

# Curriculum Vitae — Diego Zamboni

November 2008

## Personal information

Diego Zamboni  
Kronenstrasse 9,  
CH-8134 Adliswil,  
Switzerland

Daytime phone: +41-(0)44-724-8687  
Personal phone: +41-(0)43-536-9030  
Mobile phone: +41-(0)77-259-8201  
Email: [diego@zzamboni.org](mailto:diego@zzamboni.org)  
Web: <http://diego.zzamboni.org/>

## Research interests and activities

General areas of interest:

Intrusion detection, operating systems security, network security, software security, virtualization, malware detection and containment.

Selected research projects at IBM:

**Project Phantom:** (2008) Security for virtual environments using virtual machine introspection 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, 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

---

This document can be found online at <http://zzamboni.org/brt/about/vita/>

data centralization features that allow network-wide data analysis and reporting.

**Router-based Billy Goat:** (2005–2007) A worm-capture device deployed at the network boundary 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.

**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.

Additional 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 in public distribution.
- Exploration of research issues in the distributed intrusion detection area.

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.

## Educational background

Ph.D. in Computer Science: 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: May 1998.

Purdue University, Department of Computer Sciences.

Advisor: Eugene H. Spafford.

B.S. in Computer Engineering: July 1995.

National Autonomous University of Mexico (UNAM).

Thesis title: *Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix* (UNAM/Cray project for security in the Unix operating system).

## Work experience

October 2001 to date: Research staff member at the IBM Zurich Research Laboratory. The focus of my work has been in intrusion detection, malware detection and containment, and virtualization security.

June–July 1999: Security Analyst at the Internet Security Advisors Group, writing security advisories.

May–August 1997: Internship at Sun Microsystems.

- 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.

August 1995–August 1996: Head of Computer Security Area

National Autonomous University of Mexico (UNAM).

- Founded UNAM’s Computer Security Area.
- 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 21 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—the first one was before the CSA was officially formed). 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).

November 1991–August 1995: Systems Administrator  
National Autonomous University of Mexico (UNAM).

- Administrated the Network Queuing Subsystem (NQS) in UNAM's Cray supercomputer.
- Collaborated in other aspects of the supercomputer administration, including user administration, operating system installation, resource management, and policy making and implementation.
- Directly administrated three Unix workstations, provided support for 19 more.
- Monitored the security of the Cray supercomputer and related workstations.

### Student advising

- 2007: Internship advisor for Martin Carbone, Georgia Institute of Technology. Work performed: implementation of a proof of concept Hyperjacking attack on Intel platform.
- 2005–2008: Ph.D. co-advisor for Urko Zurutuza Ortega, Mondragon University, Spain. Thesis title: *Data Mining Approaches for Analysis of Worm Activity Towards Automatic Signature Generation*.
- 2005: External advisor for the Diploma Thesis of Milton Yates, ENST Bretagne, France. Thesis title: *The Router-based Billy Goat Project*.
- 2002–2003: External advisor for the Diploma Thesis of Candid Wüest, ETH Zürich, Switzerland. Thesis title: *Desktop Firewalls and Intrusion Detection*.

## Teaching experience

- May 2008: Guest lecture “Virtualization” (2 hours) at the Systems Security class in the Computer Science department at ETH Zürich.
- March 2005: Taught the lecture “Intrusion detection: Basic concepts and current research at IBM” (3 hours) at the Information Technology Security Spring School organized by the University of Lausanne.
- June 2003: Taught the class “Introduction to Computer Security” (40 hours) at the *Instituto Tecnológico de Estudios Superiores de Monterrey* in Monterrey, México.
- November 2000: Invited lecturer in the EE495 (*Information Extraction, Retrieval and Security*) course at Purdue University. Collaborated in the design of eight security-related lectures and taught two of them. Participated in the design of the class project.
- June 2000: Taught the class “Secure Shell: Achieving secure communication over insecure channels” at the 2000 CSI NetSec conference.
- April 1997: Taught the class “Protecting your computing system” at Schlumberger in Austin, TX.
- 1991–1996: Participated in the design and teaching of the syllabus, structure and contents of courses taught at the Supercomputing Department Internship Program at the National Autonomous University of Mexico. Courses were 10–40 hours long, and included the following topics:
- Introduction to Unix
  - Unix utilities
  - Unix security
  - Basic Unix administration
  - Advanced Unix administration
  - UNICOS system administration on Cray supercomputers
- 1995: Taught the *Structured Programming* class at the Engineering School of the National Autonomous University of Mexico. This was a one-semester first-year college class, covering primarily C language programming.

