CURRICULUM VITAE ET STUDIORUM
Prof. Dr. Eng. Fabio Massacci
January 2021

Contents

1 PERSONAL AND EMPLOYMENT DATA

1.1 Personal Details

- Name and Surname: **Fabio MASSACCI**
- Nationality: **Italian** Date of Birth: **1967** Sex: **Male** Status: **Married, two children**

1.2 Digital Contacts:

- Web: **https://fabiomassacci.github.io**
- ORCID: **https://orcid.org/0000-0002-1091-8486**
- E-mail: **Fabio.Massacci@ieee.org** Mobile: +39-329-2105004
- UTrento: DISI, Via Sommarive 9, 38123 Trento, IT - Tel: 0461-282086, - Fabio.Massacci@unitn.it
- VUAmsterdam: DCS, De Boelelaan 1111, 1081HV Amsterdam, NL - Tel: 020-59-86098- f.massacci@vu.nl
- Certified Email: fabio.massacci@pec.ording.roma.it

1.3 Present Position:

- 2005/Jan → permanent - Full Professor at University of Trento, Italy
- 2020/Aug→ 2021/Aug - Full Professor in Foundational Security at Vrije Universiteit Amsterdam, Netherlands

1.4 Previous Employments

- 2001/Sep → 2005/Jan - Associate Professor, Faculty of Engineering, University of Trento – Italy
- 1999/Feb → 2001/Aug - Assistant Professor, Faculty of Engineering, University of Siena – Italy
- 1998/Jan → 1999/Feb - Postdoctoral Fellow, CNR, Rome, Italy
- 1997/Nov →1998/Dec –Research Assoc. on project by ASI (Italian Space Agency), U. of Roma "La Sapienza"
- 1994/Nov → 1997/Nov - PhD Fellowship at the University of Rome “La Sapienza”

1.5 Professional Appointments

- 2017/Mar → 2021/Feb - Rector’s delegate for international ranking at UTrento
- 2015/Oct → 2019/Feb – Deputy Head of School, Coordinator of Teaching – Dipartimento Ingegneria e Scienze dell’Informazione – Univ. of Trento.
- 2011/Jan → 2012/Jan – Vice Director for Education – TrentoRISE (EIT – ICTLabs Italy)
- 2002/Mar → 2008/sep – Deputy Rector for ICT Services – University of Trento – Italy
    - Supervision of IT department and its CIO (including performance target), budget 3M€/year, staff 70 people, outsourcing contracts for Metrop. Area Network, ERP system (SAP), and education portal.

1.6 Visiting appointments

- 2020/21 – Winter Term – Institute for Advanced Studies Fellow – Durham University, UK
- 2017/Jun→2017/Jul – ISI University of Southern California – Los Angeles, USA
- 2014/Jun→2016/Jul – (1m/yr) - Durham Business School – Durham, UK
- 2013/Apr→2013/May – Visiting Researcher – KULeuven, Leuven, Belgium
- 2012/Jun → 2012/Aug – DIMACS – special program on Cybersecurity, Rutgers, USA
- 2007/Jan → 2012/Apr – Guest Scientist for the DIGIT Project – SINTEF, Oslo - Norway
- 2005/Jan → 2009/Dec – Guest Scientist for the ENFORCE Project – SINTEF, Oslo – Norway
- 2000/Jun → 2000/Dec - Visiting Researcher - IRIT - CNRS, Toulouse – France
- 1996/Feb → 1997/Feb - Visiting Student, Computer Laboratory, Univ. of Cambridge – UK

1.7 Appointments as Evaluator

- Industry, Finance and Innovation Funding Bodies
    - Enterprise Estonia: 2012 (Research Center Evaluation)
    - Italian Ministry of Economic Development: 2006, 2008, 2011, 2014-20
        - Selection Committee of the National Qualification for the European Digital Innovation Hub
- Foreign Universities and Research Center
    - Full Professor Position - University of Orleans, France
    - Assistant Professor Position - KTH, Sweeden
    - Assistant Professor Position - Vienna Science and Technology (WWTF), Austria
- Research Funding Bodies
    - European Research Council (EU): 2009, 2012, 2015, 2016, 2017
    - Canadian Research Council (CA): 2011, 2014

  - Austrian Research Council (AT): 2011
  - Dutch Research Council (NL): 2005, 2009, 2015, 2016, 2017
  - EU INTAS ex-CIS, Moldova: 2005-2006
  - Estonia Research Council (EE): 2014
  - Flemish Research Council (BE): 2015
  - Georgia Research Council (GE): 2011→2014
  - French Research Council and Foreign Affairs Ministry (FR): 2006
  - UK Research Council (EPSRC), 2015, 2019
- Italian Regional Authorities Funding Bodies
  - Emilia Romagna, Lombardia, Piemonte, Provincia Autonoma di Trento, Sardegna, Veneto

2 DEGREES, AWARDS, ASSESSMENTS AND EVALUATIONS

2.1 Academic degrees (M.Sc., Ph.D., etc.)

- 1998/Jun. - Univ. of Rome I "La Sapienza", PhD in Computer Science and Engineering. Thesis on automated reasoning for modal and security logics
- 1995/Mar. 95 – Master in International Affairs by SIOI and Ministry of Defence. Thesis on the relationship between Democracy and fundamentalist Islam.
- 1993/Nov. 93 - Univ. of Rome "La Sapienza", Master Degree in Computer Engineering. Thesis on automated autoepistemic reasoning.

2.2 Habilitations

- 2003/Dec – Habilitation as full professor
- 1999/Mar - Habilitation as United Nations Officer – Level P2
- 1995/Mar - Ordine degli Ingegneri – Habilitation as Chartered Engineer

2.3 Scientific Awards.

- 2015/Aug – **Ten Years Most Influential Paper Award** by IEEE Requirements Engineering Conference for the paper: P. Giorgini, F. Massacci, J. Mylopoulos, N. Zannone: Modeling Security Requirements Through Ownership, Permission and Delegation. In *Proc. of IEEE Requirements Engineering'05,* p. 167-176, IEEE Press 2005.
- 2012/Jul – Best paper award at the IEEE International Conference on Cyber Security (CyberSecurity)
- 2001/Sep. – "Intelligenza Artificiale" career award by the Italian Association of Artificial Intelligence (AI*IA) for young researchers in AI under 35

3 SUMMARY OF SCIENTIFIC ACHIEVEMENTS

3.1 Summary of Publications and Citations

3.1.1 Summary of publications (Data on 2021/Jan)

- Recent years highlights in *Computing (CORE/ERA)*:
  - IEEE Transactions of Software Engineering (A*), ACM Transactions on Information and System Security (A), Empirical Software Engineering Journal (A), Journal of Systems and Software (A), ACM Symposium on Principles of Programming Languages (A*), IEEE Symposium on Security and Privacy (A*), International Conference on Software Engineering (A*), ACM/IEEE Internat. Symp. on Empirical Software Engineering and Measurement (A)
- Recent years highlights in *Business and management (CABS/Academic Journal Guide)*:
  - Risk Analysis (4)
- Recent highlights in *Professional security conferences*
  - BlackHat USA, BlackHat Asia
- Raw Data (according to Scopus)
  - Journal Papers: 70 (21 in the past 5 years)
  - Conference and Workshop papers: 165 (28 in the past 5 years)
  - Edited Books and Journals: 15 (2 in the past 5 years)
  - Professional Peer-reviewed Journal Article: 2
  - Book Chapters: 6

- Italian Books: 2
- Patents: 1 (3 submitted in 2018)

3.1.2 Summary of citation data

- Google Scholar (gC_ZVPgAAAAJ) Total Citations: 7.559 – Past 5 years: 2.120 – h-index: 46
- Elsevier Scopus (55167501300) Total Citations: 3.558 – Past 5 years: 1.128 – h-index: 32
- WoS Researcher ID (C-2662-2012) Total Citations: 1.620 – Past 5 years: 701 – h-index: 20

