Diego **Zamboni**

Publications

Books

[1] Diego Zamboni. *Publishing with Emacs, Org-mode and Leanpub*. Leanpub, June 2020.

[2] Diego Zamboni. *Literate Configuration*. Leanpub, November 2019.

[3] Diego Zamboni. *Utilerías de Unix (Unix utilities course notes)*. Leanpub, August 2019.

[4] Diego Zamboni. *Learning Hammerspoon*. Leanpub, October 2018.

[5] Diego Zamboni. *Learning CFEngine*. O'Reilly Media, Inc. 2012–2017, afterwards self-published, 2012.

Editorial Activities

[6] Diego Zamboni. Computers & Security Journal. Member of the Editorial Board. 2011.

[7] Deborah Frincke, Andreas Wespi, and Diego Zamboni, editors. *From Intrusion Detection to Self-Protection*. Volume 51. Computer Networks Issue 5. New York, NY, USA: Elsevier North-Holland, Inc., April 2007.

[8] Diego Zamboni and Christopher Kruegel, editors. *Proceedings of the Recent Advances in Intrusion Detection (RAID): 9th International Symposium*. Lecture Notes in Computer Science. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2006.

[9] Alfonso Valdes and Diego Zamboni, editors. *Proceedings of the Recent Advances in Intrusion Detection (RAID): 8th International Symposium*. Lecture Notes in Computer Science. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2005.

[10] Diego Zamboni, editor. *Special issue on Security Software*. Volume 33. Software: Practice and Experience 5. John Wiley & Sons, April 2003.

Theses

[11] Diego Zamboni. "Using Internal Sensors for Computer Intrusion Detection". CERIAS TR 2001-42. PhD thesis, West Lafayette, IN: Purdue University, August 2001.

[12] Diego Zamboni. "Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix (emph{UNAM/Cray project for Unix System Security})". Spanish. B.Sc. Thesis, Universidad Nacional Autonoma de México, June 1995.

Refereed Papers

[13] Mihai Christodorescu, Reiner Sailer, Douglas Lee Schales, Daniele Sgandurra, and Diego Zamboni. "Cloud Security is Not (Just) Virtualization Security: A Short Paper". In: *Proceedings of the 2009 ACM Workshop on Cloud Computing Security*. Chicago, Illinois, USA: ACM, 2009. pages 97–102.

[14] U. Zurutuza, R. Uribeetxeberria, M. Fernández, I. Vélez 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)". Spanish. In: *Actas de la X Reunión Española sobre Criptología y Seguridad de la Información (X Spanish Meeting on Cryptology and Information Security)*. September 2008.

[15] 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)*. Alexandria, Virginia, USA: Association for Computing Machinery, October 2008. pages 61–70.

[16] 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.

[17] 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)*. September 2007. pages 87–94.

[18] 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.

[19] Florian Kerschbaum, Eugene H. Spafford, and Diego Zamboni. "Using internal sensors and embedded detectors for intrusion detection". In: *Journal of Computer Security* 10.1,2 (2002), pages 23–70.

[20] Florian Kerschbaum, Eugene H. Spafford, and Diego Zamboni. "Using embedded sensors for detecting network attacks". In: *Proceedings of the 1st ACM Workshop on Intrusion Detection Systems*. Edited by Deborah Frincke and Dimitris Gritzalis. CERIAS TR 2000-25. ACM SIGSAC, November 2000.

[21] Eugene H. Spafford and Diego Zamboni. "Intrusion Detection using Autonomous Agents". In: *Computer Networks* 34.4 (October 2000), pages 547–570.

[22] 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*. IEEE Computer Society, December 1998. pages 13–24.

[23] 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*. Awarded the 2020 IEEE Security & Privacy Test of Time Award. IEEE Computer Society, IEEE Computer Society Press, May 1997. pages 208–223.

