Diego Zamboni

Publications, Talks and Intellectual Property

Books

[1] Diego Zamboni. *Publishing with Emacs, Org-mode and Leanpub*. Leanpub, June 2020. URL: https://leanpub.com/emacs-org-leanpub.

[2] Diego Zamboni. *Literate Configuration*. Leanpub, Nov. 2019. URL: https://leanpub.com/lit-config.

[3] Diego Zamboni. *Utilerías de Unix (Unix utilities course notes)*. Leanpub, Aug. 2019. URL: https://leanpub.com/utileras-unix.

[4] Diego Zamboni. *Learning Hammerspoon*. Leanpub, Oct. 2018. URL: https://leanpub.com/learning-hammerspoon.

[5] Diego Zamboni. *Learning CFEngine*. O'Reilly Media, Inc. 2012–2017, afterwards self-published, 2012. ISBN: 9781449312206. URL: http://cf-learn.info/.

Editorial Activities

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

[7] "Computer Networks". In: 51.5 (Apr. 2007): *From Intrusion Detection to Self-Protection*. Ed. by Deborah Frincke, Andreas Wespi, and Diego Zamboni. ISSN: 1389-1286. DOI: 10.1016/j.comnet.2006.10.004.

[8] Diego Zamboni and Christopher Kruegel, eds. *Proceedings of the Recent Advances in Intrusion Detection (RAID): 9th International Symposium*. Recent Advances in Intrusion Detection (RAID): 9th International Symposium (Hamburg, Germany, Sept. 20–22, 2006). Lecture Notes in Computer Science. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2006. ISBN: 354039723X.

[9] Alfonso Valdes and Diego Zamboni, eds. *Proceedings of the Recent Advances in Intrusion Detection (RAID): 8th International Symposium*. Recent Advances in Intrusion Detection (RAID): 8th International Symposium (Seattle, WA, U.S.A. Sept. 7–9, 2005). Lecture Notes in Computer Science. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2005. ISBN: 3540317783.

[10] In: *Software: Practice and Experience* 33.5 (Apr. 2003): *Special issue on "Security Software"*. Ed. by Diego Zamboni. URL: http://onlinelibrary.wiley.com/doi/10.1002/spe.v33:5/issuetoc.

Theses

[11] Diego Zamboni. "Using Internal Sensors for Computer Intrusion Detection". CERIAS TR 2001-42. PhD thesis. West Lafayette, IN: Purdue University, Aug. 2001. URL: https://www.cerias.purdue.edu/apps/reports_and_papers/view/1800.

[12] Diego Zamboni. "Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix (*UNAM/Cray project for Unix System Security*)". Spanish. B.Sc. Thesis. Universidad Nacional Autonoma de México, June 1995. URL: https://zzamboni.org/files/theses/zamboni-bachelors-thesis.pdf.

Refereed Papers

[13] Mihai Christodorescu et al. "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, pp. 97–102. ISBN: 978-1-60558-784-4. DOI: 10.1145/1655008.1655022.

[14] U. Zurutuza et al. "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)*. Sept. 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, Oct. 2008, pp. 61–70. ISBN: 978-1-60558-291-7. DOI: 10.1145/1456377.1456394.

[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. URL: http://www.usenix.org/events/sruti07/tech/full_papers/zamboni/zamboni.pdf.

[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)*. Sept. 2007, pp. 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), pp. 23–70. URL: https://www.researchgate.net/publication/220065478_Using_Internal_Sensors_and_Embedded_Detectors_for_Intrusion_Detection.

[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*. Ed. by Deborah Frincke and Dimitris Gritzalis. CERIAS TR 2000-25. ACM SIGSAC. Nov. 2000. URL: https://www.cerias.purdue.edu/apps/reports_and_papers/view/1641/.

[21] Eugene H. Spafford and Diego Zamboni. “Intrusion Detection using Autonomous Agents”. In: *Computer Networks* 34.4 (Oct. 2000), pp. 547–570. URL: http://dx.doi.org/10.1016/S1389-1286(00)00136-5.

[22] Jai Sundar Balasubramaniyan et al. “An Architecture for Intrusion Detection using Autonomous Agents”. In: *Proceedings of the Fourteenth Annual Computer Security Applications Conference*. IEEE Computer Society, Dec. 1998, pp. 13–24. URL: http://zzamboni.org/files/pubs/aafid-acsac98.pdf.

