CURRICULUM VITAE ET STUDIORUM

Stefano Zanero

Personal Data
Birthdate: 18 July 1979
Birthplace: Melzo (MI), Italy
Residency: Milan, Italy
Citizenship: Italian

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

MAIN FACTS AND HIGHLIGHTS

- Research interests focused on **cybersecurity**, in particular on the identification of current and future threats. I focus on (large scale and automated) malware analysis, mobile security and mobile malware, extraction of threat intelligence from large-scale datasets, computer forensics and financial frauds. I associate to this an extensive experience in offensive security. My background is in anomaly-based intrusion detection techniques and their evaluation.
- Publication track: 52 papers on journals and conferences, including one paper on IEEE Transaction on Dependable and Secure Computing (with 65 citations according to Google Scholar), as well as 3 other papers on IEEE magazines and journals (one of which cited 55 times). Among the conferences, one publication at IEEE Security and Privacy (absolute top conference in the area, acceptance rate 9.7% and 59 citations), and one at ACM CCS (the competing top conference). Two publications at WWW (top conference in the Web research area, acceptance rate average 12%). Several publications at tier 2 conferences such as ACSAC, RAID, DIMVA. According to Google Scholar: 1015 citations (723 since 2010), H-index 15, i10-index 23. According to SCOPUS, 357 total citations and H-index 10. Most cited articles on conferences have 205 and 111 citations. I also edited 4 proceedings volumes and guest edited one special issue of the IEEE Transactions on Emerging Topics in Computing. In addition to the publication track, I have been an invited speaker at tens of industrial and hacking conferences around the world.
- Service in the IEEE: elected member of the Board of Governors of the Computer Society; also served on the Region 8 committees, the MGA committees, the Section ExCom, and has been a Chapter officer. In the ISSA (Information Systems Security Association), founding member of the Italy chapter, has served for 7 years on the International Board of Directors, and has been named a Fellow in 2014.
- Research funding: principal investigator for TENACE (PRIN project), SysSec (EU FP7 NoE), i-Code (EU CIPS). Research activities coordinator for WOMBAT (EU FP7 STREP). Project

Director and P.I. for SCADA-NG (NATO Science for Peace). Between 2008 and 2015 my research received over 800kEUR of funding from different external entities.

- I have been the general chair of a number of conferences, notably ESSoS 2015, EC2ND (2009 and 2010), as well as the program chair for IEEE CSS 2015. I also served on the program committee of a number of conferences and workshops, notably DIMVA 2013, ICISS (2012-2014), SAC 2015, SAFECOMP 2011. I am on the editorial board of the "Journal of Computer Virology and Hacking Techniques" (Springer-Verlag) since 2005. Since 2011 I have been on the Reviewer Board of the prestigious industrial conference "Black Hat".
- I have advised 1 PhD student in the past, and I am currently advising 3 PhD students and co-advising other 2. I have been a professor for 17 courses from 2006 to 2013 (at bachelor, Master's, and PhD levels). I have been the coadvisor or advisor of over 90 bachelor and master's theses.
- Industrial technology transfer experience (founding two startups), as well as practical experience in computer forensics in criminal and civil cases

TABLE OF CONTENTS

ACADEMIC POSITIONS

07/2015–	Associate Professor, Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano.
07/2008–06/2015	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.

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.

RESEARCH STATEMENT

My research has been always focused on the field of computer security traditionally known as "systems security" and which is now evolving in the so-called "cybersecurity" area. In particular, I moved from intrusion detection to malware analysis and threat intelligence and characterization. In addition, I found over the years that several of the most successful and satisfactory research activities were born from interdisciplinary ideas, or from needs and challenges coming from colleagues from different fields.

CURRENT RESEARCH FOCUS

My current research interests focus on current and future cybersecurity threats. Part of my most recent activities are related to strategical and political issues of cybersecurity and cyberwarfare (both through publications such as [A3], and through leadership in organizations such as chairing the IEEE Computer Society's STC on Cybersecurity).

