

CURRICULUM VITAE ET STUDIORUM

Stefano Zanero

PERSONAL DATA

Name: Stefano
Surname: Zanero
Birth date: 18 Luglio 1979
Birth Place: Melzo (MI), Italia
Citizenship: Italian

Office Address

Dipartimento di Elettronica e Informazione
Politecnico di Milano
Via Ponzio 34/5
I-20133, Milano (MI), Italia
Tel: +39 02 2399 4017
Fax: +39 02 2399 3411
Email: zanero@elet.polimi.it
Home page: <http://home.dei.polimi.it/zanero/>

ACADEMIC POSITIONS

- 07/2008– Ricercatore di ruolo MIUR (equivalent to Assistant Professor), Dipartimento di Elettronica e Informazione, Politecnico di Milano.
- 06/2006–05/2008 Assegnista di Ricerca (post-doc researcher), Dipartimento di Elettronica e Informazione, Politecnico di Milano.
- 03/2006–05/2006 Research Assistant, “FIRB-PERF” project, Dipartimento di Elettronica e Informazione, Politecnico di Milano.
- 03/2003–02/2006 PhD student, research assistant, teaching assistant and contract professor, Dipartimento di Elettronica e Informazione, Politecnico di Milano.

INDUSTRIAL EXPERIENCE

- 2004–today CTO and founder of Secure Network Srl, a computer security training and consulting firm based in Milano, Italy. I co-founded Secure Network in 2004. During these 6 years of operations as a privately owned and self-funded company, Secure Network grew to employ 6 full time employees, and to a revenue of about 650kEUR per year. Customers of renown who allowed to be cited include Poste Italiane (the Italian Postal Service, Italy’s largest corporation and bank with over 180,000 employees), Fantoni

	Group (Europe's largest furniture maker), Riello International (a leading industrial group), UBI Bank (Italy's 4th largest bank), and PartyGaming PLC (a leading online casino and gaming provider based in Gibraltar).
2002–today	Consultant and technical expert witness for courts in Italy (following high-profile cases for customers such as Google, La Clinique, Limoni, and Wind Telecommunications)
1998–2005	Technical writer for IDG Communications and others.

EDUCATION

- 03/2003–02-2006 Ph.D. degree in Computer Engineering, Dipartimento di Elettronica e Informazione, Politecnico di Milano, Milano, Italy, final evaluation "A – cum Laude" (final exam on 18/05/2006).
- Thesis title:** *Unsupervised Learning Algorithms for Intrusion Detection.*
- Advisor:** Prof. G. Serazzi.
- 09/1997–12/2002 Laurea (Vecchio Ordinamento) in Computer Engineering (equivalent to an M.Sc. degree), graduation date 20/12/2002, Politecnico di Milano, Milano, Italia; final grade 100/100 "cum laude"
- Thesis title:** *Un sistema di intrusion detection basato sull'apprendimento non supervisionato.*
- Advisor:** Prof. S. M. Savaresi.
- Coadvisor:** Prof. G. Serazzi.

PUBLICATIONS

INTERNATIONAL JOURNALS

- A1. F. Maggi, M. Matteucci, and S. Zanero. Detecting Intrusions through System Call Sequence and Argument Analysis. *IEEE Transactions on Dependable and Secure Systems*, vol. 7, n. 4, December 2010.
- A2. F. Maggi, M. Matteucci, and S. Zanero. Reducing False Positives In Anomaly Detectors Through Fuzzy Alert Aggregation. *Information Fusion*, special issue on "Information Fusion in Computer Security". Vol. 10, n. 4, October 2009. Elsevier.
- A3. S. Zanero. Wireless Malware Propagation: A Reality Check. *IEEE Security and Privacy*, vol. 7, no. 5, pp. 70-74, September/October, 2009.
- A4. F. Maggi, S. Zanero, and V. Iozzo. Seeing the Invisible - Forensic Uses of Anomaly Detection and Machine Learning. *ACM Operating Systems Review*, vol. 42, no. 3, pag. 52–59, April 2008.
- A5. G. Casale and S. Zanero. GIVS: an Integrity Validation Scheme for Grid Security. *International Journal of Critical Infrastructures*, vol. 4, no. 3, pag. 319–333, 2008.
- A6. L. Carettoni, C. Merloni, and S. Zanero. Studying Bluetooth Malware Propagation: the BlueBag Project. *IEEE Security and Privacy*, vol. 5, no. 2, March/April 2007, pp. 17–25.