## Publications

- Editorial activities: 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.

Alfonso Valdes and Diego Zamboni, editors. *Recent Advances in Intrusion Detection: 8th International Symposium, RAID 2005, Seattle, WA, USA, September 7-9, 2005, Revised Papers (Lecture Notes in Computer Science)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006. ISBN 3540317783.

Deborah Frincke, Andreas Wespi, and Diego Zamboni. Guest editorial: From intrusion detection to self-protection. *Comput. Netw.*, 51(5):1233–1238, 2007. ISSN 1389-1286. doi: <http://dx.doi.org/10.1016/j.comnet.2006.10.004>. URL <http://www.sciencedirect.com/science/journal/13891286>.

Diego Zamboni, editor. *Software: Practice and Experience, Special issue on "Security Software"*, volume 33-5. John Wiley & Sons, April 2003. URL <http://www3.interscience.wiley.com/cgi-bin/issuetoc?ID=104087122>.

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 First ACM Workshop on AISec*, October 2008.

U. Zurutuza, R. Uribeetxeberria, M. Fernández, I. Vélez de Mendizabal, and D. Zamboni. Un marco inteligente para el análisis de tráfico generado por gusanos en Internet (An intelligent framework for analysis of worm-generated Internet traffic). In *Actas de la X Reunión Española sobre Criptología y Seguridad de la Información (X Spanish Meeting on Cryptology and Information Security)*, September 2008.

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/event/sruti07/tech/full\\_papers/zamboni/zamboni.pdf](http://www.usenix.org/event/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.

Florian Kerschbaum, Eugene H. Spafford, and Diego Zamboni. Using embedded sensors for detecting network attacks. In Deborah Frincke and Dimitris Gritzalis, editors, *Proceedings of the 1st ACM Workshop on Intrusion Detection Systems*. ACM SIGSAC, November 2000. URL <http://www.cerias.purdue.edu/homes/zamboni/pubs/wids2000.ps>. CERIAS TR 2000-25.

Eugene H. Spafford and Diego Zamboni. Intrusion detection using autonomous agents. *Computer Networks*, 34(4): 547–570, October 2000. URL [http://dx.doi.org/10.1016/S1389-1286\(00\)00136-5](http://dx.doi.org/10.1016/S1389-1286(00)00136-5).

Jai Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez, David Isacoff, Eugene Spafford, and Diego Zamboni. An architecture for intrusion detection using autonomous agents. In *Proceedings of the Fourteenth Annual Computer Security Applications Conference*, pages 13–24. IEEE Computer Society, December 1998. URL <http://zzamboni.org/diego/pubs/aafid-acsc98.pdf>.

Christoph L. Schuba, Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spafford, Aurobindo Sundaram, and Diego Zamboni. Analysis of a denial of service attack on TCP. In *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, pages 208–223. IEEE Computer Society, IEEE Computer Society Press, May 1997. URL <http://www.cerias.purdue.edu/homes/zamboni/pubs/synkill.ps>.

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://www.cerias.purdue.edu/homes/zamboni/pubs/SAINT.ps>.

Technical reports: James Riordan, Diego Zamboni, and Yann Duponchel. Billy Goat, an accurate worm-detection system. Research Report RZ3609, IBM Research, November 2005. URL <http://tinyurl.com/a5hmm>.

