Diego **Zamboni**

IT Enterprise Security Architect · Team and Project Leader · Computer Security Scientist

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

Key skills

Leadership	29 years of team and project leadership experience; systems architecture; Scaled Agile Framework (SAFe) methodology and processes.
Computer Security	Enterprise security architecture; risk management; compliance; intrusion detection and prevention (Ph.D. in this area); operating systems and network security; software security and secure software development; virtualization and cloud computing security; CISSP.
Communications	Excellent written and spoken communication skills, with more than 30 years of written and spoken communication and teaching experience in different contexts and topics. I love teaching and writing.
Systems and Development	Unix/Linux systems engineering and administration, system health management and monitoring, cloud platforms (Amazon EC2, Cloud Foundry), software development experience (C, Python, Ruby, Perl, LISP, etc.).
Configuration management	CFEngine, Ansible, Puppet.
Attitude	Always willing to learn about technology, management, and any topic that allows me to continue growing. I am passionate about both technology and people.
Languages	Spanish (native), English (100%), German (B1 level).

Key professional achievements

- Responsible for security architecture, risk management and compliance (ISO27001, FINMA, ISAE3402/3000, etc.) of Swisscom's IT Clouds platforms and related services and components.
- Established and currently lead the Swisscom IT Clouds security community of practice.
- Established and managed the *Health and State Management* team at Swisscom, which designs, implements and operates a framework for scalable monitoring, logging and alerting.
- Designed the *Orchard* monitoring framework for Swisscom's *Application Cloud* platform, and led the team that implemented it and brought it into production.
- Managed the CFEngine language product roadmap.
- Managed customer relationships at HP Enterprise Services in the area of security. This included overseeing the activities of operational and engineering teams, risk and compliance management, requirements discussion and reporting.
- Established and led the first incident response team at UNAM, which has grown into the university's Information Security Organization/UNAM-CERT.
- Designed and implemented the *Billy Goat* malware capture and analysis system at IBM.
- System administration and security monitoring for UNAM's Cray Y-MP supercomputer and Unix workstations.
- Authored multiple books including *Learning CFEngine* (published by O'Reilly Media), *Learning Hammerspoon* and *Literate Configuration*.
- Designed and implemented the first version of the CFEngine Design Center.
- Program chair and program committee member for multiple conferences including RAID symposium, DIMVA conference, the first instances of the *International Computer Security Day* and the *Computer Security* conference at UNAM, and others.
- Member of the Editorial Board of the Computers & Security Journal.

Experience

Swisscom

2015 – Present *Switzerland*

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

- Dual role as a member of the Swisscom Enterprise Architecture team, and as a Solution Security Architect for the Swisscom Cloud Platforms, which include offerings targeted at both the Enterprise and the SMB segments: *Enterprise Service Cloud* (IaaS), *Enterprise Application Cloud* (PaaS), *Dynamic Computing Services* (IaaS), *Enterprise Cloud for SAP Applications* (IaaS).
- As *Solution Security Architect for IT Clouds*, I am a member of the leadership team, and my job is to ensure Swisscom's cloud platforms are secure and compliant. I define, prioritize and drive security-relevant product features, compliance and business goals of the cloud platforms built by Swisscom. I also head the IT Clouds Security Community of Practice, advise on compliance, governance and operational activities.
  - Selected achievements and ongoing activities:
    - Ensure ongoing cloud platform and service compliance with contractual and regulatory standards, including ISO27001, ISAE3402/3000, FINMA and GDPR.
    - Launched the *Security Champions* initiative to promote and improve a culture of security responsibility within the team.
    - Brought various platforms and services within the Swisscom cloud ecosystem to compliance with internal security standards and with external requirements for financial and banking customers, by defining the requirements and working with the engineering teams to prioritize and review the corresponding implementations.
    - Coordinate and oversee periodic threat modeling, audits and penetration tests against the various cloud platforms and services.
    - Establish organization- and team-wide processes for risk management.
- As *Enterprise Architect*, I participate in the design of the future products and solutions offered by Swisscom, in collaboration with architects from all other divisions of the company. These result in proposals that are brought to approval by management and planned for implementation over the next 5-10 years.

Team Lead & Product Owner for Health & State Management *Mar 2016 – Apr 2019*

- In this role, I built and lead a team which evolved on par with the Swisscom cloud platforms to provide monitoring and logging capabilities for Swisscom's cloud platforms. My responsibilities included people management (up to 16 people), requirement definition and prioritization in collaboration with Product Managers and other stakeholders, roadmap and architecture definition for the monitoring, logging and alerting platforms, driving the planning and execution of the work within the team, and participation in the technical implementation.
- Selected achievements:
  - Oversaw the transition of the *Enterprise Cloud 1* LEMM (Logging, Event Management and Monitoring) and Access & Inventory frameworks into maintenance mode as the platform was retired.
  - Oversaw the transition of the *Application Cloud* platform from the Orchard monitoring framework into a new framework based on the TICK stack.
  - Defined the scope and mission of the Health and State Management (HSM) team as part of the new *Enterprise Service Cloud* project.
  - Defined logging and monitoring architecture for the *Enterprise Service Cloud* platform based on vRealize Operations and vRealize Log Insight.
  - Defined requirements, oversaw planning and execution of the HSM team's mission to design, implement and manage Health Management and Monitoring components as the IT Clouds scope expanded to other platforms, including Application Cloud, Enterprise Cloud for SAP applications (EC4SAP), Dynamic Computing Services, and related services and components.
  - Defined architecture and oversaw implementation of Customer Log Forwarding service.
  - Managed business relationship and technical implementation of OpsGenie for alert management in IT Clouds.
  - Defined and implemented integrations between Jira and OpsGenie for alerting of user-reported incidents.
- 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 team of three people and lead the *Orchard* project through its implementation, production release and further improvements and development.