- A7. E. Filiol, M. Helenius, and S. Zanero. Open Problems in Computer Virology. *Journal In Computer Virology*, vol. 1, no. 3–4, pag. 55–66, March 2006, Springer.
- A8. P. Perri and S. Zanero. Lessons learned from the Italian legislation on privacy. *Computer Law and Security Report*, volume 20, issue 4-5, pag. 310–313, 384–389, Elsevier Science, 2004.

CHAPTERS IN INTERNATIONAL BOOKS

- B1. G. Serazzi and S. Zanero. Computer Virus Propagation Models. In M. C. Calzarossa, E. Gelenbe, ed., *Performance Tools and Applications to Networked Systems: Revised Tutorial Lectures*, Lecture Notes in Computer Science, vol. 2965, pag. 26–50, Springer-Verlag, Berlino, Germania, 2004.

EDITING OF INTERNATIONAL PROCEEDINGS VOLUMES

- C1. E. Markatos, S. Zanero, editors, “Proceedings of SysSec 2011, 1st SysSec Workshop on Systems Security”, 6 July 2011, Amsterdam, Netherlands, IEEE Computer Society Press, 2011.
- C2. S. Zanero, editor, “Proceedings of EC2ND 2009, European Conference on Computer Networks Defence”, December 2009, Milano, Italy, IEEE Computer Society Press, 2010.
- C3. S. Zanero, editor, “Proceedings of WISTDCS 2008, WOMBAT Workshop on Internet Security Threat Data Collection and Sharing”, 21-22 April 2008, Amsterdam, Netherlands, IEEE Computer Society Press, 2008.
- C4. E. Huebner and S. Zanero, editors, “Proceedings of the 1st International Workshop on Open Source Software for Computer and Network Forensics - OSSCoNF 2008”, held in conjunction with IFIP OSS 2008, 10th September 2008, Milan, Italy

CONTRIBUTIONS IN PROCEEDINGS OF INTERNATIONAL CONFERENCES

- D1. F. Maggi, S. Zanero. Integrated Detection of Anomalous Behavior of Computer Infrastructures. In *IEEE/IFIP Network Operations and Management Symposium (NOMS)*. 16-20 April 2012, Maui, Hawaii, US.
- D2. L. Sportiello, S. Zanero. Context-based File Block Classification. In *8th Annual IFIP WG 11.9 International Conference on Digital Forensics*, Pretoria, South Africa, January 2012.
- D3. F. Maggi, A. Bellini, G. Salvaneschi, and S. Zanero Finding Non-trivial Malware Naming Inconsistencies. In *7th International Conference on Information Systems Security (ICISS)*, 15-19 December 2011, Jadavpur University, Kolkata, India.
- D4. F. Maggi, A. Volpatto, S. Gasparini, G. Boracchi, S. Zanero Fast, Automatic iPhone Shoulder Surfing. In *7th International Conference on Information Assurance and Security (IAS)*, 5-8 December, 2011, Malacca, Malaysia.
- D5. L. Sportiello, S. Zanero. File Block Classification by Support Vector Machines. In *ARES 2011: Sixth International Conference on Availability, Reliability and Security*, August 2011.
- D6. F. Roveta, L. Di Mario, F. Maggi, G. Caviglia, S. Zanero and P. Ciuccarelli. BURN: Baring Unknown Rogue Networks. In *VizSec 2011: Symposium on Visualization in Computer Security*. 20 July 2011, Pittsburgh PA, USA. Best paper award.