Malware analysis: My earliest interest in malware research was computer virology, i.e. the modeling of the spread of computer viruses ([A12], [B1]). More recently, I was one of the first who analyzed the likelihood of success of Bluetooth viruses ([A11],[D34]) and concluded it just was unlikely ([A8]). I also held a successful tutorial on the subject, [F1]).

Inspired by this line of research, I moved on to explore automated malware analysis, and in particular how it could be made more efficient to cope with the growing wave of malicious samples we are seeing every day ([D29]). This led to one of my most important publications ([D31]), Reanimator, a system to combine static and dynamic analysis to find dormant code in large datasets of malicious samples. Other research results of note are related to the characterization of malware evolution [D19], to the tracking of DGA-based malware [D10], and to the automatic and malware-agnostic extraction of WebInject signatures [D9].

Mobile malware and security of mobile applications: Starting in 2012 I have been working on Android malware. I have been focusing on how to compare different antivirus application on the Android platform. That led us to the development of a publicly available platform called "AndroTotal" (`http://andrototal.org`), that anyone can use to automatically analyze suspicious APKs with multiple antivirus apps for the Android system [D16],[A1]. AndroTotal is used by a dozen of antivirus companies around the world, and by thousands of users, both via the web application and the APIs. Using AndroTotal we were also able to implement AndRadar, a system for fast discovery of Android applications on alternative markets [D11]. On a different vein, we are working on the security of mobile applications: one example is [A5], another is [D4].

Data analytics and visualization for security intelligence: A recurring theme of my research is the usage of anomaly detection, visualization and data analytics techniques to extract actionable intelligence from large datasets of security-relevant phenomena. Sometimes this extends to collecting the datasets first: for instance we collected and analyzed datasets on malicious abuses of URL shorteners that led to two publications at the highly selective WWW conference ([D17],[D14]).

Sometimes we devise clever ways of obtaining threat intelligence from publicly available data. For instance we devised a system to extract intelligence on DGA-based botnets from passive DNS data [D10], and a system to de-anonymize and tag Bitcoin users [D13] that attracted the interest of international press.

Visualization can be an important part of such experiments: this is well represented by [D25], which was presented with a best paper award.

The collection of malware datasets that supports some of our previously-described research also partially falls in this area ([D29], [A1]). Other areas we explored are phishing [D28] and social network privacy and security [D7].

Financial Fraud: Financial fraud is a growing area of concern and interest. Thanks to an industrial research relationship, we could access an extensive dataset of financial transactions, which we used to develop BankSealer, a fraud analysis and decision support system targeted to online banking environments [D12]. This paper received a best paper award, and we are currently preparing several followup works. In a way, our previously mentioned work on Bitcoin [D13] is also related to this area.

Computer Forensics: I have explored in several directions the modern challenges to file reconstruction, applying clustering and classification techniques to file carving ([D24], [D21]) as well as

studying in-depth the impact of the introduction of SSD disks on forensic analysis ([A4], [D15]). An earlier research work dealt with the rising issue of encrypted hard drives ([D38]).

Attack papers and offensive research: Systems security is unique in offering opportunities to conduct "offensive" security research, leading to attack papers describing fault in widespread or important technologies. The most significant result in this area was breaking Facebook's social authentication system ([D18], [D7]), which led to a paper (describing both the attacks and a secure design solution) in the selective CCS conference [D6]. Another interesting work demonstrated the weakness of the iOS input system to snooping [D23].