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

Senior Platform Architect — *Aug 2014 – Jul 2015*

- Designed the architecture for the *Orchard* health-management and self-healing components of Swisscom's *Application Cloud* Platform-as-a-Service Offering. This system performed self-monitoring and self-healing of the infrastructure and platform components.
- Implemented initial prototype of the *Orchard* platform.
  - 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*

- CFEngine Advocate, 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*

- Acted as 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.

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.

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: [12].

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: [17, 24]

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: [15]

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

Using 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: [10, 18, 19, 26, 31]

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: [20, 21, 27, 34, 32, 33].

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: [22].

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, Clojure, Racket, Emacs LISP.
Development environments	Unix/Linux, Cloud Foundry, Amazon EC2, macOS.
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://gitlab.com/zzamboni and 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 (Purdue University) *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.

Honors & Awards

2010	**CFEngine Champion**, CFEngine AS	*Norway*
Jul 2001	**Josef Raviv Memorial Postdoctoral Fellowship**, 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**, honor society recognizing scholarly achievement	*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 –	**The Association for Computing Machinery (ACM)**, Member	
2000	**Purdue.pm, the Purdue Perl Users Group**, Founder	*U.S.A.*
1999	**Purdue University Chapter of Upsilon Pi Epsilon**, President	*U.S.A.*
1998	**Purdue University Chapter of Upsilon Pi Epsilon**, Secretary	*U.S.A.*

Program Committees and Boards

2011–2013	**Editorial Board Member**, Computers & Security Journal	
2007–2012	**Steering Committee Member**, Intl. Symposium on Recent Advances in Intrusion Detection	
2006	**Program chair**, 9th Intl. Symposium on Recent Advances in Intrusion Detection (RAID)	*Germany*
2006	**Program Committee Member**, Intl. Symposium on Recent Advances in Intrusion Detection	
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 Member**, IEEE Security and Privacy Symposium	*U.S.A.*
2003–2007	**Program Committee Member**, Annual Computer Security Applications Conference (ACSAC)	
1994–2000	**Program Committee Member**, International Computer Security Day Conference	*Mexico*
1994–1995	**Organizer**, International Computer Security Day Conference	*Mexico*

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* — *2011 – 2013*

"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

Selected Publications

Books

[1] Diego Zamboni. *Utilerías de Unix (Unix utilities course notes)*. Aug. 2019. URL: https://leanpub.com/utileras-unix.

[2] Diego Zamboni. *Literate Config*. Nov. 2019. URL: https://leanpub.com/lit-config.

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

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

Editorial Activities

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

[6] 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.

[7] 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.

[8] 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.

[9] 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

[10] Diego Zamboni. "Using Internal Sensors for Computer Intrusion Detection". CERIAS TR 2001-42. PhD thesis. West Lafayette, IN: Purdue University, Aug. 2001. URL: https://www.cerias.purdue.edu/apps/reports_and_papers/view/1800.

[11] 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

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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/.

[19] 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/.

[20] 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.

[21] 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/files/pubs/aafid-acsac98.pdf.

[22] 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: https://www.cerias.purdue.edu/apps/reports_and_papers/view/605.

[23] 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://zzamboni.org/files/pubs/SAINT.pdf.

Tech Reports

[24] 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.

[25] 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: https://www.cerias.purdue.edu/apps/reports_and_papers/view/1842.

[26] Diego Zamboni. *Doing intrusion detection using embedded sensors— Thesis proposal*. CERIAS Technical Report 2000-21. West Lafayette, IN: CERIAS, Purdue University, Oct. 2000. URL: https://www.cerias.purdue.edu/apps/reports_and_papers/view/581.

[27] Jai Sundar Balasubramaniyan et al. *An Architecture for Intrusion Detection using Autonomous Agents*. Technical Report 98-05. COAST Laboratory, Purdue University, May 1998. URL: https://www.cerias.purdue.edu/apps/reports_and_papers/view/65.

Presentations at Conferences and Workshops

[28] 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.

[29] 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.

[30] 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.

[31] 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://zzamboni.org/files/pubs/sensors-raid2000.pdf.

[32] Diego Zamboni. *Building a Distributed Intrusion Detection System with Perl*. Presented at The Perl Conference 4.0. Monterey, CA, July 2000. URL: http://zzamboni.org/files/pubs/tpc40.pdf.

[33] 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. URL: https://www.cerias.purdue.edu/apps/reports_and_papers/view/3487.

[34] 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

[35] 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.

[36] 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: https://zzamboni.org/post/security-in-the-third-wave-of-it-engineering/.

[37] 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.

[38] 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.

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

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

[41] 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.

[42] 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.

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

[44] 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.

[45] 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.

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

Patents

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] 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.

References

Available by request.