- D7. F. Maggi, S. Zanero. System Security research at Politecnico di Milano. In *1st SysSec Workshop (SysSec 2011)*. 6 July, 2011, Amsterdam, The Netherlands.
- D8. F. Maggi, S. Zanero. Is the future Web more insecure? Distractions and solutions of new-old security issues and measures. In *Worldwide Cybersecurity Summit 2011*. 1-2 June, 2011, London, UK.
- D9. F. Maggi, A. Sisto, S. Zanero. A social-engineering-centric data collection initiative to study phishing. In *First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS 2011)*. 10 April, 2011, Salzburg, Austria.
- D10. S. Zanero. Observing the tidal waves of malware: experiences from the WOMBAT project. In *VCON 10: 2nd Vaagdevi International Conference on Information Technology for Real World Challenges*, invited paper, Warangal, India, 9-11 December 2010.
- D11. A. Volpato, F. Maggi and S. Zanero. Effective multimodel anomaly detection using cooperative negotiation. In *GameSec 2010 Conference on Decision and Game Theory for Security*, Berlin, Germany, 22-23 November 2010
- D12. P. Milani Comparetti, G. Salvaneschi, E. Kirda, C. Kolbitsch, C. Kruegel and S. Zanero. Identifying Dormant Functionality in Malware Programs. In *IEEE Security and Privacy symposium 2010*.
- D13. C. Criscione, F. Maggi, G. Salvaneschi, S. Zanero, Integrated Detection of Attacks Against Browsers, Web Applications and Databases. In *European Conference on Computer Networks Defence, EC2ND 2009*, December 2009, Milano
- D14. A. Frossi, F. Maggi, G. Rizzo and S. Zanero. Selecting and Improving System Call Models for Anomaly Detection. In *Detection of Intrusions and Malware & Vulnerability Assessment, DIMVA 2009*, Milan, Italy, July 9-10, 2009.
- D15. A. Galante, A. Kokos, and S. Zanero. BlueBat: Towards Practical Bluetooth Honeypots. In *2009 IEEE ICC International Conference on Communications*, Dresden, Germany, June 2009.
- D16. F. Amigoni, F. Basilico, N. Basilico and S. Zanero. Integrating Partial Models of Network Normality via Cooperative Negotiation - An Approach to Development of Multiagent Intrusion Detection Systems. In *2008 IEEE/WIC/ACM International Conference on Intelligent Agent Technology*, Sydney, Australia, December 9-12, 2008.
- D17. S. Zanero. ULISSE: A Network Intrusion Detection System. In *CSIIRW 2008, Cyber Security and Information Intelligence Research Workshop*, Oak Ridge TN, USA, ACM Press, 2008.
- D18. S. Zanero and G. Serazzi. Unsupervised Learning Algorithms for Intrusion Detection. *IEEE Network Operations and Management Symposium 2008*, Salvador de Bahia, Brasil, April 2008.
- D19. C. Altheide, J. Flynn, C. Merloni and S. Zanero. A methodology for the repeatable forensic analysis of encrypted drives. *ACM SIGOPS EuroSec Workshop*, Glasgow, UK, March 2008.
- D20. F. Maggi, S Zanero. On the use of different statistical tests for alert correlation - Short Paper. In *Proceedings of RAID 2007 - Recent Advances in Intrusion Detection*, pag. 167-177 Surfer's Paradise, Australia, September 2007.
- D21. S. Zanero. Flaws and frauds in the evaluation of IDS/IPS technologies. In *FIRST 2007 - Forum of Incident Response and Security Teams*, Sevilla, Spain, June 2007 (electronic publication).