SCIENTIFIC BACKGROUND

My PhD and my early years of post-doc research were mostly focused on intrusion detection, and in particular on the application of unsupervised learning techniques to anomaly detection. My seminal work in the area is [D47], to date my most cited paper, detailing a two-tier architecture for network anomaly detection which could take into account anomalous packets. This was a very novel intuition, and I worked on it through several subsequent publications, analyzing its payload detector [D42], improving its performance [D44], up to the design of a complete system named ULISSE ([D37], [D36]). I then moved on to the application of learning techniques to host-based detection through system call sequence and arguments - as opposed to sequence alone, which was the limit of previous literature. This led to a publication in the IEEE Transactions [A6], as well as another journal [A9] and conference publication [D33]. I also briefly explored the usage of multiagent techniques such as cooperative negotiation to perform network anomaly detection [D35], [D30], as well as detection of attacks on web infrastructures [D32] [D27].

Another important area I tackled was the correlation of alerts [D39] and their aggregation and false positive reduction [A7]. In this area I also oversaw the successful doctoral thesis of Dr. Federico Maggi (which was tied to publications [D39], [D33], [D30], [D20], [A7]). I also gained expertise in the intricacies of evaluation of IDS and IPS technologies [D40].

RESEARCH COLLABORATIONS

Besides the research connections related to joint projects listed in the following section, it is important to outline the following, ongoing and long-term research collaborations:

- Prof. S. Bratus of Dartmouth college: joint initiatives in the cybersecurity, cyberwarfare and policy areas [A3].
- Prof. E. Markatos and S. Ioannidis and their research group at FORTH (particularly I. Polakis): joint research on several areas, including mobile malware and social network security [D6], [D7], [D18]
- Prof. A. D. Keromytis of Columbia University: social network security research [D6], [D7], [D18]
- Prof. L. Cavallaro at Royal Holloway Univ. of London: joint research on DGA-based botnets and on mobile security [D10]
- Prof. C. Kruegel and G. Vigna at UCSB: joint research on malware analysis, as well as on emerging Internet threats [D14], [D17], [D31]
- Prof. E. Kirda at Northeastern university: joint research on malware analysis, as well as a new research project on kernel-based attack mitigation [D31]

RESEARCH FUNDING

- European Marie Curie RISE Project "PROTASIS": Local Principal Investigator. The European Union financed the project with approximately **EUR**, **320kEUR** of which for my research group at DEI.
- PRIN project "TENACE: Protecting National Critical Infrastructures From Cyber Threats": Local Principal Investigator. The Italian Ministry of University and Research financed the project. Financing received: **77kEUR** for my research group at DEIB.
- European Network of Excellence "SysSec": Local Principal Investigator. The European Union financed the project with approximately **3MEUR**, **320kEUR** of which for my research group at DEI.
- 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": Local Principal Investigator. The European Union financed the project with approximately **540kEUR**, **110kEUR** of which for my research group at DEI.
- European Project STREP FP7-ICT-216026-WOMBAT "Worldwide Observatory on Malicious Behaviors and Attack Threats": Participant and local Research Coordinator. The European Union financed the project with **2.9MEUR**, **290kEUR** of which for my research group at DEI.
- FIRB project "Performance Evaluation of Complex Systems" (FIRB-PERF, 2003–2006): Participant. The Local Principal Investigator was prof. G. Serazzi.

ASSOCIATION ACTIVITIES AND SERVICE

2001–today IEEE Computer Society

- 2013-2018 Board of Governors elected member
- 2014 Publications ad-hoc committee
- 2015-2016 Cybersecurity Special Technical Community chair
- 2015 Constitution and Bylaws committee member
- 2016 Audit committee chair
- 2012 Region 8 Membership Development Coordinator
- 2010-2012 Italy chapter chair
- 2008–2009 Italy chapter vice-chair

2001–today Institute of Electrical and Electronics Engineers

- 2014-2015 MGA Board, IT Coordination And Oversight Committee
- 2014 Region 8 Conference Coordination Subcommittee (CoCSC)
- 2011-2012 Region 8 Publications Coordinator
- 2009-2013 Section Italy, Educational Activities chair

2005–today ISSA (Information Systems Security Association)

- 2005 Founding Member, Italy chapter
- 2005–2012 Italy chapter, Board of Directors