3.2 Summary of Appropriated Grants and Industry Impact

3.2.1 Summary of grants (as PI)

- EU Pilot on CyberSecurity Network and Centre (Site leader) UniTN Funding: 0.45M€
- EU Projects as Admin. EU Coordinator: 2 STREPs and 1 IP,1H2020 UniTN Funding: 2.55 M€
- EU Projects as Scientific Coordinator: 1 IP UniTN Funding: 0.92M€
- EU projects as Site Leader: 2 IP, 1 NoE, 2 CSA, 2 EIT(*) UniTN Funding: 1.61M€
- National Projects as site leader: 1 MIUR, 1PAT, 1 ASI UniTN Funding: 0.27M€
- Industry Grants: 2 EU, 1 National, 1 International UniTN Funding: 0.60M€

(*) Excluding EIT funding for teaching I&E in security courses

3.2.2 Industrial Impact

- Contributed to CVSS – Common Vulnerability Scoring Systems – *The* World Standard on vulnerabilities
- Work on risk- vs rule-based regulation presented by National Grid to the UK Cabine Office and EU Presidency

3.3 Summary of Supervised PhD students and Post-doc researchers

3.3.1 Summary of supervised collaborators

- Graduated PhD students: 13 (BG, BY, ID, IT, UA, VN)
  - Started but dropped: 2 (BY, IT), changed advisor: 1 (IN), changed university: 2 (CO, BR)
- Current Phd students: 3 (VN, IT)
- Past Postdoctoral researchers: 9 (CN, DE, FR, KR, ID, IT, RU)
- Current PostDoctoral researchers: 2 (RU,VN)

3.3.2 Current position of past collaborators

- Assistant professor, dozent, lecturer, and full professor: 7 (in CH, CN, DK, IT, NL)
  - DTU (1), TU Eindhoven (2), UIBE (1), ULeiden (1), UVerona (1), ZAHW (1)
- Researcher at research centers: 3 (CNR – IT, INRIA - FR, KIPA - KR)
- International companies: 6 (ATOS, Bosch, Bromium, Forescout, Google, WorldQuant)
- Public administration: 1 (CA)
- Senior developer in SME: 1 (IT)
- Post-doctoral researchers: 5 (CA, ID, LU, NL)

3.3.3 Awards of PhD Students

- I. Pashchenko, 2017, 2nd place at ESEC/FSE SRC Graduate Student Competition
- M. S. Tran, 2016. CAiSE PhD Award for Best Doctoral Dissertation
- L. Allodi, 2016. University of Trento Best Doctoral Dissertation

4 SELECTED RESEARCH HIGHLIGHTS –ONE'S LIFE IN 3 PAGES

I illustrate below some of the major milestones in my research with some sample papers. They are not necessarily the most cited; they are the ones that one could actually read to have a comprehensive idea of my research.

In Vivo Experimental Security: My current research effort is to ***empirically validate how security solutions works in the real world*** when users and developers interact. Often security solutions stop at a mathematical model or laboratory experiment (in vitro) or might just be validated as pure computing programs (in silico), I think we must go the last mile and empirically understand the trade-off in risk and opportunities that make sure that a technical solution will work in practice. They might be just ***satisficing solutions,*** in the sense of the Nobel Laureate Herbert Simon, but this is what actually exists. This requires also to understand the economics implication of our choices (which is my second point below). This is also the result of a long standing collaboration with SAP. Three very recent papers illustrate this research, in flagship computer security venue and software engineering venues. A paper in a business journal is currently under submission (R&R).

P1. Pashchenko, I., Vu, D.-L., Massacci, F. A Qualitative Study of Dependency Management and Its Security Implications. *Proceedings of the ACM Conference on Computer and Communications Security (ACM CCS)*, pp. 1513-1531. (2020). Finding a home for this paper was far from trivial as a reviewer put it. At first, it was a classical piece of social science research with semi-structured interviews, coding by Atlas.ti and quotations from developers from several different countries from Asia to Europe. Second, its message was not aligned with the current religious credo that updates are a good thing. Its purpose was to shed light on the motivations behind security and dependency managements choices and emerged clearly that there are a lot of reason for such updates not to be good.

P2. Pashchenko, I., Plate, H., Ponta, S. E., Sabetta, A., & Massacci, F. Vulnerable open source dependencies: counting those that matter. In *Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement ESEM* 2018. Several papers studied the FOSS Ecosystem for vulnerabilities and always conclude that we are in very dire state of practice because we have many vulnerabilities and the developers cannot do anything as such vulnerabilities are introduced by obscure third party libraries. In this paper we review the claims from an industry perspective and by a correct calculation show that several libraries were directly chosen by the developers (and thus they could do something) and finally that several vulnerabilities where never there..

P3. Massacci. F, Pashchencko I. Technical Leverage in a Software Ecosystem: Development Opportunities and Security Risks. Conditionally Accepted for the *Proceedings of the IEEE Conference on Software Engineering (ICSE 2021)*, (2021). This is the first paper ever to introduce an actual metric (Technical Leverage), similar to the notion of Financial Leverage that capture quantitatively why using third party dependencies pays off (you ship a project whose code is 4x times your own code and pay a small delay of two extra days in interval between releases) and the corresponding security risk (ship 4x times your code base and the odds of shipping a vulnerable code increases by 60%). This comparison captures the full extent of the moral hazard that we are facing now as a community.

Empirical Security Economics: For a security solution to be practical and for an attack to be credible they both needs to be *affordable* security solution, albeit they might not be perfec (see above for the satisficing concept). Focusing on the affordable (for the bad and the good guys) often go against the "ethos" of academic security research working to protect us against an all powerful adversary, yet it has an unfettered potential of industry impact (you can better prioritize your finite resources protecting a against a threat that exists, instead of pretending to fight a Sith Lord that doesn't exist). Three papers illustrate this research, two in flagship computer security venue and one in a top business journal.

P4. Allodi, L, Massacci, F. Comparing vulnerability severity and exploits using case-control studies. *ACM Trans. on Information and System Security*, 17(1):1 (2014). The conference version was rejected several times (ICSE, CCS, ESORICS, etc.) because "It is just bad scholarship to suggest that one should not worry about all vulnerabilities". People in industry knew better (they invited us at BlackHat USA 2013), as they know too well that their budget is fixed and therefore the academic advice of worrying about all vulnerabilities is useless. We looked at data from Symantec and black markets, combined it with solid mathematical research on statistics and risk reduction and we identified the vulnerabilites one should worry about. The outcome made up to the CVSS world standard. Out of this research we also made available to the community several databases licensed to Fraunhofer, MITRE, NCSU, MIT Sloan, MIT Lincoln Lab among others.

P5. De Gramatica, M., Massacci, F., Shim, W., Turhan, U. & Williams, J. (2016). Agency Problems and Airport Security: Quantitative and Qualitative Evidence on the Impact of Security Training. *Risk Analysis 2017.* This paper evaluates which type of security training is most effective for airport security officers (training costs

>900€/person). We have a solid model based on principal-agent theory and validated it with interviews with high profile stakeholders. We transformed a "gut feeling" into an actionable model. The results were presented to ACI Europe, the federation of European Airport Directors.

P6. Massacci, F., Ngo, C. N., Nie, J., Venturi, D., & Williams, J. FuturesMEX: secure distributed futures market exchange. *Proceedings of IEEE Symposium on Security and Privacy. 2018.* This is a joint paper with economists and cryptographers: how to run a exchange like the Chicago Mercantile Exchange in a distributed fashion. We solved an already solved problem (an exchange is just an example of multi party computation - MPC), except that we did in a way that it was solvable with real empirical data. By using MPC even from top theory papers not only running a small market like Lean Hog trades would have required an year to just run a day of trading, but, to add insult to injury, retail and institutional investors (who only do 20% of the trades) would have had to spend 80% of the overall computational resources to allow high-frequency traders to place speculative orders that would have then been almost immediately canceled. When my business colleague J. Williams presented the paper and our patents in China to hedge funds he expected 20 people. He had 200.

