Curriculum Vitæ— Diego Zamboni

May 10, 2011— 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

Areas of interest and expertise

Computer security:
: Intrusion detection and prevention, operating systems security, network security, software security, secure software development, virtualization and cloud computing security, malware detection and containment.

Other areas:
: Virtualization and cloud computing; configuration management; operating system design, implementation and administration; network administration; programming languages; human-computer interfaces.

Work experience

October 2010 to date:
: Account Security Officer at HP Enterprise Services Mexico. In this position I am the first point of contact for all security-related issues for five HP enterprise customers in Mexico, some of them with international presence. I initiate, advise and manage security-related projects. I handle communication and coordination between technical teams involved in security initiatives. I am involved in all security-related decisions at the sales, design, implementation, delivery and ongoing maintenance stages of IT Outsourcing projects.

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 and by performing analysis, design and implementation of solutions in multiple areas of expertise, including system automation, configuration management, system administration, system design, virtualization, performance and security.

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.

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

November 1991–August 1995:
: Systems Administrator of Cray Supercomputer and Unix workstations; 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.

Research activities

Selected research projects at IBM:

Project Phantom: (2008-2009) Security for VMware virtual environments using virtual machine introspection (in particular, the VMware VMsafe API to provide detection and prevention capabilities with increased security and reliability.

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

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**

Other software projects (not publicly available): Pilatus, SOC in a Box, Billy Goat, Embedded Sensors Project (ESP).

System administration experience

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

Configuration management: cfengine 3. I am a member of the Cfengine Community Contributor program.

Virtualization platforms: VMware ESX server 3.5-4.0, Xen 3.x, User Mode Linux, KVM.

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

Other systems: PostgreSQL, MySQL, DB2, Postfix, Cyrus IMAP, Courier IMAP, Apache.

Publications (sample)

Editorial activities: I am 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://www.sciencedirect.com/science/journal/13891286`.

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/`.

Other professional activities (sample)

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

2010–2011: Member of the Cfengine Community Contributor program, which recognizes outstanding contributions to the cfengine community.

2007–2011: Member of the Steering Committee for the International Symposium on Recent Advances in Intrusion Detection (RAID).

2009: Program co-chair for the 2009 IBM Academy of Technology Security and Privacy Symposium (internal worldwide IBM event).

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

Spoken languages

Spanish (native), English (fluent spoken and written), German (intermediate), French (basic).

References

Available by request.