2008–2016 International Board of Directors, elected member

2005–today Milan's order of chartered Professional Engineers

2008–today Standing Committe on Information Engineering, appointed member

2000–today National Order of Journalists, associate member;

ACADEMIC SERVICES AND RESPONSIBILITIES

2014–today Node coordinator for POLIMI, CINI National Cyber Security Lab

2013-2014 Director, "Security Specialist" specialization degree ("Master universitario di primo livello") at Politecnico di Milano

INDUSTRIAL EXPERIENCE

2011–today Co-founder of 18Months Srl, a startup delivering cloud-based ticketing solutions for cinemas, based in Milano, Italy.

2004–today President and founder of Secure Network Srl, a computer security consulting firm based in Milano, Italy and in London, UK. I co-founded Secure Network in 2004. During these years of operations as a privately owned and self-funded company, Secure Network grew to employ 10 full time employees, and to a yearly revenue of about 1MEUR.

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.

AWARDS AND RECOGNITIONS

2014 Best paper award for paper [D12], "BankSealer: An Online Banking Fraud Analysis and Decision Support System" at the 29th IFIP International Information Security and Privacy Conference

2014 ISSA Fellow

2013 IEEE Computer Society Golden Core Award

2012 ISSA Senior Membership

2012 ACM Senior Membership

2011 Best paper award for paper [D25], "BURN: Baring Unknown Rogue Networks", at the 2011 Symposium on Visualization in Computer Security (VizSec).

2010 IEEE Senior Membership

2003 Cisco's "Best Technical Journalist" award

PUBLICATIONS

INTERNATIONAL JOURNALS

A1. A. Valdi, E. Lever, S. Benefico, D. Quarta, S. Zanero, F. Maggi. Scalable Testing of Mobile Antivirus Apps. *IEEE Computer*, vol.48, no.11, pp.60-68, Nov. 2015

A2. M. Carminati, R. Caron, I. Epifani, F. Maggi, S. Zanero. BankSealer: A Decision Support System for Online Banking Fraud Analysis and Investigation. *Computers & Security*, Elsevier, Vol. 53, pp. 175–186, September 2015.

A3. S. Bratus, I. Arce, M. E. Locasto, S. Zanero. Why Offensive Security Needs Engineering Textbooks: Or, How to Avoid a Replay of "Crypto Wars" in Security Research. *;login:*, USENIX, Vol. 39, No. 4, August 2014.

A4. G. Bonetti, M. Viglione, A. Frossi, F. Maggi, S. Zanero. Black-box Forensic and Antiforensic Characteristics of Solid-state Drives. *Journal of Computer Virology and Hacking Techniques*, Vol. 10, No. 4, November 2014.

A5. A. Dardanelli, F. Maggi, M. Tanelli, S. Zanero, S. M. Savaresi, R. Kochanek and T. Holz. Secure integration of mobile devices for automotive services. *IEEE Embedded System Letters*, vol. 5, n. 3, 2013.

A6. 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.

A7. 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.

A8. S. Zanero. Wireless Malware Propagation: A Reality Check. *IEEE Security and Privacy*, vol. 7, no. 5, pp. 70-74, September/October, 2009.

A9. 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.

A10. G. Casale and S. Zanero. GIVS: an Integrity Validation Scheme for Grid Security. *Internation Journal of Critical Infrastructures*, vol. 4, no. 3, pag. 319–333, 2008.

A11. 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.

A12. 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.

A13. 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. L. Falsina, Y. Fratantonio, S. Zanero, C. Kruegel, G. Vigna, F. Maggi. Grab 'n Run: Secure and Practical Dynamic Code Loading for Android Applications. In *Proceedings of ACSAC 2015*, pp. 201-210, December 2015, Los Angeles CA.

D2. N. Andronio, S. Zanero, F. Maggi. HelDroid: Dissecting and Detecting Mobile Ransomware. In *Proceedings of RAID 2015*, pp. 382-404. November 2014, Kyoto, Japan.