Security Requirements Engineering: I started this work in 2003 with N. Zannone and J. Mylopoulos. The key idea is to develop a robut methodology to capture security requirements as first class citizens. Two, very different, ten-years apart, papers illustrate this research: initially I worked on design and formal reasoning capabilities, now understanding what really works in security risk analysis is the other focus in my research that complements it.

P7. Giorgini P., Massacci F., Mylopoulos J., Zannone N., "Requirements Engineering for Trust Management: Model, Methodology, and Reasoning". *Int. J. of Information Security*, 5(4):257-274, 2006. The short version of this paper appeared in IEEE RE'2005 and received in 2015 the Ten Years Most Influential Paper Award by the IEEE Requirements Engineering Conference. In this paper we designed a security methodology to capture security requirements, an underlying formalization in terms of logic programs and a verification methodology that would check whether desirable security properties would be satified.

P8. De Gramatica M, Labunets K, Massacci F, Paci F, Tedeschi A. The Role of Catalogues of Threats and Security Controls in Security Risk Assessment: An Empirical Study with ATM Professionals. In *Proc. of the Int. Conf. on Req. Engineering: Foundation for Software Quality (REFSQ)*. 2015. So, we invented a "super-duper" security requirements method, why did industry not flock to adopt it? Since 2010, I have been experimenting to understand what works in practice. For example, in this paper with an industry co-author, we focus on catalogues: academic methods never have them, industry works with catalogues of several hundred pages (eg the NIST-800-x and ISO-2700x). They *do* make the difference between novices and experts. Understanding what makes a research method empirically usable by somebody else than its inventor is the pre-requisite for successful innovation.

Run-time and load-time security enforcement. This research is a mixture of theoretical research on the limit of what can be actually enforced and what can be practically achieved. Out of this research stream started my long standing collaboration with KU Leuven (F. Piessens and Wouter Josen).

P9. Ngo M., Massacci F., Milushev D., Piessens F.. "Runtime Enforcement of Security Policies on Black Box Reactive Programs". In *Proc. of the 42nd ACM Symp. on Principles of Progr. Lang.. POPL'2015*. This paper summarizes the theoretical investigation on the limit and power of run-time enforcement mechanisms. With another students, N. Bielova we investigated the limits of edit automata (IJIS, JCS and POLICY'11) showing that practical enforcement cannot be simply caputred by the two basic concept of transparency and soundness.

P10. Desmet L, Joosen W., Massacci F., Philippaerts P., Piessens F., Siahaan I., Vanoverberghe D. Security-by-contract on the .NET platform. *Inform. Security Technical Rep.*13 (1):25-32, Jan 2008. This is one of the first papers describing the formal security checking of apps on a mobile phones. It is a comprehensive paper spannign from theory to implementation. We could run a checker testing whether an app respected some security policies. On the same year US researchers proposed at CCS to use very simple checks on android apps and could onlyuse the manifest of the app, we used real code. Our industry partner of the S3MS project, DoCoMo, licensed the industrial application in Japan and I tried to negotiate with Vodafone Itay its commercialization. Alas, .NET and Microsoft lost to Android…

P11. Koshutanski H., Massacci F.: Interactive access control for autonomic systems: From theory to implementation. *ACM Trans. on Autonomous and Autonomic Systems* 3(3): 2008. H. Koshutanski was my first "own" phd student in 2002 and started his research with a workshop paper that got significantly more citations than this final "round-up" journal. This paper summarizes our work on trust negotiation in which we combined a solid theory (abduction) with a running implementation (an opens source is available at http://www.interactiveaccess.org). This research is basically the only academic background of Microsoft's patent US8060920 and Apple's patent US8813185B2 on the dynamic management of users' credentials.

Formal Methods for Security: In 1996, half-way through my Phd, I went to Cambridge to work with Robin Milner (one of the inventor of the Hennessy-Milner logic). Alas, Milner had just been elected head of department and suggested I could work with Roger Needham and Larry Paulson who had a joint project on modal logic for security. This "one year long mishap" gave a whole new turn to my research career.

P12. Bella G., Massacci F., Paulson L.C,: Verifying the SET Purchase Protocols. *J. of Automated Reasoning* 36(1-2):5-37, 2006. This paper describes the first work ever of verification of a major industrial protocol. Up to that point most of the formal security verification papers where about breaking and fixing academic protocols whose description could fit in a single page. Security researchers woud claim that formal methods could not scale. SET (Secure Electronic Transactions) was VISA's and Mastercard's protocol for the web. Its specification was thicker than a dictionary. We proved it correct and put to rest any claim that formal methods could not scale, but the effort in terms of time and person months was far from push-button technologies...

P13. Massacci F., Marraro L., "Logical Cryptanalysis as a SAT-Problem: Encoding and Analysis of the U.S. Data Encryption Standard". *Journal of Automated Reasoning*, 24(1-2):165-203, 2000. This research stemmed from a crazy idea I had when I returned from Cambridge. In the AI and formal method community SAT solvers were the new research fad that seemed to crack previously unsolvable problems. At the end of the day what is a cryptoraphic circuit? Just a big boolean formula. What is a cryptanalysis problem? Just a bit SAT problem. The devil is of course in the detail and managing to encode symmetric and public key crypto was far easy (for the latter it appeared in Discrete Applied Mathematics). We failed to crack real crypto and that time but SAT competitions still use crypto benchmarks today but Marc Stevens SHA-1 cracking in 2017 used a SAT solver of a MSc Student of mine (V. Nossum) as a major component..

Automated Resoning for Modal Logic: When I started my Phd, reasoning in modal logic was divided in two fields: those that purely manipulate formulas and those that manipulated the corresponding models. I tried to combine both ideas to get something better than both. The tableaux for modal and description logics that I did as single author or with a couple of colleagues revamped the area.

P14. Massacci F., "Single Step Tableaux for Modal Logics". *Journal of Automated Reasoning*, 24(3): 319-364, 2000. In the Handbook of Tableaux Methods (1999) the chapter on modal tableaux by Gorè devotes 30 pages to my CADE paper of the mid 90s (the journal version is the one reported here). In 2014 our works in the area are still cited. My greatest satisfaction is a paper in the volume in memoriam of H. Ganzinger by R. Schmidt and U. Hustadt, the recognized advocates of the scientific competitor of tableaux (translation+resolution). Their paper "First-Order Resolution Methods for Modal Logics" is a survey with 90+ citations. There are only 2 citations for tableaux: the handbook above and one of my papers. I left the field 15 years ago and a citation by a scientific "enemy" to a paper 10 years old is truly "l'honneur des armes".

5 SCIENTIFIC ACTIVITIES

5.1 Appropriated Grants as PI

Research activities, in particular applied security research, require funding and I have secured a significant amount of funding for the projects I have been involved with. I intend to keep seeking funding at all levels as empirical and applied research cannot be done without a significant amount of human resources. Only projects for which I'm the project leader are listed. I participate to other projects as Co-PI but they are no listed.

5.1.1 Research council funds.

- MIUR-PRIN-TENACE 2014-16 - Protecting National Critical Infrastructures from Cyber Threats – (site leader) - Trento Funding 93K€. Basic research national project funded by Ministry of Education, University and Research.
- MIUR-FIRB-SECURITY 2004-06 - Automatic Verification of Internet Security Protocols – (site leader) - Trento Funding 92K€. Basic research national project funded by Ministry of Education, University and Research.