[23] Christoph L. Schuba et al. “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, pp. 208–223. URL: https://www.cerias.purdue.edu/apps/reports_and_papers/view/605.

[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. URL: http://zzamboni.org/files/pubs/SAINT.pdf.

Tech Reports

[25] James Riordan, Diego Zamboni, and Yann Duponchel. *Billy Goat, an Accurate Worm-Detection System*. Research Report RZ 3609. IBM Research, Nov. 2005. URL: https://dominoweb.draco.res.ibm.com/reports/rz3609_revised.pdf.

[26] Eugene Spafford and Diego Zamboni. *Data Collection mechanisms for intrusion detection systems*. CERIAS Technical Report 2000-08. 1315 Recitation Building, West Lafayette, IN: CERIAS, Purdue University, June 2000. URL: https://www.cerias.purdue.edu/apps/reports_and_papers/view/1842.

[27] Diego Zamboni. *Doing intrusion detection using embedded sensors— Thesis proposal*. CERIAS Technical Report 2000-21. West Lafayette, IN: CERIAS, Purdue University, Oct. 2000. URL: https://www.cerias.purdue.edu/apps/reports_and_papers/view/581.

[28] Jai Sundar Balasubramaniyan et al. *An Architecture for Intrusion Detection using Autonomous Agents*. Technical Report 98-05. COAST Laboratory, Purdue University, May 1998. URL: https://www.cerias.purdue.edu/apps/reports_and_papers/view/65.

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. Recording. May 2016. URL: http://sched.co/6aQ2.

[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. URL: https://www.usenix.org/conference/ucms14/summit-program/presentation/zamboni.

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

[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). Oct. 2000. URL: http://zzamboni.org/files/pubs/sensors-raid2000.pdf.

[33] Diego Zamboni. *Building a Distributed Intrusion Detection System with Perl*. Presented at The Perl Conference 4.0. Monterey, CA, July 2000. URL: http://zzamboni.org/files/pubs/tpc40.pdf.

[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, Sept. 1999. URL: https://www.cerias.purdue.edu/apps/reports_and_papers/view/3487.

[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, Sept. 1998.

Invited Talks and Articles

[36] Mark Burgess and Diego Zamboni. “CFEngine’s Decentralized Approach to Configuration Management”. In: *InfoQ* (June 2014). URL: http://www.infoq.com/articles/cfengine-view-on-it-automation.

[37] Diego Zamboni. *Security in the Third Wave of IT Engineering*. Keynote talk, presented at the 2011 Computer Security Congress in Mexico City. Nov. 2011. URL: https://zzamboni.org/post/security-in-the-third-wave-of-it-engineering/.

[38] Martim Carbone, Diego Zamboni, and Wenke Lee. “Taming Virtualization”. In: *IEEE Security and Privacy* 6.1 (2008), pp. 65–67. ISSN: 1540-7993. URL: https://ieeexplore.ieee.org/document/4446700.

[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. Nov. 2006.

[40] James Riordan, Andreas Wespi, and Diego Zamboni. “How to Hook Worms”. In: *IEEE Spectrum* (May 2005). URL: https://spectrum.ieee.org/computing/networks/how-to-hook-worms.

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

[42] James Riordan and Diego Zamboni. “Billy Goat Detects Worms and Viruses”. In: *ERCIM News* 56 (Jan. 2004). URL: http://www.ercim.org/publication/Ercim_News/enw56/riordan.html.

[43] 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.

[44] 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, Oct. 1999.

[45] 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, Nov. 1998.

Patents

[46] Martim Carbone et al. *Hardware Emulation Using On-the-fly Virtualization*. Granted Patent US 9250942 B2. United States, Feb. 2, 2016. URL: https://lens.org/107-038-681-631-856.

[47] Bernhard Jansen et al. *Secure User Interaction Using Virtualization*. Granted Patent US 8516564 B2. United States, Aug. 20, 2013. URL: https://lens.org/012-709-360-909-626.

[48] Yann Duponchel et al. *Methods For Operating Virtual Networks, Data Network System, Computer Program And Computer Program Product*. Granted Patent JP 4886788 B2. Japan, Feb. 29, 2012. URL: https://lens.org/029-398-797-666-948.

