CURRICULUM VITAE OF EMMANUELE ZAMBON

Personal information

Name	Emmanuele Zambon
E-mail	emmanuele.zambon@gmail.com
Nationality	Italian
Date of birth	27/11/1980
Affiliation	Security Group, Eindhoven University of Technology P.O. Box 513 5600 MB Eindhoven, the Netherlands

Employment history

Dates	02/2021 -
Position	Researcher at Eindhoven University of Technology
Main activities and responsibilities	Supervision of Master and PhD students Research on ICS and IoT network security Technical consultant in setting up a student-powered Security Operation Center
Dates	11/2018 – 12/2020
Position	Sr. Director of OT Technology at Forescout Technologies BV
Main activities and responsibilities	▪ Senior advisor for product architecture and engineering ▪ Supervision of a team of elite engineers (6 engineers) ▪ Network security and operation analysis for top customers ▪ Analysis of Industrial Control System network protocols and vulnerabilities ▪ Product development of OT technology support and of new detection mechanisms
Dates	01/2011 – 11/2018
Position	Co-Founder and Chief Technology Officer at SecurityMatters BV
Main activities and responsibilities	▪ Research and engineering of new and cutting edge network monitoring and intrusion detection solutions for Operational Technology networks ▪ Responsible for product vision, architecture and design ▪ Analysis of Industrial Control System network protocols and vulnerabilities ▪ Management of the product team (20+ engineers) ▪ Network security and operation analysis for customer production environments ▪ Coordinator of activities and tasks within national and international research projects
Dates	01/2011 – 09/2016
Position	Postdoc researcher (part-time) at University of Twente
Main activities and responsibilities	▪ Principal contributor of several national and EU successful research projects ▪ New EU project proposals ▪ Supervision of PhD student ▪ OT security research
Dates	04/2005 – 08/2006
Position	IT consultant for Telecom Italia SpA at ValueTeam SpA
Main activities and responsibilities	▪ Technical and Architectural consulting, design of distributed architectures for accessing telephone traffic data. ▪ Analysis and testing of data loading processes into a telephone traffic database. ▪ Analysis and testing of a JAVA/STRUTS-based web application for accessing large amounts of telephone traffic data. ▪ Analysis and testing of integrated telephone traffic post processing systems.
Dates	09/2003 – 09/2004
Position	IT security consultant at KPMG Italy SpA

Main activities and responsibilities	▪ Penetration tests (ethical hacking) ▪ Risk assessment ▪ IT Audit support ▪ Design and building of Intrusion Detection Systems ▪ Application develop on the J2EE platform
Dates	01/2003 – 08/2003
Position	Freelance software developer
Main activities and responsibilities	Design and development of software for real estate organizations.

Education

09/2006 – 01/2011	PhD in Computer Science at the University of Twente
10/2002 – 03/2005	MSc in Computer Science at the Ca' Foscari University of Venice (Italy)
09/1999 – 09/2002	BSc in Computer Science at the Ca' Foscari Universify of Venice (Italy)

Short Trainings

11/2009	Adavaced SCADA Security Red/Blue Team at the Idaho National Laboratory (Idaho Falls, USA), sponsored by the Department of Homeland Security
07/2008	BCS Professional Certification in Information Risk Management (PCIRM) at the BCS, The Chartered Institute for IT (London, UK)

Research Projects

I participated in the proposal phase as well as the realization phase (sometimes as coordinator of the involved partner) of several national and international research projects.

2014-2017	PREEMPTIVE. EU FP7 project on the protection of critical infrastructure. Cooperation between UTwente, SecurityMatters, AIA, Fraunhofer, HW Communications, University Roma3, ENCS, Israel Electric Corporation, Katolieke Universiteit Leuwen, IREC, Harnser, Vitrociset. 3.8M Euros, duration four years. I was one of the two main scientific contributors. I was the unofficial project coordinator for 1 year due to lack of suitable people from the appointed partner.
2012-2015	CRISALIS. EU FP7 project on the protection of critical infrastructure. Cooperation between Alliander, Chalmers University, Enel, Eurecom, SecurityMatters, Symantec, UTwente, Ulm University, Siemens. 670K Euros, duration four years. I actively participated in the consortium creation and in writing the project proposal. I was the main scientific contributor for SecurityMatters.
2010-2014	Hermes, Castor, Midas. 3 projects on the protection of critical infrastructure. Cooperation between UTwente, Fox-IT, SecurityMatters, ABB, Waternet, Brabant Water, GasUnie, Alliander. Funded by ministry of Internal Affairs. Budget 1.1M Euros, duration, four years. I participated in writing the three project proposals. I was one of the two main scientific contributors for the three projects.
2009 - 2011	SecurityMatters. Phase 2 valorization grant. Funded by STW. I was one of the three writers of the project proposal and prepared all the project evaluation meetings.
2008 - 2009	Atlantides. Phase 1 valorization grant. Funded by STW. I was one of the three writers of the project proposal and prepared all the project evaluation meetings.