D3. M. Polino, A. Scorti, F. Maggi, S. Zanero. Jackdaw: Towards Automatic Reverse Engineering of Large Datasets of Binaries. In *Proceedings of DIMVA 2015*, July 2015, Milano, Italy.

D4. D. Gallingani, R. Gjomemo, V.N. Venkatakrishnan, S. Zanero. Static Detection and Automatic Exploitation of Intent Message Vulnerabilities in Android Applications. In *Proceedings of MoST 2015*, San Jose, CA, May 2015.

D5. D. Gallingani, R. Gjomemo, V.N. Venkatakrishnan, S. Zanero. Practical Exploit Generation for Intent Message Vulnerabilities in Android. In *Proceedings of CODASPY 2015*, San Antonio, TX, USA, March 2015. **Outstanding Poster Award**

D6. I. Polakis, P. Ilia, F. Maggi, M. Lancini, G. Kontaxis, S. Zanero, S. Ioannidis, A. D. Keromytis. Faces in the Distorting Mirror: Revisiting Photo-based Social Authentication. In *Proceedings of the 21st ACM Conference on Computer and Communications Security, CCS '14*, Scottsdale, Arizona, November 2014.

D7. I. Polakis, F. Maggi, S. Zanero, A. D. Keromytis. Security and Privacy Measurements on Social Networks: Experiences and Lessons Learned. In *Proceedings of the 3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, BADGERS'14*, Wroclaw, Poland, September 2014.

D8. A. Antonini, F. Maggi, S. Zanero. A Practical Attack Against a KNX-based Building Automation System. In *Proceedings of the 2nd International Symposium for ICS & SCADA Cyber Security Research*, St. Pölten, Austria, September 2014.

D9. C. Criscione, F. Bosatelli, S. Zanero, F. Maggi. Zarathustra: Extracting WebInject Signatures from Banking Trojans. In *Twelfth Annual International Conference on Privacy, Security and Trust (PST)*.

D10. S. Schiavoni, F. Maggi, L. Cavallaro and S. Zanero. Phoenix: DGA-based Botnet Tracking and Intelligence. In *Proceedings of DIMVA 2014*, Egham, UK, July 10-11 2014.

D11. M. Lindorfer, S. Volanis, A. Sisto, M. Neugschwandtner, E. Athanasopoulos, F. Maggi, C. Platzer, S. Zanero and S. Ioannidis. AndRadar: Fast Discovery of Android Applications in Alternative Markets. In *Proceedings of DIMVA 2014*, Egham, UK, July 10-11 2014.

D12. M. Carminati, R. Caron, F. Maggi, I. Epifani, S. Zanero. BankSealer: An Online Banking Fraud Analysis and Decision Support System. In *Proceedings of the 29th IFIP International Information Security and Privacy Conference*, Marrakech, Morocco, June 2-4, 2014. **Best paper award**.

D13. M. Spagnuolo, F. Maggi and S. Zanero. BitIodine: Extracting Intelligence from the Bitcoin Network. In *Proceedings of the 18th International Conference on Financial Cryptography and Data Security, Financial Crypto 2014*, Christ Church, Barbados, March 3-7, 2014.

D14. N. Nikiforakis, F. Maggi, G. Stringhini, M. Z. Rafique, W. Joosen, C. Kruegel, F. Piessens, G. Vigna and S. Zanero. Stranger Danger: Exploring the Ecosystem of Ad-based URL Shortening Services. In *Proceedings of the 23rd International World Wide Web Conference (WWW2014)*, Seoul, Republic of Korea, April 7-11, 2014.

D15. G. Bonetti, M. Viglione, A. Frossi, F. Maggi, S. Zanero. A Comprehensive Black-box Methodology for Testing the Forensic Characteristics of Solid-state Drives. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, New Orleans LA, December 2013.