[24] Diego Zamboni. “SAINT —A Security Analysis Integration Tool”. In: *Proceedings of the 1996 Systems Administration, Networking and Security Conference*. Washington, D.C., May 1996.

Technical Reports

[25] James Riordan, Diego Zamboni, and Yann Duponchel. *Billy Goat, an Accurate Worm-Detection System*. technical report RZ 3609. IBM Research, November 2005.

[26] Eugene Spafford and Diego Zamboni. *Data Collection mechanisms for intrusion detection systems*. technical report 2000-08. 1315 Recitation Building, West Lafayette, IN: CERIAS, Purdue University, June 2000.

[27] Diego Zamboni. *Doing intrusion detection using embedded sensors— Thesis proposal*. technical report 2000-21. West Lafayette, IN: CERIAS, Purdue University, October 2000.

[28] 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.

Presentations at Conferences and Workshops

[29] 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. href{https://www.youtube.com/watch?v=Wr4E–kr_KE} Recording. May 2016.

[30] 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.

[31] 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.

[32] 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.

[33] Diego Zamboni. Building a Distributed Intrusion Detection System with Perl. Presented at The Perl Conference 4.0. Monterey, CA, July 2000.

[34] 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.

[35] 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.

Invited Talks and Articles

[36] Mark Burgess and Diego Zamboni. “CFEngine’s Decentralized Approach to Configuration Management”. In: *InfoQ* (June 2014).

[37] Diego Zamboni. Security in the Third Wave of IT Engineering. Keynote talk, presented at the 2011 Computer Security Congress in Mexico City. November 2011.

[38] Martim Carbone, Diego Zamboni, and Wenke Lee. “Taming Virtualization”. In: *IEEE Security and Privacy* 6.1 (2008), pages 65–67.

[39] 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.

[40] James Riordan, Andreas Wespi, and Diego Zamboni. “How to Hook Worms”. In: *IEEE Spectrum* (May 2005).

[41] Diego Zamboni. Intrusion what? From detection to prevention and beyond. Talk at the Zurich Information Security Center Information Security Colloquium. December 2005.

[42] James Riordan and Diego Zamboni. “Billy Goat Detects Worms and Viruses”. In: *ERCIM News* (January 2004).

[43] Diego Zamboni. emph{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.

[44] Diego Zamboni. “emph{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 emph{Día Internacional de la Seguridad en Cómputo} (International Computer Security Day) conference*. Mexico City, Mexico, October 1999.

[45] Diego Zamboni. “AAFID: emph{Detección de Intrusos usando Agentes Autónomos} (Intrusion Detection using Autonomous Agents)”. In: *Proceedings of the 1998 emph{Día Internacional de la Seguridad en Cómputo} (International Computer Security Day) conference*. Mexico City, Mexico, November 1998.

Patents

[46] Martim Carbone, Bernhard Jansen, Harigovind Ramasamy, Matthias Schunter, Axel Tanner, and Diego Zamboni. “Hardware Emulation Using On-the-fly Virtualization”. Granted Patent US 9250942 B2 (United States). 2 February 2016.

[47] Bernhard Jansen, Matthias Schunter, Axel Tanner, and Diego Zamboni. “Secure User Interaction Using Virtualization”. Granted Patent US 8516564 B2 (United States). 20 August 2013.

[48] Yann Duponchel, James Riordan, Ruediger Rissmann, and Diego Zamboni. “Methods For Operating Virtual Networks, Data Network System, Computer Program And Computer Program Product”. Granted Patent JP 4886788 B2 (Japan). 29 February 2012.

[49] James Riordan, Yann Duponchel, Ruediger Rissmann, and Diego Zamboni. “Network Attack Detection”. Patent Application US 2012/0096548 A1 (United States). 19 April 2012.

[50] Diego Zamboni, Dominique Alessandri, Daniela Bourges-Waldegg, and James Riordan. “Detection And Control Of Peer-to-peer Communication”. Patent Family of US 8219679 B2 (United States, others). 10 July 2012.