Supervision

I was the daily supervisor of:

2013 - 2016	Ali Abbasi (PhD completed). Daily supervisor as part of PostDoc employment at UTwente.
2008 - 2011	Ayse Morali (PhD completed). Supervision tasks during own PhD were coordinated by prof. Sandro Etalle. I also supervised around 15 master thesis projects as PhD student/postdoc at the University of Twente, and while at SecurityMatters. I am currently supervising or co-supervising two master thesis projects at the TU/e, and will begin in November 2021 the daily supervision of a new PhD student.

Awards

SecurityMatters is awarded the *COMMIT Wetenschapsvalorisatieprijs* 2012. The prize is awarded to a person or group that has managed to convert the results of scientific ICT research in the Netherlands into a successful application that is economically or socially beneficial.

Publications

[ID]: Intrusion Detection, [RM]: Risk Management

Non-Academic Conferences

Emmanuele Zambon and Damiano Bolzoni: *NIDS: False Positive Reduction Through Anomaly Detection*. Black Hat USA, Las Vegas, 2006. [ID]

Damiano Bolzoni and Emmanuele Zambon: *Sphinx: An Anomaly-based Web Intrusion Detection System*. Black Hat USA, Las Vegas, 2007. [ID]

Patents

Emmanuele Zambon: *Method and system for classifying a protocol message in a data communication network*. US11012330B2, 2017. [ID]

Daniel Trivellato and Emmanuele Zambon: *Comprehensive risk assessment*. US20200412758A1, 2020. [RM]

Academic

Ali Abbasi, Thorsten Holz, Emmanuele Zambon, Sandro Etalle:
ECFI: Asynchronous Control Flow Integrity for Programmable Logic Controllers. ACSAC 2017. [ID]

Ali Abbasi, Jos Wetzels, Wouter Bokslag, Emmanuele Zambon, Sandro Etalle:
uShield - Configurable Code-Reuse Attacks Mitigation For Embedded Systems. NSS 2017. [ID]

Davide Fauri, Bart de Wijs, Jerry den Hartog, Elisa Costante, Emmanuele Zambon, Sandro Etalle: *Encryption in ICS networks: A blessing or a curse?* SmartGridComm 2017. [ID]

Ali Abbasi, Majid Hashemi, Emmanuele Zambon, Sandro Etalle:
Stealth Low-Level Manipulation of Programmable Logic Controllers I/O by Pin Control Exploitation. CRITIS 2016. [ID]

Caselli, M. and Zambon, Emmanuele and Amann, J. and Sommer, R. and Kargl, F. (2016) *Specification Mining for Intrusion Detection in Networked Control Systems*. In: Proceedings of the 25th USENIX Security Symposium, 10-12 Aug 2016, Austin, TX, USA. pp. 791-806. USENIX Association. ISBN 978-1-931971-32-4. [ID]

Caselli, M. and Zambon, Emmanuele and Kargl, F. (2015) *Sequence-aware intrusion detection in industrial control systems*. In: Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, 14-17 April 2015, Singapore. pp. 13-24. CPSS Workshop - AsiaCCS'15. ACM. ISBN 978-1-4503-3448-8. [ID]

Caselli, M. and Zambon, Emmanuele and Petit, J.Y. and Kargl, F. (2015) *Modeling message sequences for intrusion detection in industrial control systems*. In: Proceedings of the Ninth IFIP 11.10 International Conference on Critical Infrastructure Protection, ICCIP 2015, 16-18 March 2015, Arlington, Virginia, US. pp. 49-71. Critical Infrastructure Protection IX. Springer Verlag. ISSN 1868-4238 ISBN 978-3-319-26566-7. [ID]

Abbasi, A. and Wetzel, J. and Bokslag, W. and Zambon, Emmanuele and Etalle, S. (2014) *On Emulation-Based Network Intrusion Detection Systems*. In: Proceedings of the 17th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 17-19 September 2014, Gothenburg, Sweden. pp. 384-404. Lecture Notes in Computer Science 8688. Springer. ISSN 0302-9743 ISBN 978-3-319-11379-1. [ID]