Diego Zamboni. Doing intrusion detection using embedded sensors— thesis proposal. CERIAS Technical Report 2000-21, CERIAS, Purdue University, West Lafayette, IN, October 2000. URL <http://www.cerias.purdue.edu/homes/zamboni/pubs/prelim.ps>.

Eugene Spafford and Diego Zamboni. Data collection mech-

anisms for intrusion detection systems. CERIAS Technical Report 2000-08, CERIAS, Purdue University, 1315 Recitation Building, West Lafayette, IN, June 2000. URL <http://www.cerias.purdue.edu/homes/zamboni/pubs/2000-08.ps>.

Jai Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez, Eugene Spafford, and Diego Zamboni. An architecture for intrusion detection using autonomous agents. Technical Report 98-05, COAST Laboratory, Purdue University, May 1998. URL <http://www.cerias.purdue.edu/homes/zamboni/pubs/tr9805.ps>.

Theses:

Diego Zamboni. *Using Internal Sensors for Computer Intrusion Detection*. PhD thesis, Purdue University, West Lafayette, IN, August 2001. URL <http://www.cerias.purdue.edu/homes/zamboni/docs/pubs/thesis-techreport.pdf>. CERIAS TR 2001-42.

Diego Zamboni. Proyecto UNAM/Cray de seguridad en el sistema operativo unix (*UNAM/Cray project for Unix System Security*). B.Sc. thesis, Universidad Nacional Autonoma de México, June 1995. URL <http://www.cerias.purdue.edu/homes/zamboni/docs/pubs/thesis-bs.pdf>. In Spanish.

Presentations at conferences and workshops:

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), October 2000. URL <http://www.cerias.purdue.edu/homes/zamboni/pubs/sensors-raid2000.ps>.

Diego Zamboni. Building a distributed intrusion detection system with perl. Presented at The Perl Conference 4.0, July 2000. URL <http://www.cerias.purdue.edu/homes/zamboni/pubs/tpc40.ps>.

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, October 1999.

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)*,

West Lafayette, IN, September 1999. Online proceedings, available at <http://www.raid-symposium.org/raid99/>.

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)*, Louvain-la-Neuve, Belgium, September 1998. Online proceedings, available at <http://www.raid-symposium.org/raid98/>.

Invited talks and articles:

Martim Carbone, Diego Zamboni, and Wenke Lee. Taming virtualization. *IEEE Security and Privacy*, 6(1):65–67, 2008. ISSN 1540-7993. doi: <http://dx.doi.org/10.1109/MSP.2008.24>. URL <http://tinyurl.com/6zccpk>.

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, November 2006.

Diego Zamboni. Intrusion what? from detection to prevention and beyond. Talk at the Zurich Information Security Center Information Security Colloquium., December 2005.

James Riordan, Andreas Wespi, and Diego Zamboni. How to hook worms. *IEEE Spectrum*, May 2005. URL <http://www.spectrum.ieee.org/may05/1124>.

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.

Diego Zamboni. AAFID: Autonomous agents for intrusion detection. Invited talk, presented at the 1999 Indiana Client Server and Internet Conference, September 1999.

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, November 1998.

Diego Zamboni. Unix host security tools. Invited talk, presented at the Cellular Telecommunications Industry Associa-

tion (CTIA) Network Vulnerability Workshop, January 1998.

Patents (partial): James Riordan, Diego Zamboni, Yann Duponchel, and Ruediger Rissmann. Network attack detection. Patent WO2006100613, IBM, September 2006.

Morton Swimmer, Andreas Wespi, and Diego Zamboni. Preventing attacks in a data processing system. U.S. Patent 20040255163, IBM, December 2004.

C. Schuba, I. Krsul, D. Zamboni, E. Spafford, A. Sundaram, and M. Kuhn. Network protection for denial of service attacks. U.S. Patent 6725378, Purdue Research Foundation, April 2004.