D16. F. Maggi, A. Valdi, S. Zanero. AndroTotal: A Flexible, Scalable Toolbox and Service for Testing Mobile Malware Detectors. In *Proceedings of the 3rd Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, Berlin, November 2013.

D17. F. Maggi, A. Frossi, G. Stringhini, B. Stone-Gross, S. Zanero, C. Kruegel, G. Vigna. Two Years of Short URLs Internet Measurement: Security Threats and Countermeasures. In *Proceedings of the 22nd International World Wide Web Conference (WWW2013)*. May 2013, Rio de Janeiro, Brazil.

D18. J. Polakis, M. Lancini, G. Kontaxis, F. Maggi, S. Ioannidis, A. Keromytis, S. Zanero. All Your Faces Are Belong to Us: Breaking Facebook's Social Authentication. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*. December 2012, Orlando, Florida, US.

D19. M. Lindorfer, A. Di Federico, F. Maggi, P. Milani Comparetti, S. Zanero. Lines of Malicious Code: Insights Into the Malicious Software Industry. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*. December 2012, Orlando, Florida, US.

D20. 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.

D21. 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.

D22. 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.

D23. 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.

D24. L. Sportiello, S. Zanero. File Block Classification by Support Vector Machines. In *ARES 2011: Sixth International Conference on Availability, Reliability and Security*, August 2011.

D25. 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**.

D26. F. Maggi, S. Zanero. System Security research at Politecnico di Milano. In *1st SysSec Workshop (SysSec 2011)*. 6 July, 2011, Amsterdam, The Netherlands.

D27. 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.

D28. 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.

D29. 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.

D30. A. Volpatto, 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

D31. 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*.

D32. 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

D33. 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.

D34. A. Galante, A. Kokos, and S. Zanero. BlueBat: Towards Practical Bluetooth Honeypots. In *2009 IEEE ICC International Conference on Communications*, Dresden, Germany, June 2009.

D35. 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.

D36. 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.

D37. S. Zanero and G. Serazzi. Unsupervised Learning Algorithms for Intrusion Detection. *IEEE Network Operations and Management Symposium 2008*, Salvador de Bahia, Brasil, April 2008.

D38. 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.

D39. 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.

D40. 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).

D41. 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

D42. 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

D43. 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

D44. 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

D45. 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

D46. 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.

D47. 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

D48. 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. Making sense of a million samples per day. Istituto Superior Tecnico, Lisbon, Portugal, December 2015.

E2. S. Zanero. Building cybersecurity research capabilities: the European experiences of the SysSec and PROTASIS networks. Science Council of Japan, Tokyo, Japan, November 2015.

E3. S. Zanero. Jackdaw: Automatic, unsupervised, scalable extraction and semantic tagging of (interesting) behaviors. Waseda University, Tokyo, Japan, November 2014.

E4. S. Zanero. Jackdaw: Automatic, unsupervised, scalable extraction and semantic tagging of (interesting) behaviors. BlueHat Security Conference. Microsoft, Redmond, WA, October 2014.

E5. S. Zanero. Jackdaw: Automatic, unsupervised, scalable extraction and semantic tagging of (interesting) behaviors. Hack In The Box Security Conference, Kuala Lumpur, Malaysia, October 2014.

E6. S. Zanero. Tracking and Characterizing Botnets Using Automatically Generated Domains. Hack In The Box Security Conference, Kuala Lumpur, Malaysia, October 2013.

E7. S. Zanero. Behavior-based methods for automated, scalable malware analysis. International Software Summit 2013, Techno India NJR Institute of Technology, Udaipur, India

E8. S. Zanero. Security of cyber-physical systems. GITEX, Dubai, October 2012.

E9. S. Zanero. Behavior-based methods for automated, scalable malware analysis. Hack In The Box Security Conference, Kuala Lumpur, Malaysia, October 2012.