Hadžiosmanović, D. and Sommer, R. and Zambon, Emmanuele and Hartel, P.H. (2014) *Through the eye of the PLC: semantic security monitoring for industrial processes*. In: ACSAC'14 Proceedings of the 30th Annual Computer Security Applications Conference, 8-12 Dec 2014, New Orleans, LA, USA. pp. 126-135. ACM. ISBN 978-1-4503-3005-3. [ID]

Caselli, M. and Hadžiosmanović, D. and Zambon, Emmanuele and Kargl, F. (2013) *On the feasibility of device fingerprinting in industrial control systems*. In: Critical Information Infrastructures Security, 16-18 Sept 2013, Amsterdam. pp. 155-166. Lecture Notes in Computer Science (8328). Springer. ISSN 0302-9743 ISBN 978-3-319-03963-3. [ID]

Hadžiosmanović, D. and Simionato, L. and Bolzoni, D. and Zambon, Emmanuele and Etalle, S. (2012) *N-gram Against the Machine: On the Feasibility of the N-gram Network Analysis for Binary Protocols.* In: Proceedings of the 15th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2012), 12-14 Sep 2012, Amsterdam, The Netherlands. pp. 354-373. Lecture Notes in Computer Science 7462. Springer Verlag. ISSN 0302-9743 ISBN 978-3-642-33337-8. [ID]

Zambon, Emmanuele and Etalle, S. and Wieringa, R.J. (2012) *A²thOS: availability analysis and optimisation in SLAs* International Journal of Network Management, 22 (2). pp. 104-130. ISSN 1055-7148 *** ISI Impact 0,323 ***. [RM]

Kolesnichenko, A.V. and de Boer, P.T. and Remke, A.K.I. and Zambon, Emmanuele and Haverkort, B.R.H.M.(2011) *Is Quantitative Analysis of Stuxnet Possible?* In: QEST 2011: Fast Abstracts, 5-8 Sep 2011, Aachen, Germany. pp. 9-10. CTIT Workshop Proceedings WP11-03. Centre for Telematics and Information Technology University of Twente. ISSN 0929-0672. [ID]

Zambon, Emmanuele (2011) *Towards Optimal IT Availability Planning: Methods and Tools.* PhD thesis,University of Twente. CTIT Ph.D.-thesis series No. 10-188 ISBN 978-90-365-3102-3. [RM]

Zambon, Emmanuele and Etalle, S. and Wieringa, R.J. and Hartel, P.H. (2011) *Model-based Qualitative Risk Assessment for Availability of IT Infrastructures.* Software and Systems Modeling, 10 (4). pp. 553-580. ISSN1619-1366 *** ISI Impact 1,269 ***. [RM]

Morali, A. and Zambon, Emmanuele and Etalle, S. and Wieringa, R.J. (2010) *CRAC: Confidentiality Risk Assessment and IT-Infrastructure Comparison.* In: Security & Privacy Silver Linings in the Cloud, 25th IFIP International Information Security Conference (SEC 2010). Springer Verlag. [RM]

Morali, A. and Zambon, Emmanuele and Houmb, S.H. and Sallhammar, K. and Etalle, S. (2009) *Extended eTVRA vs. Security Checklist: Experiences in a Value-Web.* In: 31st International Conference on Software Engineering - Companion. IEEE Computer Society Press. [RM]

Morali, A. and Zambon, Emmanuele and Etalle, S. and Overbeek, P. (2008) *IT Confidentiality Risk Assessment for an Architecture-Based Approach.* In: Third IEEE International Workshop on Business-Driven IT Management. IEEE Computer Society Press. [RM]

Zambon, Emmanuele and Bolzoni, D. and Etalle, S. and Salvato, M. (2007) *A model supporting Business Continuity auditing & planning in Information Systems.* In: Second International Conference on Internet Monitoring and Protection (ICIMP. IEEE Computer Society Press. [RM]

Zambon, Emmanuele and Bolzoni, D. and Etalle, S. and Salvato, M. (2007) *Model-Based Mitigation of Availability Risks.* In: Second IEEE/IFIP International Workshop on Business-Driven IT Management. IEEE Computer Society Press. [RM]

Bolzoni, D. and Zambon, Emmanuele and Etalle, S. and Hartel, P.H. (2006) *Poseidon: a 2-tier Anomaly-based Network Intrusion Detection System.* In: 4th IEEE Int. Information Assurance Workshop (IWIA2006). IEEE Computer Society. [ID]