Curriculum Vitæ— Diego Zamboni

December 8, 2014 — short version

Personal information

Full name: Diego Martín Zamboni

Email: diego@zzamboni.org
Web: http://zzamboni.org/
LinkedIn: http://mx.linkedin.com/in/zzamboni
Twitter: http://twitter.com/zzamboni

Introduction I possess a strong combination of theoretical and practical knowledge in multiple areas of computing that make me able to analyze complex problems and both design and implement elegant solutions. I am a team player and a natural leader. I am self-motivated and have excellent communication skills in both Spanish and English, including ample experience in technical writing, teaching and public speaking. I have a strong and rich background, including advanced education, scientific research, practical technical knowledge and customer-facing experience.

Areas of interest and expertise

Computer security: I have extensive experience in intrusion detection and prevention, operating systems security, network security, software security, secure software development, virtualization and cloud computing security, malware detection and containment.

Configuration management and automation: I am a CFEngine 3 expert, author of "Learning CFEngine 3" published by O'Reilly Media, and have knowledge of other configuration management systems including Puppet, Chef and Ansible.

Other areas: Virtualization and cloud computing; software development (C, Perl, Ruby and others); operating system design, implementation and administration; network administration; programming languages; human-computer interfaces.

Work experience

August 2014 to date: Senior Platform Architect at Swisscom Cloud Lab. I am coordinating the health-management and self-healing architecture for Elastic Cloud infrastructure.

August 2013–June 2014: Product Manager at CFEngine AS. I coordinated the CFEngine Design Center, participated in the development of the CFEngine language roadmap, and coordinated the work on CFEngine third-party integration.

October 2011–June 2014: Senior Security Advisor at CFEngine AS. I worked as an overall advocate and fanatic for CFEngine, with a special focus on security. I also worked on developing and implementing the strategy for CFEngine in security.

October 2010–October 2011: Account Security Officer at HP Enterprise Services Mexico. In this position 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.

November 2009–October 2010: IT Outsourcing Service Delivery Consultant at HP Enterprise Services Mexico. My role was to help customer teams by solving complex problems in customer environments.

October 2001–October 2009: Research staff member at the IBM Zurich Research Laboratory. The focus of my work was in intrusion detection, malware detection and containment, and virtualization security. See *Research activities* for details of research.

This is a short version. The full version of this document can be found online at http://zzamboni.org/vita.html.

August 1995–August 1996: Founder and head of Computer Security Area
National Autonomous University of Mexico (UNAM).

Education

Ph.D. in Computer Science: August 1996–August 2001.
Purdue University, Department of Computer Sciences.
Thesis title: *Using Internal Sensors for Computer Intrusion Detection.*
Advisor: Eugene H. Spafford.

M.S. in Computer Science: August 1996–May 1998.
Purdue University, Department of Computer Sciences.
Advisor: Eugene H. Spafford.

Publications (sample)

Books: Diego Zamboni. *Learning CFEngine 3.* O'Reilly Media, Inc., March 2012. ISBN 9781449312206. URL `http://cf-learn.info/`.

Editorial activities: From 2011–2013 I was a member of the Editorial Board for the Computers & Security Journal.

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

Deborah Frincke, Andreas Wespi, and Diego Zamboni. Guest editorial: From intrusion detection to self-protection. *Computer Networks*, 51(5):1233–1238, 2007. ISSN 1389-1286. URL `http://dx.doi.org/10.1016/j.comnet.2006.10.004`.

Refereed papers: 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)*, pages 61–70, New York, NY, USA, October 2008. ISBN 978-1-60558-291-7. URL `http://doi.acm.org/10.1145/1456377.1456394`.

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`.

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.

Florian Kerschbaum, Eugene H. Spafford, and Diego Zamboni. Using internal sensors and embedded detectors for intrusion detection. *Journal of Computer Security*, 10(1,2):23–70, 2002. URL `http://iospress.metapress.com/content/rkylmv8hepn2p71d/`.

Certifications

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

IBM Micro MBA program, March 2003.

Research activities

Selected research projects at IBM:

Project Phantom: (2008-2009) Security for VMware virtual environments using virtual machine introspection.

Code instrumentation for intrusion detection: (2007) Exploration of code instrumentation and low-level monitoring mechanisms for intrusion detection.

Billy Goat: (2002–2008) An active worm-detection system.

Router-based Billy Goat: (2005–2007) An active worm-capture device.

SOC in a Box: (2005–2007) Integrated device containing multiple security tools.

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.

Additional projects: Using autonomous agents for intrusion detection.

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

Software development

Programming language experience: C, Perl, C++, Java, AWK, Unix shells (Bourne, C shell, Korn shell), Python, PHP, Ruby, Objective C, Cocoa (MacOS X).

Other experience: VMware VMsafe virtual machine introspection API, XML and related technologies, network programming, database programming (SQL), kernel programming (OpenBSD and Linux), HTML.

Major publicly-available software projects: CopperExport, **mailer**, **AAFID$_2$ prototype**

System administration experience

Unix systems: Linux, OpenBSD, FreeBSD, MacOS X, MacOS X Server, Solaris.

Configuration management: CFEngine 3, Puppet, Chef, Ansible.

Virtualization, container and cloud platforms: Amazon EC2, Docker, VMware ESX and vSphere.

Security systems and software: Snort IDS, Bro IDS, Nessus vulnerability scanner, HoneyNet platform, Nepenthes malware collection platform.

Other professional activities (sample)

2011–2013: Member of the Editorial Board for the Computers & Security Journal.

2010–2012: Member of the Cfengine Champions (C^3) program, which recognizes outstanding contributions to the CFEngine community.

2007–2012: Member of the Steering Committee for the International Symposium on Recent Advances in Intrusion Detection (RAID).

2009: Program chair for the 2009 workshop of the Zurich Information Security Center (ZISC).

2008: Program chair for the SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA).

2006: Program chair for the 9th International Symposium on Recent Advances in Intrusion Detection (RAID).

Spoken languages

Spanish (native), English (near-native spoken and written fluency), German (basic), French (basic).

References

Available by request.