Curriculum Vitae — Diego Zamboni

November 2003

Personal information

Diego Zamboni
Etzelstrasse 33,
CH-8820 Wädenswil,
Switzerland

Daytime phone: +41-1-724-8687
Personal phone: +41-1-(0)76-370-7969
Email: `diego@zzamboni.org`
`http://www.cerias.purdue.edu/homes/zamboni/`

Research interests and activities

General areas of interest:

Intrusion detection, operating systems security, network security.

Sample research projects at IBM:

Billy Goat: An active worm-detection tool.

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

Living laboratory: Environment for deployment and testing of intrusion detection systems in a real production network.

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.

Other projects: Using autonomous agents for intrusion detection.

This document can be found online at `http://www.cerias.purdue.edu/homes/zamboni/vita/`

- Design and documentation of an architecture 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 a 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, as part of the GSAL (Global Security Analysis Laboratory) group.

June 1999: Temporary work at Internet Security Advisory Group

- Studied security problems from different sources and wrote advisories for distribution to customers.

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 (CSA).
- 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 a static 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.

Teaching experience

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.

September 2000: Invited lecturer in the CS590T (*Software tools*) course at Purdue University. Taught one lecture about Perl programming.

June 2000: Taught the class “Secure Shell: Achieving secure communication over insecure channels” at the 2000 CSI NetSec conference.

September 1999: Taught the informal short class “Using CVS” at the Computer Sciences department at Purdue University.

June 1999: Taught the class “Installing and using AAFID” at the 1999 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.

Awards and honors

July 2001: Received the first “Josef Raviv Memorial Postdoctoral Fellowship” awarded by IBM.

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.

Service activities

2003: Member of the Program Committee for the Annual Computer Security Applications Co
in 2003.

2001–2003: Member of the Program Committee for the International Symposium on Recent Advan
in 2001–2003.

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

This list includes only major publicly-available projects.

1999–2000: Development of **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: Development of the AAFID$_2$ prototype, based on the AAFID intrusion detection architecture developed at CERIAS, in Purdue University.

Publications

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.` CERIAS TR 2001-42.

Diego Zamboni. Proyecto UNAM/Cray de seguridad en el sistema operativo unix. 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.

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

Refereed papers: 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://www.elsevier.nl/gej-ng/10/15/22/49/30/25/article.pdf`.

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://www.cerias.purdue.edu/homes/zamboni/pubs/aafid-acsac98.ps`.

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`.

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/Prog_RAID98/Table_of_content.html`.

Technical reports:

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 mechanisms 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`.

Invited talks: 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 Association (CTIA) Network Vulnerability Workshop, January 1998.

Patents: C. Schuba, I. Krsul, D. Zamboni, E. Spafford, A. Sundaram, and M. Kuhn. *Network Protection for Denial of Service Attacks*. Patent filed in 1999.

Other publications: Diego Zamboni. *Notas de Utilerías de Unix (Unix utilities course notes)*. Academic Computing Services Center, National Autonomous University of Mexico, March 1993.