and implementation issues for embedded sensors in intrusion detection*. Presented at the Third International Workshop on Recent Advances in Intrusion Detection (RAID2000). Oct. 2000. URL: http://homes.cerias.purdue.edu/~zamboni/pubs/sensors-raid2000.pdf.

[30] Diego Zamboni. *Building a Distributed Intrusion Detection System with Perl*. Presented at The Perl Conference 4.0. Monterey, CA, July 2000. URL: http://homes.cerias.purdue.edu/~zamboni/pubs/tpc40.pdf.

[31] Eugene H. Spafford and Diego Zamboni. “New directions for the AAFID architecture”. In: *Proceedings of the Second International Workshop on Recent Advances in Intrusion Detection (RAID99)*. Online proceedings, available at http://www.raid-symposium.org/raid99/. West Lafayette, IN, Sept. 1999.

[32] Eugene H. Spafford and Diego Zamboni. “AAFID: Autonomous Agents for Intrusion Detection”. In: *Proceedings of the First International Workshop on Recent Advances in Intrusion Detection (RAID98)*. Online proceedings, available at http://www.raid-symposium.org/raid98/. Louvain-la-Neuve, Belgium, Sept. 1998.

Invited Talks and Articles

[33] Mark Burgess and Diego Zamboni. "CFEngine's Decentralized Approach to Configuration Management". In: *InfoQ* (June 2014). URL: http://www.infoq.com/articles/cfengine-view-on-it-automation.

[34] Diego Zamboni. *Security in the Third Wave of IT Engineering*. Keynote talk, presented at the 2011 Computer Security Congress in Mexico City. Nov. 2011. URL: http://blog.zzamboni.org/security-in-the-third-wave-of-it-engineering.

[35] Martim Carbone, Diego Zamboni, and Wenke Lee. "Taming Virtualization". In: *IEEE Security and Privacy* 6.1 (2008), pp. 65–67. ISSN: 1540-7993. URL: http://www.computer.org/portal/web/csdl/doi/10.1109/MSP.2008.24.

[36] Diego Zamboni. *From Intrusion Detection to Remediation and Beyond: Evolution, Trends, and Research at IBM*. Invited talk at the annual meeting of the Swiss Chapter of the Sigma XI Honorary Scientific Society. Nov. 2006.

[37] James Riordan, Andreas Wespi, and Diego Zamboni. "How to Hook Worms". In: *IEEE Spectrum* (May 2005). URL: http://www.spectrum.ieee.org/may05/1124.

[38] Diego Zamboni. *Intrusion what? From detection to prevention and beyond*. Talk at the Zurich Information Security Center Information Security Colloquium. Dec. 2005.

[39] James Riordan and Diego Zamboni. "Billy Goat Detects Worms and Viruses". In: *ERCIM News* 56 (Jan. 2004). URL: http://www.ercim.org/publication/Ercim_News/enw56/riordan.html.

[40] Diego Zamboni. Diez Años de Aciertos y Fallas — ¿Qué Hemos Aprendido y Qué nos Depara el Futuro en la Seguridad? *(Ten years of hits and misses — what have we learned, and what does the future in security hold for us?)* Keynote talk, presented at the 2004 Computer Security Congress in Mexico City. May 2004.

[41] Diego Zamboni. *AAFID: Autonomous Agents for Intrusion Detection*. Invited talk, presented at the 1999 Indiana Client Server and Internet Conference. Sept. 1999.

[42] Diego Zamboni. "*Avances en el sistema y arquitectura AAFID para detección de intrusos* (Advances in the AAFID intrusion detection architecture and system)". In: *Proceedings of the 1999* Día Internacional de la Seguridad en Cómputo *(International Computer Security Day) conference*. Mexico City, Mexico, Oct. 1999.

[43] Diego Zamboni. "AAFID: *Detección de Intrusos usando Agentes Autónomos* (Intrusion Detection using Autonomous Agents)". In: *Proceedings of the 1998* Día Internacional de la Seguridad en Cómputo *(International Computer Security Day) conference*. Mexico City, Mexico, Nov. 1998.

[44] Diego Zamboni. *Unix Host Security Tools*. Invited talk, presented at the Cellular Telecommunications Industry Association (CTIA) Network Vulnerability Workshop. Jan. 1998.

Patents

[45] Carbone Martim et al. "Hardware Emulation Using On-the-fly Virtualization". Granted Patent US 9250942 B2 (United States). Feb. 2, 2016. URL: https://lens.org/107-038-681-631-856.

[46] Jansen Bernhard et al. "Secure User Interaction Using Virtualization". Granted Patent US 8516564 B2 (United States). Aug. 20, 2013. URL: https://lens.org/012-709-360-909-626.

[47] Zamboni Diego M et al. "Detection And Control Of Peer-to-peer Communication". Patent Family of US 8219679 B2 (United States, others). July 10, 2012. URL: https://lens.org/151-595-773-205-878.

[48] Riordan James F, Rissmann Ruediger, and Zamboni Diego M. "IP Network Management Based On Automatically Acquired Network Entity Status Information". Patent Family of US 8055751 B2 (United States, others). Nov. 8, 2011. URL: https://lens.org/065-534-634-366-763.

[49] Duponchel Yann et al. "Methods For Operating Virtual Networks, Data Network System, Computer Program And Computer Program Product". Patent Family of US 7908350 B2 (United States, others). Mar. 15, 2011. URL: https://lens.org/080-322-567-493-840.

[50] Rissmann Ruediger et al. "Network Attack Detection". Patent Family of EP 1866725 B1 (European Patent Office, others). Oct. 20, 2010. URL: https://lens.org/044-792-433-937-531.

[51] Duponchel Yann et al. "Method For Operating Several Virtual Networks". Patent Family of EP 1969777 B1 (European Patent Office, others). Jan. 27, 2010. URL: https://lens.org/159-743-880-849-911.

[52] Swimmer Morton D, Wespi Andreas, and Zamboni Diego M. "Preventing Attacks In A Data Processing System". Granted Patent US 7555777 B2 (United States). June 30, 2009. URL: https://lens.org/077-245-544-178-974.

[53] Schuba Christoph L et al. "Network Protection For Denial Of Service Attacks". Granted Patent US 6725378 B1 (United States). Apr. 20, 2004. URL: https://lens.org/009-701-089-204-105.

Other Publications

[54] Diego Zamboni. *Notas de Utilerías de Unix (Unix utilities course notes)*. Academic Computing Services Center, National Autonomous University of Mexico. Mar. 1993. URL: http://zzamboni.org/files/pubs/unixutil.pdf.

References

Available by request.