[49] James Riordan et al. *Network Attack Detection*. Patent Application US 2012/0096548 A1. United States, Apr. 19, 2012. URL: https://lens.org/025-823-888-291-212.

[50] Diego Zamboni et al. *Detection And Control Of Peer-to-peer Communication*. Patent Family of US 8219679 B2. United States, others, July 10, 2012. URL: https://lens.org/151-595-773-205-878.

[51] Diego Zamboni et al. *Detection And Control Of Peer-to-peer Communication*. Granted Patent CN 101390369 B. China, Nov. 14, 2012. URL: https://lens.org/113-267-068-964-958.

[52] Yann Duponchel et al. *Methods For Operating Virtual Networks, Data Network System, Computer Program And Computer Program Product*. Patent Family of US 7908350 B2. United States, others, Mar. 15, 2011. URL: https://lens.org/080-322-567-493-840.

[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, Nov. 8, 2011. URL: https://lens.org/065-534-634-366-763.

[54] Ruediger Rissmann et al. *Network Attack Detection*. Granted Patent JP 4753264 B2. Japan, Aug. 24, 2011. URL: https://lens.org/090-147-732-334-753.

[55] Ruediger Rissmann et al. *Network Attack Detection*. Granted Patent KR 101090815 B1. Republic of Korea, Dec. 8, 2011. URL: https://lens.org/180-018-185-996-580.

[56] Diego Zamboni et al. *Detection And Control Of Peer-to-peer Communication*. Granted Patent JP 4829982 B2. Japan, Dec. 7, 2011. URL: https://lens.org/046-970-961-390-965.

[57] Yann Duponchel et al. *Method For Operating Several Virtual Networks*. Patent Family of EP 1969777 B1. European Patent Office, others, Jan. 27, 2010. URL: https://lens.org/159-743-880-849-911.

[58] Yann Duponchel et al. *Methods For Operating Virtual Networks, Data Network System, Computer Program And Computer Program Product*. Granted Patent KR 100998418 B1. Republic of Korea, Dec. 3, 2010. URL: https://lens.org/002-818-728-052-940.

[59] Yann Duponchel et al. *Verfahren Zum Betrieb Von Mehreren Virtuellen Netzwerken*. Granted Patent DE 602006012095 D1. Germany, Mar. 18, 2010. URL: https://lens.org/023-500-648-492-606.

[60] Yann Duponchel et al. *Verfahren Zum Betrieb Von Mehreren Virtuellen Netzwerken*. Granted Patent AT 456890 T. Austria, Feb. 15, 2010. URL: https://lens.org/066-334-395-713-288.

[61] Ruediger Rissmann et al. *Erkennung Von Netzwerkangriffen*. Granted Patent DE 602006017668 D1. Germany, Dec. 2, 2010. URL: https://lens.org/179-407-514-833-082.

[62] Ruediger Rissmann et al. *Erkennung Von Netzwerkangriffen*. Granted Patent AT 485552 T. Austria, Nov. 15, 2010. URL: https://lens.org/002-199-882-054-266.

[63] Ruediger Rissmann et al. *Network Attack Detection*. Patent Family of EP 1866725 B1. European Patent Office, others, Oct. 20, 2010. URL: https://lens.org/044-792-433-937-531.

[64] Diego Zamboni et al. *Methods For Operating Virtual Networks, Equipment, Data Network System*. Granted Patent CN 101326771 B. China, Sept. 15, 2010. URL: https://lens.org/032-065-473-420-813.

[65] Ruediger Rissmann and Yann Duponchel. *Network Attack Detection Method And Device*. Granted Patent CN 100561492 C. China, Nov. 18, 2009. URL: https://lens.org/038-781-979-981-306.

[66] Morton Swimmer, Andreas Wespi, and Diego Zamboni. *Preventing Attacks In A Data Processing System*. Granted Patent US 7555777 B2. United States, June 30, 2009. URL: https://lens.org/077-245-544-178-974.

[67] Christoph Schuba et al. *Network Protection For Denial Of Service Attacks*. Granted Patent US 6725378 B1. United States, Apr. 20, 2004. URL: https://lens.org/009-701-089-204-105.