Curriculum Vitæ— Diego Zamboni

September 27, 2018

Personal information

Full name: Diego Martín Zamboni

diego@zzamboni.org
http://zzamboni.org/
http://mx.linkedin.com/in/zzamboni
http://twitter.com/zzamboni

Introduction I am a senior computer scientist, IT architect, team and project leader with more than 25 years of experience, specialized in the areas of Cloud Computing, Computer Security, Self-healing Systems and Configuration management. 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 self-motivated and have excellent communication skills in 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, software architecture, practical technical knowledge, team leadership and customer-facing experience.

Areas of interest and expertise

Leadership: Technical team and project leadership. I am experienced in the SAFe methodology and processes, and have the SAFe Product Owner certification.

Systems architecture and development:
Unix/Linux systems engineering and administration, systems health management and monitoring, cloud computing environments and platforms (OpenStack, Amazon EC2, Cloud Foundry) and software development experience (C, Python, Ruby, Perl, Java).

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.

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 Ansible, Puppet and Chef. I am very interested in the area of self-healing systems and architectures.

Other skills: Excellent written and spoken communication skills, customer-facing experience, project and product management experience.

Work experience

March 2018 to date: Squad Lead and Product Owner for Health and State Management (HSM) in the One

This document can be found online at http://zzamboni.org/vita.html.

Cloud Enabling project at Swisscom.

As part of the One Cloud initiative, the HSM team has an expanded scope to design, implement and manage Health Management and Monitoring components for all the IT Clouds platforms, including Enterprise Service Cloud, Application Cloud, Enterprise Cloud 1.x, Enterprise Cloud for SAP applications (EC4SAP), Marketplace Services, and Cloud Connectivity Management. I work with Architects and Product Managers to define the necessary technical features, and lead the team which implements, deploys and operates these components.

Main technologies involved: VMware vSphere (ESX, vCenter, NSX), VMware vRealize Operations Manager and Log Insight, Ansible (configuration management), OpsGenie (alert management).

January 2017–April 2018: Squad Lead and Product Owner for Health and State Management (HSM) in the Enterprise Service Cloud project at Swisscom.

I worked with Product Management to define the technical features necessary for Health Management and Monitoring in the Enterprise Service Cloud project, and lead the team which implements, deploys and operates these components.

March 2016–January 2017: Head of Health & State Management at Swisscom.

I lead a team of people working on multiple projects related to Health Management and monitoring/logging of the Swisscom cloud offerings, including Application Cloud (CloudFoundry-based PaaS offering), Enterprise Cloud 1.x and Enterprise Service Cloud (IaaS offerings) .

June–December 2016: Lead of Squad LEMM in the Enterprise Cloud project at at Swisscom.

I lead the architecture and delivery of the Logging, Event Management and Monitoring framework (LEMM) of the Swisscom Enterprise Cloud, which handles all the processing, analysis and monitoring of the logging messages, health events, and other relevant infrastructure events .

August 2015–March 2016: Cloud Architect and Orchard Project Lead at Swisscom.

I continued leading the *Orchard* project through its implementation, release and further improvements and development.

August 2014–July 2015: Senior Platform Architect (consultant) at Swisscom Cloud Lab.

I designed the architecture for the *Orchard* health-management and self-healing components of Swisscom's "Application Cloud" Platform as a Service Offering. This system performs self-monitoring and self-healing of the infrastructure and platform components. In addition to designing the architecture, I worked on its implementation together with a team of three people managed by me.

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).

July 2012–July 2014: *Director de Investigación y Capacitación* (Head of Research and Training) at Boundless Innovation and Technology.

I advised and coordinated teams working on teaching- and security-related products, consulting and services.

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 (including with technologies like AWS EC2, VMware, Docker and OpenStack). I participated in the coding for both the Design Center and some of the integrations. I am familiar with the internals of the CFEngine C source code base.

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 gave talks, wrote articles and blog posts, taught classes, and in general spread the word about CFEngine. I also worked on developing and implementing the strategy for CFEngine in security. CFEngine is a configuration management system, but it can be a fantastic security tool, useful for preventing, detecting and fixing security problems, as well as aiding in achieving compliance.

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. I initiated, advised and managed security-related projects. I handled communication and coordination between technical teams involved in security initiatives. I was 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 my research.

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: Founder and 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). 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: System Administrator at supercomputing center for UNAM's Cray Supercomputer; National Autonomous University of Mexico (UNAM).

- Part of the system administration team.
- 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: 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.

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).

Publications

Books: Diego Zamboni. *Learning CFEngine 3.* O'Reilly Media, Inc., March 2012. ISBN 9781449312206. URL `http://cf-learn.info/`. Self-published since Aug. 2017.

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.