E10. S. Zanero. Security of cyber-physical systems. Boeing-IEEE New Technologies Industry Seminar, Washington D.C., USA, August 2012.

E11. S. Zanero. Threat analysis and malware data gathering – Experiences in the WOMBAT project. VCON 10 International Conference, Warangal, India, December 2010.

E12. S. Zanero, P. Milani Comparetti. The WOMBAT API: querying a global network of advanced honeypots. Black Hat Federal, Washington, D.C., February 2010

E13. S. Zanero. WOMBAT: Building a Worldwide Observatory of Malicious Behavior and Attack Threats. Keynote talk, SecureIT Conference 2009, Los Angeles CA, March 2009

E14. S. Zanero. Global Threat Intelligence: a call for action. SHAKACon Conference 2008, Honolulu, Hawaii, June 2008

E15. S. Zanero. Behavioral analysis in host-based IDS and its application to honeypots. Invited talk, TERENA Networking Conference 2008, Bruges, Belgium, May 2008

E16. S. Zanero. Observing the Tidal Waves of Malware. DeepSec Conference, Vienna, Austria, November 2007.

E17. S. Zanero. 360° Unsupervised Anomaly Detection. Hack In The Box Security Conference, Kuala Lumpur, Malaysia, September 2007.

E18. S. Zanero. Observing the Tidal Waves of Malware. Black Hat USA, Las Vegas, NV, USA, August 2007.

E19. S. Zanero. My IPS is better than yours... or is it ?. WSIP - World Summit on Intrusion Prevention, Baltimore, May 2007.

E20. S. Zanero. My ID(P)S is better than yours... or is it ?. SecurityOpus conference, San Francisco, April 2007.

E21. S. Zanero. 360° Unsupervised Anomaly Detection. Black Hat Europe, Amsterdam, Netherlands, April 2007.

E22. S. Zanero. 360° Unsupervised Anomaly Detection. Black Hat Federal, Washington, D.C., March 2007.

E23. S. Zanero. Host Based Anomaly Detection on System Call Arguments. Black Hat USA, Las Vegas, NV, USA, August 2006.

E24. S. Zanero. Host Based Anomaly Detection on System Call Arguments. Black Hat Europe, Amsterdam, Netherlands, April 2006.

E25. S. Zanero. My IDS is better than yours... or is it ?. Black Hat Federal, Washington, D.C., February 2006.

E26. S. Zanero. Automatic Detection of Web Application Security Flaws. Black Hat Europe, Amsterdam, Netherlands, April 2005

E27. S. Zanero. Detecting 0-days Attacks With Learning Intrusion Detection Systems. Black Hat USA, Las Vegas, NV, USA, July 2004.

E28. S. Zanero. Detecting 0-days Attacks With Learning Intrusion Detection Systems. Black Hat Europe, Amsterdam, Netherlands, May 2004.

E29. 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 ORGANIZATIONAL ACTIVITIES

EDITORIAL SERVICES

- Guest Editor, IEEE Transactions on Emerging Technologies in Computing, Special Issue on "Emerging Topics in Cyber Security" (completed, scheduled for 2015)
- Editorial board of the "Journal in Computer Virology", now "Journal of Computer Virology and Hacking Techniques", Springer-Verlag, since 2005
- Editorial board of "Ciberspazio e Diritto", Mucchi Ed., since 2012
- Editorial board of the "Encyclopedia of Computer Science and Technology", Taylor&Francis, since 2013
- Guest Editor, "Upgrade", journal of CEPIS (Council of European Professional Information Societies), special issue on "Business Continuity and Security", 2005

CONFERENCE ORGANIZATION

- General Chair, Engineering Secure Sofware and Systems, ESSoS, 2015
- General Chair, SysSec Workshop, 2013–2014
- General Chair, European Conference on Computer Network Defense (EC2ND), 2009–2010
- General Chair, ISSA International Conference, 2009–2015
- General Chair, OSSCoNF – International Workshop on Open Source Software for Computer and Network Forensics, 10/09/2008, Milano, Italia
- General Chair, WOMBAT Workshop on Internet Security Threath Data Collection and Sharing, 21-22 April 2008, Amsterdam, Vrije Universiteit
- Program Chair, 7th International Symposium on Cyberspace Safety and Security, IEEE CSS 2015, Aug. 24–26 2015, New York, USA.