- D22. G. Casale, P. Cremonesi, G. Serazzi and S. Zanero. Performance Issues in Video Streaming Environments. In *Workshop FIRB-Perf 2005*, pag. 3–14, IEEE Press, September 2005
- D23. S. Zanero. Analyzing TCP Traffic Patterns using Self Organizing Maps. In *Proceedings of the International Conference on Image Analysis and Processing – ICIAP 05*, Special session on Pattern Recognition in Computer Security, pag. 83–90, Lecture Notes in Computer Science, vol. 3617, Springer-Verlag, September 2005
- D24. S. Zanero. Security and Trust in the Italian Legal Digital Signature Framework. In *Proceedings of the iTrust '05 International Conference on Trust Management*, pag. 34–44, Lecture Notes in Computer Science, Vol. 3477, Springer-Verlag, May 2005
- D25. S. Zanero. Improving Self Organizing Map Performance for Network Intrusion Detection. In *Proceedings of the International Workshop on High-Dimensional Data Mining and its applications, SDM 05 SIAM conf. On Data Mining*, pag. 30–37, published online by SIAM (<http://www.siam.org/meetings/sdm05/sdm-clustering.zip>), April 2005
- D26. G. Casale and S. Zanero. GIVS: Integrity Validation for Grid Security. In *Proceedings of the 5th International Conference on Computational Science*, pag. 69–88, Springer Verlag, May 2005
- D27. S. Zanero. Behavioral Intrusion Detection. In *Proceedings of the 19th ISCIS symposium*, Antalya, Turkey, pag. 657–666, Lecture Notes in Computer Science series, Springer-Verlag, October 2004.
- D28. S. Zanero and S. M. Savaresi. Unsupervised Learning Techniques for an Intrusion Detection System. In *Proceedings of the 2004 ACM Symposium on Applied Computing*, Nicosia, Cyprus, pag. 412–419, ACM Press, March 2004
- D29. G. Casale, F. Granata, L. Muttoni and S. Zanero. Optimal Number of Nodes for Computations in a Grid Environment. In *Proceedings of the 12th EuroMicro Conference on Parallel and Distributed Processing*, pag. 282–289, IEEE conference proceedings, February 2004

INVITED TALKS

- E1. S. Zanero. Threat analysis and malware data gathering – Experiences in the WOMBAT project. VCON 10 International Conference, Warangal, India, December 2010.
- E2. S. Zanero, P. Milani Comparetti. The WOMBAT API: querying a global network of advanced honeypots. Black Hat Federal, Washington, D.C., February 2010
- E3. S. Zanero. WOMBAT: Building a Worldwide Observatory of Malicious Behavior and Attack Threats. Keynote talk, SecureIT Conference 2009, Los Angeles CA, March 2009
- E4. S. Zanero. Global Threat Intelligence: a call for action. SHAKACon Conference 2008, Honolulu, Hawaii, June 2008
- E5. S. Zanero. Behavioral analysis in host-based IDS and its application to honeypots. Invited talk, TERENA Networking Conference 2008, Bruges, Belgium, May 2008
- E6. S. Zanero. Observing the Tidal Waves of Malware. DeepSec Conference, Vienna, Austria, November 2007.
- E7. S. Zanero. 360° Unsupervised Anomaly Detection. Hack In The Box Security Conference, Kuala Lumpur, Malaysia, September 2007.
- E8. S. Zanero. Observing the Tidal Waves of Malware. Black Hat USA, Las Vegas, NV, USA, August 2007.