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. *Computer Networks*, 51(5):1233–1238, 2007. ISSN 1389-1286. URL `http://dx.doi.org/10.1016/j.comnet.2006.10.004`.

Diego Zamboni, editor. Software: Practice and Experience*, Special issue on "Security Software"*, volume 33-5. John Wiley & Sons, April 2003. URL `http://onlinelibrary.wiley.com/doi/10.1002/spe.v33:5/issuetoc`.

Presentations at conferences and workshops: 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 `http://sched.co/6aQ2`.

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`.

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, November 2013. URL `https://www.usenix.org/conference/lisa13/leveraging-memory-key-value-stores-large-scale-operations`.

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://homes.cerias.purdue.edu/~zamboni/pubs/sensors-raid2000.pdf`.

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

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/.

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.

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.

Urko Zurutuza, Roberto Uribetxeberria, and Diego Zamboni. Análisis 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)*, pages 87–94, September 2007.

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/.

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 https://www.cerias.purdue.edu/apps/reports_and_papers/view/1641/. 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.

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-acsac98.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 *Pro-*

ceedings of the 1997 IEEE Symposium on Security and Privacy, pages 208–223. IEEE Computer Society, IEEE Computer Society Press, May 1997. URL http://homes.cerias.purdue.edu/~zamboni/pubs/synkill.pdf.

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://homes.cerias.purdue.edu/~zamboni/pubs/SAINT.pdf.

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/bgtechreport.

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://homes.cerias.purdue.edu/~zamboni/pubs/prelim.pdf.

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://homes.cerias.purdue.edu/~zamboni/pubs/2000-08.pdf.

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://homes.cerias.purdue.edu/~zamboni/pubs/tr9805.pdf.

Theses:

Diego Zamboni. *Using Internal Sensors for Computer Intrusion Detection*. PhD thesis, Purdue University, West Lafayette, IN, August 2001. URL http://homes.cerias.purdue.edu/~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://homes.cerias.purdue.edu/~zamboni/docs/pubs/thesis-bs.pdf. In Spanish.

Invited talks and articles:

Mark Burgess and Diego Zamboni. CFEngine's decentralized approach to configuration management. *InfoQ*, June 2014. URL http://www.infoq.com/articles/cfengine-view-on-it-automation.

Diego Zamboni. Security in the third wave of it engineering. Keynote talk, presented at the 2011 Computer Security Congress in Mexico City, November 2011. URL http://blog.zzamboni.org/security-in-the-third-wave-of-it-engineering.

Martim Carbone, Diego Zamboni, and Wenke Lee. Taming virtualization. *IEEE Security and Privacy*, 6(1):65–67, 2008. ISSN 1540-7993. URL http://www.computer.org/portal/web/csdl/doi/10.1109/MSP.2008.24.

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 Association (CTIA) Network Vulnerability Workshop, January 1998.

Patents (sample): 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.

Martim Carbone, Bernhard Jansen, Harigovind Ramasamy, Matthias Schunter, Axel Tanner, and Diego Zamboni. Protection and security provisioning using on-the-fly virtualization. Patent application (pending), IBM, 2008.

Certifications *SAFe® 4 Certified Product Owner/Product Manager*, July 31st, 2017.

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.

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 (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, 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.

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

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), Go, Clojure.

Environments: Unix/Linux, OpenStack, Amazon EC2, Mac OS X.

Other experience: REST APIs, Riemann (event stream processing), XML and related technologies, network programming, database programming (SQL), kernel programming (OpenBSD and Linux), HTML.

Major 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$_2$ 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 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.

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.

Other technology experience

Unix systems: Linux (multiple distributions, including Gentoo, RedHat, Fedora Linux, Ubuntu, and Debian) , OpenBSD, FreeBSD, MacOS X, MacOS X Server, Solaris.

In addition, I have experience in creation of packages and customized distributions based on Gentoo, RedHat/Fedora and Ubuntu.

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

Virtualization, container and cloud platforms: OpenStack, Amazon EC2, Docker, VMware (ESX, vSphere, vRealize Operations Manager, vRealize Log Insight).

Student advising

2009: Internship advisor for Daniele Sgandurra, University of Pisa, Italy. Project: design and implementation of process injection using virtual machine introspection.

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

2011–2013: Multiple instances of teaching the CFEngine one-day training class (8 hour class) at multiple venues throughout the world.

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, Mexico.

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

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: Purdue University chapter of Upsilon Pi Epsilon.

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

Other professional activities

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 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), with the topic of Security in Virtualized Environments and Cloud Computing .

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 9th 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.

Spoken languages

Spanish (native), English (near-native spoken and written fluency), German (medium, B2-C1 level), French (basic).

Professional memberships

Professional societies: ACM.

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

References

Available by request.