5.1.2 Funding from EU

- EU-H2020-AssureMOSS --- **Assurance and certification in secure Multi-party Open Software and Services**– Trento Funding 460K€, Vrije Universiteit Funding 360K
- EU-H2020-Pilot-CyberSec4EU --- Cyber Security Network of Competence Centres for Europe – Trento Funding 450K€
- EU-H2020-CA-OPTICS2 --- Observation Platform for Technological and Institutional Consolidation of research in Safety and Security – Trento Funding 90K€
- EU-EIT-UNBIAS-2018 --- Blockchain for Supply Chain Management – Trento Funding 150K€
- EU-EIT-VAMOSS-2016 --- Vulnerability Analysis and Management for Open-Source Software – Trento Funding 80K€
- EU-FP7-SEC-CP-SECONOMICS- 2012-2015 – Socio-Economics meets Security (EU Coordinator) – total 3.4M€ - Trento funding 700K€
- EU-FP7-IST-CA-SECCORD-2012-2015 - Security and Trust Coordination and Enhanced Collaboration – Trento funding 120K€
- EU-FP7-IST-NoE-NESSOS - 2010-2014 - Network of Excellence on Engineering Secure Future Internet Software Services and Systems - Trento funding 273K€
- EU-FP7-IST-CA-EFFECTSPLUS-2009-2013 - European Framework for Future Internet – Compliance, Trust, Security and Privacy through effective clustering – Trento funding 80K€
- EU-FP7-FET-IP-SecureChange 2009-2012- Security Engineering for Lifelong Evolvable Systems- (EU Coordinator) – Total Funding 5.1M€ - Trento funding 710K€
- EU-FP7-IST-IP-MASTER 2008-2010- Managing Assurance, Security and Trust for Services - (EU Scientific Coordinator, from Y2 passed site leadership to B. Crispo) – Trento funding 920K€
- EU-FP6- IST-STREP S3MS 2006-08 –Security of Software and Services for Mobile Systems (EU Admin Coordinator) - Total funding 2.4M € - Trento funding 401K€
- EU-FP6- IST-IP SERENITY 2006-08 –Security and Dependability Engineering – Trento 586K€

5.1.3 Funding from trade, industry and public authorities

- SAP – 2018 – 1year PhD Fellowship – 17K€
- CISCO-Digital Innovation WP4- 250K€
- PosteItaliane-CyberSecurityDistrict-2015-2016 – Defining a qualitative and quantitive model for the assessment of possible impact scenarios in relation to threat agents - 35K€
- EuroControl-SESAR-INNOVATE-2015-2016 – Support to SESAR B.5 Framework for Integration of Performance data into EATMA models – Trento Funding 60K€
- EuroControl-SESAR-WPE-EMFASE-2013-2015 – Empirical Framework for Security Design and Economic Tradeoff – (EU Coordinator) -- Total 557K€ - Trento Funding 250K€
- PAT-FU-MOSTRO 2004-2007 - Modelling Sec. and Trust Relationships within Organizations - 81K€- Project from the local government.
- ASI-DOVES 2003 - On-board Autonomy: a platform for the Development Of VErified Software – 29K€ - Project from the Italian Space Agency

5.2 Organization of international conferences

- Founder and Steering Committee Member of Conferences and Workshop

  - QoP – Quality of Protection Workshop (now MetriSec) (2005→2014). This became a standard workshop co-located with the ACM ESEM conference.
  - ESSoS – International Symposium on Engineering Secure Software and Systems (2009→now). This is a joint effort with W. Joosen.
  - IJCAR – International Joint Conference on Automated Reasoning (2001-2003).
- Program Chair of
  - REFSQ'17 – STM Track Requirements Engineering, Foundations for Software Quality
  - ESSoS 2009-2010 – International Symposium on Engineering Secure Software and Systems
  - IEEE SSIRI 2011- International Conference on Secure Software Integration and Reliability Improvement
  - IEEE NTMS 2008 - New Technologies, Mobility and Security
- Program committee member of many conferences and workshops among them AAAI, CADE, CSFW, ESORICS, ICSE, IEEE GlobeCom Security).

5.3 Editorial assignments in international periodicals.

- Department Editor:
  - IEEE Security and Privacy Magazine ("Building Security In") - now
- Associate Editor:
  - International Journal of Information Security
- Special Issue Editor:
  - Information Software Technology
  - Journal of Computer Security on "EU funded Security Research",
  - Science of Computer Programming

5.3.1 Review / referee assignments by the above

- AIJ; C&S, DMKD, IandC, IJIS, JAR, JoSS, JSL, TISSEC, TPDS, TSE, TWEB, TIFS, etc.

5.4 Assignments as public examiner/opponent

- Katholieke University of Leuven
  - Pieter Philippaerts (advisor F. Piessens, W. Joosen) – 2010
- University of Innsbruck
  - Berthold Agreiter (Advisor R. Breu) - 2011
- University of Siena
  - Pierluigi Falilla (Advisor M. Barni) – 2011
- Technical University of Berlin
  - Jan Nordholz (Advisor J.P. Seifert) -- 2017
- University of Twente
  - André van Cleeff (advisors R. Wieringa) – 2015
  - Emanuele Zambon (advisors S. Etalle, R. Wieringa) – 2011
  - Ayse Morali (advisors S. Etalle, P. Hartel) – 2011
  - Marnix Dekker (Advisor S. Etalle, P. Hartel) - 2009

5.5 Contribution to Industrial Innovation and Policy Making

5.5.1 CVSS FIRST Standardization Group

- Thanks to our work on vulnerabilities that was published in BlackHat in 2013 we were invited to participate to the FIRST standardization group (www.first.org CVSS-SIG) that will determine the next rating of the Common Vulnerability Scoring System (CVSS), an industry standard whose impact affects almost all governments and private industries. For example, the PCI DSS standard for credit card payments requires that all vulnerabilities with a score higher than 4 be patched; the US Government mandated the use of CVSS for any configuration management software.
- In May 2014 the standard group approved UNITN proposal for the scores for Attack Complexity as a part of the standard. Luca Allodi, my PhD student and co-author in this endeavour, is among the 23 authors of the standard. I am still non voting member part of the CVSS SIG.

5.5.2 Government Policy

- In 2015 our research findings for policy makers on the trade-off between risk-based and rule-based regulations for cyber security have been presented to the UK Cabinet office by National Grid UK, the major electricity

transmission provider in the UK and in the Eastern part of the US. It has been presented again at a high-level meeting on the security of the power grid organized by the EU Presidency Council in early 2016.

5.5.3 Own contacts with companies

- Throughout my research project I have developed a number of contacts ith people from the R&D department of the major IT companies (IBM, SAP, and ATOS). Through these contacts I have occasionally got funding for some of my PhD students to visit them or discussed applications of our technologies to their products.
- For example, a patent application for the TestRex framework described in the Usenix CSET paper [C21] has been filed by SAP.
- I secured a pro-bono access to SYMANTEC's database summarizing their Global Intelligence Network (240K+ sensors in over 200 countries) where Symantec monitors attack activity and gathers malicious code intelligence from 130M+ client, server, and gateway systems running its antivirus products, and its distributed honeypot network with 2.5M+ decoy accounts. [J13,C1]

6 TEACHING AND SUPERVISION

I illustrate below some of the raw numbers of my teaching experience. More details, and in particular my teaching strategy, are available in the ***Research and Teaching Statement***.