- E9. S. Zanero. My IPS is better than yours... or is it ?. WSIP - World Summit on Intrusion Prevention, Baltimore, May 2007.
- E10. S. Zanero. My ID(P)S is better than yours... or is it ?. SecurityOpus conference, San Francisco, April 2007.
- E11. S. Zanero. 360° Unsupervised Anomaly Detection. Black Hat Europe, Amsterdam, Netherlands, April 2007.
- E12. S. Zanero. 360° Unsupervised Anomaly Detection. Black Hat Federal, Washington, D.C., March 2007.
- E13. S. Zanero. Recent advances on unsupervised learning for intrusion detection. IT Underground Conference, Praga, Rep. Ceca, February 2007.
- E14. S. Zanero. Recent advances on unsupervised learning for intrusion detection. IT Underground Conference, Varsavia, Polonia, November 2006.
- E15. S. Zanero. Host Based Anomaly Detection on System Call Arguments. Black Hat USA, Las Vegas, NV, USA, August 2006.
- E16. S. Zanero. Host Based Anomaly Detection on System Call Arguments. Black Hat Europe, Amsterdam, Netherlands, April 2006.
- E17. S. Zanero. My IDS is better than yours... or is it ?. Black Hat Federal, Washington, D.C., February 2006.
- E18. S. Zanero. Unsupervised learning for intrusion detection. IT Underground Conference, Varsavia, Polonia, October 2005.
- E19. S. Zanero. Automatic Detection of Web Application Security Flaws. Black Hat Europe, Amsterdam, Netherlands, April 2005
- E20. S. Zanero. Unsupervised learning for intrusion detection. IT Underground Conference, Praga, Rep. Ceca, February 2005.
- E21. S. Zanero. Detecting 0-days Attacks With Learning Intrusion Detection Systems. Black Hat USA, Las Vegas, NV, USA, July 2004.
- E22. S. Zanero. Detecting 0-days Attacks With Learning Intrusion Detection Systems. Black Hat Europe, Amsterdam, Netherlands, May 2004.
- E23. S. Zanero. Unsupervised Learning Techniques and Data Mining for Intrusion Detection. CanSecWest Security Conference, Vancouver, Canada, April 2004.

TUTORIAL LECTURES

- F1. S. Zanero. Modeling the spread of computer viruses: aiming at a moving target. VCON 10 International Conference, Warangal, India, December 2010.

SCIENTIFIC AND PROFESSIONAL ACTIVITIES

RESEARCH PROJECTS

- European Project STREP FP7-ICT-216026-WOMBAT “Worldwide Observatory on Malicious Behaviors and Attack Threats”: I have been involved since the inception of the project, participating to the grant proposal writing. The European Union financed the

project with **2.9MEUR, 290kEUR** of which for my research group at DEI. I am the representative of DEI in the General Assembly of the project, and the research coordinator of our research group.

- FIRB project “Performance Evaluation of Complex Systems” (FIRB-PERF, 2003–2006): I was a research assistant.
- NATO Science for Peace project Sfp-983805, “SCADA-NG”. NATO Project Director. The project has been financed with a NATO grant of approximately **250kEUR**, to be shared with our partner, University of Zagreb.
- European CIPS Project “i-Code”: I have been involved since the inception of the project, participating to the grant proposal writing. The European Union financed the project with approximately **540kEUR, 110kEUR** of which for my research group at DEI. I am the representative of DEI for the project.
- European Network of Excellence “SysSec”: I have been involved since the inception of the project, participating to the grant proposal writing. The European Union financed the project with approximately **3MEUR, 320kEUR** of which for my research group at DEI. I am the representative of DEI for the project.

SCIENTIFIC COMMITTEES AND EDITORIAL BOARDS

- Editorial board of the “Journal in Computer Virology”, Springer-Verlag, since 2005; Associate Editor since 2008.
- Editorial board of “Ciberspazio e Diritto”, Mucchi Ed., since 2012
- European Project FORWARD (www.ict-forward.eu), working group on Smart Environments threats (<http://www.ict-forward.eu/wg/smart-environments/>), 2008–2010.
- PROCENT (Priorities of Research On Current and Emerging Network Technologies) expert group of ENISA, 2009–2010.
- General Chair, SysSec Workshop, co-located with DIMVA, 2011
- General Chair, European Conference on Computer Network Defense (EC2ND), 2009–2010
- General Chair, ISSA International Conference, 2009–2010
- General Chair, OSSCoNF 2008 – 1st International Workshop on Open Source Software for Computer and Network Forensics, 10/09/2008, Milano, Italia
- General Chair, WOMBAT Workshop on Internet Security Threat Data Collection and Sharing, 21-22 April 2008, Amsterdam, Vrije Universiteit
- Steering Committee Member, Workshop on Complexity in Engineering, IEEE Italy Section, 2009
- Reviewer Board of the Black Hat Conference, since 2011
- Programme Committee COMPENG 2012
- Programme Committee IMIS/CISIS 2012
- Programme Committee InfQ 2011–2012
- Programme Committee SAFECOMP 2011 – 30th International Conference on Computer Safety, Reliability and Security