Daniela Bourges-Waldegg, James Riordan, Diego Zamboni, and Dominique Alessandri. Detection and control of peer-to-peer software in an enterprise network. Patent application (pending), IBM, 2005.

James Riordan, Diego Zamboni, Yann Duponchel, and Ruediger Rissmann. Gentle VLAN isolation. Patent application (pending), IBM, 2005.

### **Awards and honors**

July 2001: Received the first “Josef Raviv Memorial Postdoctoral Fellowship” awarded by IBM to “a recent Ph.D. who shows exceptional promise for a research career in computer science”.

April 2001: Inducted as a member of the Purdue University Chapter of Phi Beta Delta, the honor society dedicated to recognizing scholarly achievement in international education.

September 2000: Received the “2000 UPE Microsoft Scholarship Award,” awarded by Upsilon Pi Epsilon, the Computer Sciences honor society, on the basis of academic record, extra-curricular activities, and advisor recommendation.

April 1998: Inducted as a member to the Purdue University chapter of Upsilon Pi Epsilon.

May 1996: Received the Fulbright Scholarship for pursuing Ph.D. studies at Purdue University.

1993–1995: Member of the Outstanding Students program at the Engineering School in the National Autonomous University of Mexico, designed to recognize students on the basis of grade point average.

## Other professional activities

- 2007–2008: Member of the Steering Committee for the International Symposium on Recent Advances in Intrusion Detection (RAID).
- 2008: Program chair for the SIG SIDAR Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), held in Paris, France.
- 2007: Member of the Program Committee for the IEEE Security and Privacy Symposium.
- 2006: Program chair for the International Symposium on Recent Advances in Intrusion Detection (RAID), held in Hamburg, Germany.
- 2003–2007: Member of the Program Committee for the Annual Computer Security Applications Conference (ACSAC).
- 2001–2005: Member of the Program Committee for the International Symposium on Recent Advances in Intrusion Detection (RAID).
- 2000: Founded Purdue.pm, the Purdue Perl Users Group, as a chapter of the Perl Mongers organization.
- 1999–2000: President of the Purdue University Chapter of Upsilon Pi Epsilon.
- 1998–1999: Secretary of the Purdue University Chapter of Upsilon Pi Epsilon.
- 1994–2000: Member of the Program Committee for the International Computer Security Day conference, organized yearly at the National Autonomous University of Mexico.
- 1994, 1995: Organizer of the International Computer Security Day conference.

## Software development

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

Other experience: XML and related technologies, network programming, database programming (SQL), kernel programming (OpenBSD and Linux), HTML.

(only major projects are mentioned below)

**Publicly-available software projects:**

- 2005-2008: **CopperExport.** An export plugin for iPhoto.
- 1999–2000: **mailer.** An email alias and list manager, for use at CERIAS (Center for Education and Research in Information Assurance and Security) in Purdue University.
- 1997–1999: **AAFID<sub>2</sub> prototype.** A distributed intrusion detection system, based on the AAFID intrusion detection architecture developed at CERIAS, in Purdue University.
- Other software projects (not publicly available):**
- 2005–2007: **Pilatus.** A system installer that allows arbitrary system installation and configurations, allowing both for 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.
- 2005–2007: **SOC in a Box.** 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.
- 2002–2007: **Billy Goat.** 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.
- 2000–2001: **Embedded Sensors Project (ESP).** 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.

### **Unix system administration experience**

Linux (multiple distributions, including Gentoo, RedHat, Ubuntu, and Debian), OpenBSD, FreeBSD, MacOS X, Solaris, Cray Unix, Irix.

### **Spoken languages**

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

**Professional memberships**

Professional societies: ACM, IEEE Computer Society.

Honorary scientific societies: Sigma Xi, Upsilon Pi Epsilon, Phi Beta Delta.

**References**

Available by request.