6.1 Summary of BSc and MSc Courses

					Assist.		Assoc.				Full Professor					
		Univ.	**#ECTS**	**#Studs**	**99**	**00**	**01**	**02**	**03**	**04**	**05**	**06**	**07**	**08-10**	**11-12**	**14-20**
Master	ICT Innovation	Trento	9	30												**EN**
	Lab on Offensive Technologies	Trento	12	25												**EN**
	Cyber Security Risk Assessment	Trento	6	40												**EN**
	Security Engineering	Trento	6	25									**EN**	**EN**	**EN**	
	Computational Complexity	Trento	6	75									**EN**	**EN**	**EN**	
	Security (introduction to)	Trento	6	15				IT	IT	IT	**EN**	**EN**				
	EGov Security & Privacy	Trento	3	10										**EN**		
	Scientific Programming	Trento	3	100						IT	IT	IT				
	Network Security	Trento	6	50					IT	IT	IT					
	Digital Design (TA)	Siena	12	100	IT											
Bachelor	Programming II	Trento	6	150				IT								
	Op. Sys. and Security	Trento	6	10				IT	IT	IT	IT	IT				
	O.O. Programming	Trento	6	100			IT	IT		IT						
	Progr. and Comp. Graphics	Trento	6	150			IT	IT	IT							
	Compilers	Siena	6	20	IT	IT										
	Progr. and Comp. Graphics	Rome	6	50	IT	IT										

TA = as teaching assistant, 6 ECTS = approx. 48h Lectures (30% by a TA). IT = in Italian, EN=In English

6.2 Tutorials and Lectures at International Schools and Events

I have also held a number of invited tutorials at conferences and PhD Schools. One must show the broad picture hile giving enough technical details so that attendees get a grasp of the underlying complexity.

- IEEE ISSRE-2014, ESSOS-2015 (Jointly with L. Allodi, L)
- IEEE ISI-11 (jointly with Y. Asnar)
- BPM-08 (jointly with Y. Asnar and P. Giorgini)
- ESSLI-05 (jointly with H. Koshutanski who gave the lecture as I could not make it for personal reasons)
- FOSAD-00, 03, 05, 11 (6 hours in 2011)
- IEEE RE-06 (jointly with J. Mylopoulos and N-Zannone)
- TABLEAUX-98

Among the invited particpation at Dagstuhl Seminars:

- 2019
- 2016 Invited keynote at Seminar Assessing ICT Security Risks in Socio-Technical Systems (Other Keynotes A. Sasse, R. Anderson, R. Boeheme).

- 2009-16 Invited on automated reasoning, evolving requirements, and security topics. Twice in 2010 and 2012.

6.3 MSc Degree Project Works.

A thesis in Trento runs for around 24ETC (+6ECTS of internship at a company or University lab and then the thesis). I only report a subset of the theses.

- Giorgio Di Tizio (2017) – "Drive-by Download Attacks as a Stackelberg Planning Problem" – joint Thesis with R. Kunnemann at CISPA (DE).
- Elia Geretto (2017) – "A QBDI-based Fuzzer Targeting Magic Bytes Comparisons" – EIT MS, Double Degree with UTwente, (Thesis at Quarkslab, FR now PhD Student with H. Bos at VUA).
- Qiao Zhongying (2016) – "Security Impact Modelling and Analysis using Quantitative Incident Data for Large Financial Institutions" – (EIT MS, now PhD student at NYU).
- Nikki Mark Battin (2016) – "Economic benefits of running a Bug Bounty program" – EIT MS, now security researcher at Atlassian (AU).
- Martin Podzena (2016) – "Collecting Actionable Threat Intelligence from Digital Underground" – EIT MS, Double Degree with TU Berlin.
- Yared Semu (2016) – "Analysis and Comparison of Source Code to distinguish between Vulnerable and Secure Releases of Open Source Libraries" – industry sup. H. Plate (SAP Research - FR)
- Yesuf Ahmed (2013) – "A Computer-Aided Context Aware Attack Tree Modeling Approach for Software Development" – industry sup. M. Kohler (SAP Research - DE)
- Alexander Garaga (2012) – "Architecture Based Threat Modelling" –industry sup. A. Schaad (SAP Research - DE) .- now a PhD student at SAP Research (FR)
- Sarila Rana (2011) – "Security Issue of Online Storage System and Usability Testing of OpenArgument tool" – internship at Open University
- Lisong Guo (2011) - "Towards Automated Security Testing of Web-Based Applications" – industry sup. L. Compagna (SAP Research - FR) – now PhD at Univ. Pier and Marie Curie, France.
- Mikhail Borozdin (2011) - "Architecture-Based Threat Analysis" – industry sup. A. Schaad SAP Research, DE)

6.4 Graduated Doctoral students.

- 2001/Nov → 2005/ Mar Hristo Koshutanski (senior researcher – ATOS)
  - Title: Interactive Access Control for Autonomic Systems
  - Funded by a Education Ministry Grant
- 2003/Nov →2007/Feb Nicola Zannone (Associate prof. - Univ. of Eindhoven)
  - Title: A Requirements Engineering Methodology for Trust, Security, and Privacy
  - Seconding supervisor: John Mylopoulos
  - Funded by MIUR-FIRB-ASTRO
  - **Ten Years Most Influential Paper 2015 for paper published at RE'05**
- 2003/Nov →2007/Feb Natallia Rasadka (senior developer –GPI Group , IT)
  - Title: Generalized XML Security Views
  - Co-supervisor: G. Kuper
  - Funded by a University Grant
- 2004/Nov →2009/Mar Artsiom Yautsiukhin (researcher - CNR – Pisa)
  - Title: A Framework for Quantitative Security Analysis of Complex Business Systems
  - Funded by EU-IP-SERENITY/MASTER
- 2005/Nov →2009/Mar Katsyarina Naliuka (software engineer – Google, CH)
  - Title: Security Run-Time Monitoring for Mobile Devices
  - Funded by MIUR-FIRB-SECURITY
- 2005/Nov → 2010/Mar Ida S.R. Siahaan (research assoc. – New Brunswick Univ., CA)
  - Title: Security-by-Contract using Automata Modulo Theory
  - Funded by a University Grant
- 2006/Nov→2011/Nov Nataliia Bielova (researcher 1st class– INRIA)
  - Title: A theory of constructive and predictable runtime enforcement mechanisms
  - Funded by a University Grant
- 2009/Nov→ Jan/2014 Le Minh Sang Tran (quant researcher – Yandex, VN)
  - Title: Managing the Uncertainty of the Evolution of Requirements Models
  - Funded by EU-NoE-NESSOS
  - **CAiSE PhD Award 2016 for Best Dissertation**
- 2009/May→Mar/2014 Viet Hung Nguyen (software architect, Bosch, VN)

  - Title: Empirical Methods for Evaluating Vulnerability Models
  - Funded by a University Grant
- 2011/Nov →Apr/2015 Luca Allodi (assistant prof – Univ. of Twente, NL)
  - Title: Risk-based vulnerability management
  - Funded by a University Grant
  - **UNITN PhD Award 2016 for Best Dissertation**
- 2011/Nov →Apr/2015 Katsyarina Labunets (post-doc – TU Delft, NL)
  - Title: Empirical Comparison of Security Risk Assessment Methods
  - Funded by a University Grant and the EMFASE Project
- 2011/Nov →Apr/2015 Minh Ngo Nguyen (post-doc – Stevens Institute, US)
  - Title: A Programmable Enforcement Framework for Security Policies
  - Funded by a University Grant
- 2013/Nov →May/2016 Stanislav Dashenski (post-doc – Univ- Lux, LU)
  - Title: Security Assessment of Open Source Third-Parties Applications
  - Funded by an EU industrial doctorate with SAP
- 2014/Nov →Sep/2019 Ivan Pashchencko (Research Assistant Prof. – UTrento, LU)
  - Title: "Decision Support of Security Assessment of Software Vulnerabilities in Industrial Practice"
  - Funded by a University Grant and the VAMOSS Project
- 2014/Nov →Oct/2019 Chan Nam Ngo (post-doc – UTrento)
  - Title: Secure, Distributed Financial Exchanges: Design and Implementation
  - Funded by a University Grant, the SECONOMICS project and the UNBIAS project