- Programme Committee Conference on Cyber Conflict 2010–2011
- Programme Committee EICAR conference 2009–2012
- Programme Committee European Conference on Computer Network Defense (EC2ND), 2007–2008
- Programme Committee workshop ACM EuroSec 2008, 2011, 2012
- Programme Committee DeepSec conference, 2007–2008
- Guest Editor, “Upgrade”, journal of CEPIS (Council of European Professional Information Societies), special issue on “Business Continuity and Security”, 2005
- Working Group AICA/CEPIS on the EUCIP certification – module 5 “Information Security”

REVIEWER SERVICE

- Reviewer for the international journals “ACM Computing Reviews”, “IEEE Security&Privacy”, “Performance Evaluation”, “Journal of Systems Architecture”, “ACM Transactions on Information Systems Security”, “International Journal of Information Security”, “IEEE Transactions on Dependable and Secure Computing”, “IEEE Transactions on Computers”, “Computers and Security”.
- Reviewer for the international conferences (besides the ones for which I served as a PC member): ACM Workshop on Secure Web Services (SWS) 2008, ACM Symposium on Applied Computing (SAC), 2004–2005; International Conference on Image Analysis and Processing (ICIAP), 2005; European Symposium on Research in Computer Security (ESORICS), 2005–2006.

ASSOCIATION ACTIVITIES

2000–today	National Order of Journalists, associate member;
2001–today	Association for Computer Machinery, lifetime member <ul style="list-style-type: none"> • ACM SIGSAC, Special Interest Group on Security and Access Control • ACM SIGOPS, Special Interest Group on Operating Systems
2001–today	Institute of Electrical and Electronics Engineers, Student Member, Member (since 2006), Senior Member (since 2010) <ul style="list-style-type: none"> • IEEE Computer Society, member
2008–2009	IEEE Computer Society, Italian chapter, vice-chair
2008	IEEE Section Italy, primary delegate to IEEE Sections Congress 2008 (18–22 Settembre 2008, Quebec City, Canada)
2009–2010	IEEE Section Italy, Educational Activities chair
2010–2011	IEEE Computer Society, Italian chapter, chair
2011–2012	IEEE Region 8 Publications Coordinator
2012	IEEE Computer Society Region 8 Membership Development Coordinator
2005–today	Milan’s order of chartered Professional Engineers, Member;

2008–today Standing Committee on Information Engineering, member
2005–today ISSA (Information Systems Security Association); Senior Member (since 2012)
2005–today Founding Member and Director, ISSA Italy chapter
2008–2012 ISSA International Board of Directors member

TEACHING ACTIVITIES

- Director of the “Security Specialist” specialization degree (“Master universitario di primo livello”) at Politecnico di Milano
- I have been a professor for 11 courses from 2006 to 2011 (at bachelor, master’s, and PhD levels).
- I have been a teaching assistant in 18 courses between 2003 and 2009.
- I have been the coadvisor or advisor of over 90 bachelor and master’s thesis at the Politecnico di Milano, the University of Illinois at Chicago, University of Milan, and the University of Milano-Bicocca.
- I have advised 1 PhD thesis (F. Maggi), leading to “cum laude” graduation
- I have also lectured at the University of Milan, University of Rome “Tor Vergata”, and at the LaSalle University of Barcelona, Spain.