PROGRAMME COMMITTEE SERVICE

- Black Hat Conference, 2011–2016
- Mobile, Secure and Programmable Networking (MSPN) 2015–2016
- LangSec Workshop at Security & Privacy, 2014–2016
- SAC 2015
- ACM EuroSec workshop 2008, 2011–2015
- ECTCM (Emerging Cyberthreats and Countermeasures) 2014–2015
- WISTP 2013–2015
- WSDF 2013, 2015
- DIMVA 2013
- PPREW 2012
- ICISS 2012–2015

- COMPENG 2012
- IMIS/CISIS 2012
- InfQ 2011–2012
- SAFECOMP 2011 – 30th International Conference on Computer Safety, Reliability and Security
- NATO Conference on Cyber Conflicts (CyCon) 2010–2016
- EICAR conference 2009–2012
- European Conference on Computer Network Defense (EC2ND), 2007–2008

REVIEWER SERVICE

- Reviewer, Austrian national FWF funded projects
- Reviewer of Scientific Projects (PRIN) for MIUR
- Reviewer of Scientific Projects for the Autonomous Province of Trento.
- 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", "Journal of Computer Security", "IEEE Transactions on Information Forensics & Security", "Information Processing Letters".

OTHER SERVICES

- Doctoral defense committee, Mr. Diogo Monica, Istituto Superior Tecnico, Lisbon, Portugal.
- Doctoral defense committee, Mr. Iason-Stylianos Polakis, University of Crete, Greece.
- Representative of Politecnico di Milano in the Vision2020 initiative, for the Security research line
- 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
- Working Group AICA/CEPIS on the EUCIP certification – module 5 "Information Security"

TEACHING ACTIVITIES

- Director of the "Security Specialist" specialization degree ("Master universitario di primo livello") at Politecnico di Milano
- I have been a professor for 17 official courses from 2006 to 2013 (at bachelor, Master's, and PhD levels). Course titles:
  - "Progetto di Impianti Informatici" (2005/2006, 2006/2007, 2007/2008) (I livello - B.Sc.)

  - "Impianti di Elaborazione" (2007/2008) (I livello - B.Sc.)
  - "Impianti Informatici" (2008/2009) (I livello - B.Sc.)
  - "Progetto di Ingegneria Informatica" (2009/2010) (I livello - B.Sc.)
  - "Sicurezza delle Applicazioni Informatiche" (2008/2009) (II livello - M.Sc.)
  - "Computer Security" (2009/2010, 2010/2011, 2011/2012, 2012/2013, 2013/2014, 2014/2015) (II livello - M.Sc.)
  - "Informatica Forense" (2011/2012, 2012/2013, 2013/2014, 2014/2015) (II livello - M.Sc.)
  - "Privacy and Security" (2011/2012, 2012/2013, 2013/2014, 2014/2015) (II livello - M.Sc.)
  - "Advanced Topics in Computer Security" (2010, 2012, 2013, 2014, 2015) (Ph.D. course)

- 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 theses at Politecnico di Milano, the University of Illinois at Chicago, the Technical University of Eindhoven, University of Milan, and the University of Milano-Bicocca.
- I have advised 1 PhD thesis (F. Maggi), leading to "cum laude" graduation
- I am currently advising 3 PhD students (Mario Polino, Michele Carminati, Davide Quarta) and co-advising other 2 (Andrea Continella, Eugenio Massa).
- I have also lectured at the University of Milan, University of Rome "Tor Vergata", and at the LaSalle University of Barcelona, Spain.