6.5 Post-doctoral Researchers

- Aida Saidane (PhD Toulouse, FR) (security expert – Revenu Quebec, CA)
- Nicola Dragoni (PhD Bologna, IT) (full prof. - Örebro Univ., SE, and assoc. prof DTU, DK)
- Stephan Neuhaus (PhD Saarland, DE) (dozent – Zurich Univ. of App. Sci., CH)
- Yudis Asnar (PhD Trento, IT) (academic assistant –ITB, ID)
- Olga Gadyatskaya (PhD Novosibirsk, RU) (post-doc. - Univ. of Luxembourgh, LU)
- Vadim Kotov (PhD Ufa, RU) (senior researcher – Bromium, US)
- Federica Paci (PhD Milano, IT) (Associate professor - Univ. of Verona, IT)
- Wooyun Shim (PhD Michigan State, US) (researcher – KIPA, KR)
- Jing Nie (PhD Durham Business School, UK) (Asssist professor, - Bejing Univ. of Econ. and Buiness)

6.6 Doctoral students at present being supervised

- 2017/Nov → Duc Ly (On automated vulnerability repairs)
- 2017/Nov → Ganbayar Uuganbayar (on cyberinsurance jointly with Fabio Martinelli, CNR)
- 2018/Nov → Giorgio Di Tizio (on Advanced Persistent Threats)
- 2020/Nov → Francesco Minna (On Run-time security, jointly with Bala Chandrasekaran, VU)

7 ADMINISTRATIVE ASSIGNMENTS

7.1 Administration of education.

- 2016 → 2019 – Coordinator of Teaching – Dip. Ingegneria e Scienze dell'Informazione – Univ. of Trento.
- 2009→2012: Director of Studies for Computer Science BSc and MSc, Univ. of Trento
- 2010→2012: Vice-Director for Education of the Trento node of ICT-Labs, the European Institute of Innovation and Technology.

7.2 Research unit leadership

- 2001-now: I coordinated my own research group that is funded by the projects that I have been able to secure. This makes 2-5 post-docs and 5-8 PhD students.
- 2001-2003: I coordinated the Software Engineering Research group: 5 member of staff, their post-doc and phd-students. This is means acting as a negotiator on behalf of the group towards the department for what concerns spaces, doctoral students and other resources.

7.3 Membership of university boards or councils.

- 2017→ 2021: Rector's delegate for international ranking

- 2015→ 2019: Deputy Head of School “Ingegneria e Scienze dell’Informazione”
- 2009→2012: Executive Committee of the Faculty of Science at the University of Trento as elected representative of the CS members of staff
- 2002→2009: deputy rector for ICT procurements and services, University of Trento.

7.4 Other expert and leadership assignments of significance

- 2019→ now:Member of the Executive Committee of the National CyberSecurity Laboratory of CINI (the Italian Consortium of Computer Science and Engineering Universities)
- 2001→2005 Elected Member of the National Committee of the Italian Association for Artificial Intelligence. I was also Treasurer till 2003
- 1992 →96 European Treasurer of Service Civil International, a non-governmental organization with consultative status at UNESCO, Council of Europe and the European Youth Forum. My responsibility included setting the budget for the European Secretariat located in Antwerpen, and negotiate its approval by the 20 European member states organizations. I coordinated the lobby activities towards the EC.
- 1993/Nov →1994/Nov – Compulsory Civil Service

8 FULL LIST OF PUBLICATIONS

8.1 Papers published in international peer-reviewed journals

J1. Pashchenko, I., Plate, H., Ponta, S.E., Sabetta, A., Massacci, F. Vuln4Real: A Methodology for Counting Actually Vulnerable Dependencies. ***IEEE Transactions on Software Engineering***, 2021 Appeared as online first in 2020

J2. Uuganbayar, G., Yautsiukhin, A., Martinelli, F., Massacci, F. Optimisation of cyber insurance coverage with selection of cost effective security controls. *Computers and Security*, 2021, 101. To Appear

J3. Allodi, L., Cremonini, M., Massacci, F., Shim, W. Measuring the accuracy of software vulnerability assessments: experiments with students and professionals. ***Empirical Software Engineering***, 25 (2):1063-1094. (2020)

J4. Kuper, G., Massacci, F., Shim, W., Williams, J. Who Should Pay for Interdependent Risk? Policy Implications for Security Interdependence Among Airports. ***Risk Analysis***, 40 (5), pp. 1001-1019. (2020)

J5. Massacci, F., Ngo, N.C. Distributed Financial Exchanges: Security Challenges and Design Principles. *IEEE Security and Privacy*, (2020)

J6. Pape, S., Paci, F., Jürjens, J., Massacci, F. Selecting a secure cloud provider-an empirical study and multi criteria approach. *Information*, 2020, 11 (5), (2020)

J7. Dashevskyi, S., Brucker, A.D., Massacci, F. A Screening Test for Disclosed Vulnerabilities in FOSS Components. ***IEEE Transactions on Software Engineering***, 2019, 45 (10): 945-966.

J8. Dashevskyi, S., dos Santos, D.R., Massacci, F., Sabetta, A. TestREx: a framework for repeatable exploits. *International Journal on Software Tools for Technology Transfer*, 21 (1), pp. 105-119. (2019). See Patent

J9. Giaretta, A., Dragoni, N., Massacci, F. IoT security configurability with security-by-contract. ***Sensors***, 19 (19), art. no. 4121, (2019)

J10. Massacci, F. Is "deny Access" a Valid "fail-Safe Default" Principle for Building Security in Cyberphysical Systems? IEEE Security and Privacy, 17 (5), (2019)

J11. Pham, D.-P., Vu, D.-L., Massacci, F. Mac-A-Mal: macOS malware analysis framework resistant to anti evasion. *Journal of Computer Virology and Hacking Techniques*, 2019, 15 (4), pp. 249-257. (2019) Presented at **BlackHat Asia**

J12. Van Ginkel, N., De Groef, W., Massacci, F., Piessens, F. A Server-Side JavaScript Security Architecture for Secure Integration of Third-Party Libraries. *Security and Communication Networks*, 2019.

J13. Vu, D.-L., Nguyen, T.-K., Nguyen, T.V., Nguyen, T.N., Massacci, F., Phung, P.H. HIT4Mal: Hybrid image transformation for malware classification. *Transactions on Emerging Telecommunications Technologies*, 31 (11), (2019)

J14. Allodi, L., & Massacci, F. Security events and vulnerability data for cybersecurity risk estimation. ***Risk Analysis***, 37(8), 1606-1627. 2018

J15. Riaz, M., King, J., Slankas, J., Williams, L., Massacci, F., Quesada-López, C., & Jenkins, M. (2017). Identifying the implied: Findings from three differentiated replications on the use of security requirements templates. ***Empirical Software Engineering***, 22(4), 2127-2178. 2017

J16. de Gramatica, M., Massacci, F., Shim, W., Turhan, U., & Williams, J. Agency problems and airport security: Quantitative and qualitative evidence on the impact of security training. ***Risk Analysis***, 37(2), 372-395. 2017.

J17. Labunets, K., Massacci, F., Paci, F., Marczak, S., & de Oliveira, F. M. Model comprehension for security risk assessment: An empirical comparison of tabular vs. graphical representations. ***Empirical Software Engineering***, 22(6), 3017-3056. 2017. *Invited at ICSE 2018* as a Journal First Presentation.

J18. Nguyen, V. H., Dashevskyi, S., & Massacci, F. An automatic method for assessing the versions affected by a vulnerability. ***Empirical Software Engineering***, 21(6), 2268-2297. 2016

J19. Allodi L, Corradin M, Massacci F. Then and Now: On The Maturity of the Cybercrime Markets. The lesson black-hat marketeers learned. *IEEE Transactions on Emerging Topics in Computing*. 2016.