[51] Diego Zamboni, Alessandri Dominique, Daniela Bourges-Waldegg, and James Riordan. “Detection And Control Of Peer-to-peer Communication”. Granted Patent CN 101390369 B (China). 14 November 2012.

[52] Yann Duponchel, James Riordan, Ruediger Rissmann, and Diego Zamboni. “Methods For Operating Virtual Networks, Data Network System, Computer Program And Computer Program Product”. Patent Family of US 7908350 B2 (United States, others). 15 March 2011.

[53] James Riordan, Ruediger Rissmann, and Diego Zamboni. “IP Network Management Based On Automatically Acquired Network Entity Status Information”. Patent Family of US 8055751 B2 (United States, others). 8 November 2011.

[54] Ruediger Rissmann, Yann Duponchel, Diego Zamboni, and James Riordan. “Network Attack Detection”. Granted Patent JP 4753264 B2 (Japan). 24 August 2011.

[55] Ruediger Rissmann, Yann Duponchel, Diego Zamboni, and James Riordan. “Network Attack Detection”. Granted Patent KR 101090815 B1 (Republic of Korea). 8 December 2011.

[56] Diego Zamboni, Alessandri Dominique, Daniela Bourges-Waldegg, and James Riordan. “Detection And Control Of Peer-to-peer Communication”. Granted Patent JP 4829982 B2 (Japan). 7 December 2011.

[57] Yann Duponchel, James Riordan, Ruediger Rissmann, and Diego Zamboni. “Method For Operating Several Virtual Networks”. Patent Family of EP 1969777 B1 (European Patent Office, others). 27 January 2010.

[58] Yann Duponchel, James Riordan, Ruediger Rissmann, and Diego Zamboni. “Methods For Operating Virtual Networks, Data Network System, Computer Program And Computer Program Product”. Granted Patent KR 100998418 B1 (Republic of Korea). 3 December 2010.

[59] Yann Duponchel, James Riordan, Ruediger Rissmann, and Diego Zamboni. “Verfahren Zum Betrieb Von Mehreren Virtuellen Netzwerken”. Granted Patent DE 602006012095 D1 (Germany). 18 March 2010.

[60] Yann Duponchel, James Riordan, Ruediger Rissmann, and Diego Zamboni. “Verfahren Zum Betrieb Von Mehreren Virtuellen Netzwerken”. Granted Patent AT 456890 T (Austria). 15 February 2010.

[61] Ruediger Rissmann, Yann Duponchel, Diego Zamboni, and James Riordan. “Erkennung Von Netzwerkangriffen”. Granted Patent AT 485552 T (Austria). 15 November 2010.

[62] Ruediger Rissmann, Yann Duponchel, Diego Zamboni, and James Riordan. “Erkennung Von Netzwerkangriffen”. Granted Patent DE 602006017668 D1 (Germany). 2 December 2010.

[63] Ruediger Rissmann, Yann Duponchel, Diego Zamboni, and James Riordan. “Network Attack Detection”. Patent Family of EP 1866725 B1 (European Patent Office, others). 20 October 2010.

[64] Diego Zamboni, Yann Duponchel, James Riordan, and Ruediger Rissmann. “Methods For Operating Virtual Networks, Equipment, Data Network System”. Granted Patent CN 101326771 B (China). 15 September 2010.

[65] Ruediger Rissmann and Yann Duponchel. “Network Attack Detection Method And Device”. Granted Patent CN 100561492 C (China). 18 November 2009.

[66] Morton Swimmer, Andreas Wespi, and Diego Zamboni. “Preventing Attacks In A Data Processing System”. Granted Patent US 7555777 B2 (United States). 30 June 2009.

[67] Christoph Schuba, Ivan Krsul, Diego Zamboni, Eugene Spafford, Aurobindo Sundaram, and Markus Kuhn. “Network Protection For Denial Of Service Attacks”. Granted Patent US 6725378 B1 (United States). 20 April 2004.