J20. Elliott, K., Massacci, F., Williams, J. Action, Inaction, Trust, and Cybersecurity's Common Property Problem. *IEEE Security and Privacy* 14(1):82-86 (2016).

J21. Massacci, F., Ruprai, R., Collinson, M., Williams, J. Economic Impacts of Rules-versus Risk-Based Cybersecurity Regulations for Critical Infrastructure. *IEEE Security and Privacy* 14(3):52-60 (2016)

J22. De Gramatica, M., Massacci, F., Shim, W., Tedeschi, A., Williams, J. IT Interdependence and the Economic Fairness of Cybersecurity Regulations for Civil Aviation. *IEEE Security and Privacy* (2015)

J23. Allodi, L, Massacci, F. Comparing vulnerability severity and exploits using case-control studies. ***ACM Transactions on Information and System Security***, 17(1):1 (2014).

J24. Gadyatskaya O, Massacci F, Zhauniarovich Y. Security in the Firefox OS and Tizen mobile platforms. *IEEE Computer* 47(6):57-63 (2014).

J25. Massacci F, Paci F, Tran LMS, Tedeschi A. Assessing a requirements evolution approach: Empirical studies in the air traffic management domain. ***Journal of Systems and Software***, 95:70-88 (2014).

J26. Massacci F, Nguyen VH. An Empirical Methodology to Evaluate Vulnerability Discovery Models. ***IEEE Transactions on Software Engineering***. 40(12):1147-1162 (2014)

J27. Bielova N., Massacci F. Iterative enforcement by suppression: Towards practical enforcement theories. *Journal of Computer Security* 20(1):51-79 (2012)

J28. Dragoni, N., Gadyatskaya, O., Massacci, F., Philippov, A. High-level algorithms and data structures requirements for security-by-contract on Java cards *International Journal of Critical Computer-Based Systems*, 3(4):284-304 (2012)

J29. Asnar Y., Massacci F., Saïdane A., Riccucci C., Felici M., Tedeschi A., El Khoury P., Li K., Seguran M., Zannone N.: Organizational Patterns for Security and Dependability: From Design to Application. *International Journal of Secure Software Engineering* 2(3):1-22 (2011)

J30. Bielova N., Massacci F.: Do you really mean what you actually enforced? - Edited automata revisited. . *International Journal of Information Security* 10(4):239-254 (2011)

J31. Karsai G., Massacci F., Osterweil L.J., Schieferdecker I.: Evolving Embedded Systems. *IEEE Computer* 43(5):34-40 2010.

J32. Compagna L., El Khoury P., Massacci F., Saïdane A.: A Dynamic Security Framework for Ambient Intelligent Systems: A Smart-Home Based eHealth Application. *Transactions on Computational Science* 10:1-24 (2010)

J33. Bielova N., Dragoni N., Massacci N., Naliuka K., Siahaan I.: Matching in security-by-contract for mobile code. *Journal of Logic and Algebraic Programming* 78(5):340-358, (2009)

J34. Compagna L., El Khoury P., Krausová A., Massacci F, and Zannone N..How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns. *Artificial Intelligence and Law Journal* 17(1):1-30, 2009.

J35. Dragoni N., Massacci F., Walter T., Schaefer C.. What the Heck is this application doing? - A security-by-contract architecture for pervasive services, *Computer & Security* 28(7):566-577 2009.

J36. Dragoni N., Massacci F., Saïdane A. A self-protecting and self-healing framework for negotiating services and trust in autonomic communication systems. ***Computer Networks*** 53(10):1628-1648 2009

J37. Kuper G.M., Massacci F., Rassadko N.. Generalized XML security views. *International Journal of Information Security* 8(3): 173-203 2009

J38. Desmet L, Joosen W., Massacci F., Philippaerts P., Piessens F., Siahaan I., Vanoverberghe D., Security-by-contract on the .NET platform. *Information Security Technical Report* 13 (1):25-32, Jan 2008.

J39. Koshutanski H., Massacci F.: Interactive access control for autonomic systems: From theory to implementation. ***ACM Transactions on Autonomous and Autonomic Systems*** 3(3): 2008.

J40. Kohutanski, H., Massacci F.: A Negotiation Scheme for Access Rights Establishment in Autonomic Communication. *Journal of. Network and System. Managements* 15(1):117-136 2007.

J41. Massacci F., and Mylopoulos J., Zannone N. Computer-aided Support for Secure Tropos. ***Automated Software Engineering***. 14(3): 341-364, 2007

J42. Massacci F., Mylopoulos J., Zannone N., "From Hippocratic Databases to Secure Tropos: a Computer-Aided Re-Engineering Approach". *International Journal of Software engineering and Knowledge Engineering*, 17(2):265-284, 2007.

J43. Bella G., Massacci F., Paulson L.C,: Verifying the SET Purchase Protocols. ***Journal of Automated Reasoning*** 36(1-2):5-37, 2006.

J44. Dobson S., Denazis S., Fernández A., Gaïti D., Gelenbe E., Massacci F., Nixon P., Saffre F., Schmidt N., Zambonelli F.: A survey of autonomic communications. ***ACM Transactions on Autonomous and Autonomic Systems*** 1(2):223-259, 2006

J45. Giorgini P., Massacci F., Mylopoulos J., Zannone N., "Requirements Engineering for Trust Management: Model, Methodology, and Reasoning". *International Journal of Information Security*, 5(4):257-274, 2006.

J46. Massacci F., Mylopoulos J., Zannone N., "Hierarchical Hippocratic Databases with Minimal Disclosure for Virtual Organizations". In ***VLDB Journal***, 15(4): 370-387. 2006.

J47. Bella G., Massacci F., Paulson L. C., "Overview of the Verification of SET". *International Journal on Information Security*, 4(1-2):17-28. 2005

J48. Massacci F., Prest M., Zannone N., "Using a Security Requirements Engineering Methodology in Practice: the compliance with the Italian Data Protection Legislation". *Computer Standards & Interfaces*, 2005, v. 27, n. 5, p. 445-455.

J49. Bella G., Massacci F., Paulson L. C., "Verifying the SET registration protocols**". *IEEE Journal on Selected Areas in Communications***, 21(1):77-87, 2003.

J50. Fiorini C., Massacci F., Martinelli E., "How to fake an RSA signature by encoding modular root finding as a SAT problem". *Discrete Applied Mathematics*, 130(2): 101-127, 2003.

J51. Carlucci Aiello L., Massacci F., "Verifying security protocols as planning in logic programming". *ACM Transactions on Computational Logic*, 2(4):542-580. 2001.

J52. De Giacomo G., Massacci F., "Combining deduction and model checking into tableaux and algorithms for Converse-PDL.". ***Information and Computation***, 162:117-137, 2000.

J53. Donini F. M., Massacci F., "EXPTIME Tableaux for ALC". ***Artificial Intelligence Journal***, 124(1): 87-138, 2000.

J54. Massacci F., "The Complexity of Analytic and Clausal Tableaux". *Theoretical Computer Science*, 243(1-2): 477-487, 2000.
J55. Massacci F., "Single Step Tableaux for Modal Logics". ***Journal of Automated Reasoning***, 24(3): 319-364, 2000
J56. Massacci F., Marraro L., "Logical Cryptanalysis as a SAT-Problem: Encoding and Analysis of the U.S. Data Encryption Standard". ***Journal of Automated Reasoning***, 24(1-2):165-203, 2000.
J57. Massacci F., "Tableaux Methods for Formal Verification in Multi-agent Distributed Systems". *Journal of Logic and Computation*, 8(3):373-400, 1998.

8.2 Patents

P1. Sabetta, A., Compagna, L., Ponta, S., Dashevskyi, S., Dos Santos, D., & Massacci, F. (2017). "Multi-context exploit test management." U.S. Patent No. 9,811,668. Washington, DC: U.S. Patent and Trademark Office.
P2. Massacci, F., Ngo, C. N., Nie, J., Venturi, D., & Williams, J (2018). "A method and apparatus for distributed, privacy- and integrity-preserving exchange, inventory and order book.". Submitted as US Patent and EU Patent.
P3. Massacci, F., Ngo, C. N., Nie, J., Venturi, D., & Williams, J (2018). "A Secure Transaction System". Submitted a UK Patent with WTO option.

8.3 Edited Books and Journals

E1. Baik J., Massacci F., Zulkernine M. eds. Special section on software reliability and security. *Information & Software Technology 54(12): 1376 (2012).*
E2. Baik J., Massacci F., Zulkernine M. eds. *Proceedings of the 5th International Conference on Secure Software Integration and Reliability Improvement.* IEEE, 2011.
E3. F. Massacci, D. Wallach, Zannone N. eds. *Proceedings of the 2nd International Symposium on Engineering Secure Software and Systems (ESSoS'10)*. LNCS 5965, Springer Verlag 2010.
E4. Camenisch J., Lopez J., Massacci F., Ciscato M., Skordas T. Special issue on EU-funded ICT research on trust and security. *Journal of Computer Security*. 18(1), IOS Press 2010.
E5. Massacci F., Redwine S., Zannone N. eds.. *Proceedings of the 1st International Symposium on Engineering Secure Software and Systems (ESSoS'09)*. LNCS 5429, Springer Verlag 2009.
E6. Aggarwal A., Badra M., Massacci F. eds.. *Proceedings of New Technologies, Mobility and Security Conference and Workshops (NTMS 2008)*: 2008, IEEE Press.
Massacci F., Piessens F., Mauw S.. Special Issue on Security and Trust for Mobile and Embedded Systems. *Science of Computer Programming*. 74(1), Elsevier 2008.
E7. L. Compagna, V. Lotz, F. Massacci.eds. *Proc. of the ERCIM Security and Trust Management Workshop.(STM'07)* ENTCS, Elsevier, 2007.
E8. G. Karjoth, F. Massacci eds. *Proc. of the 2nd Workshop on Quality of Protection: Security measurements and metrics.* ACM Press, 2006.
E9. F. Massacci, F. Piessens eds.. *Proc. of the 1st Workshop on Run-time Monitoring for Embedded and Mobile Systems (REM'07)*- ENTCS, Elsevier, 2007.
E10. Gollmann, D; Massacci, F.; Yautsiukhin, A. eds. *Proc. of the 1st Quality of Protection: Security Measurements and Metrics*. Springer, 2006
E11. Stølen, K., Winsborough W.H., Martinelli F., Massacci F. eds.. *Trust Management, Proceedings of the 4th International Conference, iTrust 2006*, Pisa, 2006. LNCS 3986. Springer Verlag.

8.4 Professional Refereed Journals

PJ1. Asnar Y., Lim H. W., Massacci F., Worledge C. Realizing Trustworthy Business Services Through a New GRC Approach. In *ISACA Journal (Online edition)*. April 2010.
PJ2. Lotz V., Pigout E., Fischer P.M., Kossmann D., Massacci F., Pretschner A. Towards Systematic Achievement of Compliance in Service-Oriented Architectures: The MASTER Approach. *Wirtschaftsinformatik* 50(5): 383-391 2008

8.5 Invited Book Chapters

BC1. Allodi, L., Biagioni, S., Crispo, B., Labunets, K., Massacci, F., & Santos, W. Estimating the assessment difficulty of CVSS environmental metrics: An experiment . *Proceedings of FDSE 2017*
BC2. de Gramatica M, Massacci F, Gadyatskaya O. An Empirical Study of the Technology Transfer Potential of EU Security and Trust R&D Projects. *Cyber Security and Privacy - 3rd Cyber Security and Privacy EU Forum Revised and selected papers*. volume 470 of Communications in Computer and Information Science, Springer 2014.
BC3. Scandariato R., Paci F., Tran L.M:S., Labunets K., Yskout K., Massacci F., Joosen W. "Empirical Assessment of Security Requirements and Architecture: Lessons Learned". In: *Engineering Secure Future Internet Services and Systems*, volume 8431 of LNCS, Springer, 2014
BC4. Asnar Y., Massacci F.: A Method for Security Governance, Risk, and Compliance (GRC): A Goal-Process

Approach. FOSAD 2011:152-184

BC5. Massacci F. and Zannone N.. Detecting Conflicts between Functional and Security Requirements with Secure Tropos: John Rusnak and the Allied Irish Bank. In *Social Modeling for Requirements Engineering*. MIT Press, 2010.

BC6. Dragoni, N. Martinelli F., Massacci F., Mori P., Schaefer C., Walter T., Vetillard E.. Security-by-Contract (SxC) for Software and Services of Mobile Systems. In *At Your Service – Selected Papers on EU research on Software and Services*. MIT Press 2008.

BC7. Koshutanski H. and Massacci F.. Interactive Access Control with Trust Negotiation for Autonomic Communication. In *Advances in Enterprise Information Technology Security*. Chap. VII, p.120-148, IGI Global, 2007.

BC8. Massacci F., Mylopoulos J., and Zannone N.. An Ontology for Secure Socio-Technical Systems. In *Handbook of Ontologies for Business Interaction*. Chap. IX, p. 188-206 IGI Global, 2007.

BC9. Giorgini P., Massacci F., Zannone N., "Security and Trust Requirements Engineering". In *Foundations of Security Analysis and Design III: Tutorial Lectures*. In Aldini A., Gorrieri R., Martinelli F. (eds), Springer, 2005, p. 237-272. , Lecture Notes in Computer Science, 3655;

BC10. Carlucci Aiello L., Massacci F., "Planning attacks to security protocols: case studies in logic programming". In *Computational logic: logic programming and beyond : essays in honor of Robert A. Kowalski*, Springer, 2002. p. 533-560

BC11. Massacci F. and Marraro L.. Logical cryptanalysis as a SAT-problem: Encoding and analysis of the U.S. Data Encryption Standard. In *SAT-2000: Highlights of Satisfiability Research at the Year 2000*, vol. 63 of Frontiers in AI and Applications, p. 343-376. IOS Press, 2000. Essentially the same as the JAR Paper.

8.6 Peer Reviewed International Conferences and Workshops

C1. Di Tizio, G., Massacci, F., Allodi, L., Dashevskyi, S., Mirkovic, J. An Experimental Approach for Estimating Cyber Risk: A Proposal Building upon Cyber Ranges and Capture the Flags. *Proceedings - 5th IEEE European Symposium on Security and Privacy Workshops*, Euro S&PW 2020, art. no. 9229652, pp. 56-65. (2020)

C2. Ngo, C.N., Friolo, D., Massacci, F., Venturi, D., Battaiola, E. Vision: What If They All Die? Crypto Requirements for Key People. *Proceedings of the 5th IEEE European Symposium on Security and Privacy Workshops*, Euro S&PW 2020, art. no. 9229860, pp. 178-183 2020.

C3. Pashchenko, I., Vu, D.-L., Massacci, F. A Qualitative Study of Dependency Management and Its Security Implications ***Proceedings of the ACM Conference on Computer and Communications Security (ACM CCS)***, pp. 1513-1531. (2020)

C4. Pashchenko, I., Vu, D.-L., Massacci, F. Preliminary Findings on FOSS Dependencies and Security : A Qualitative Study on Developers' Attitudes and Experience. *Poster at the 2020 ACM/IEEE 42nd International Conference on Software Engineering: Companion, ICSE-Companion* 2020, art. no. 9270337, pp. 284-285. (2020).

C5. Vu, D.-L., Nguyen, T.-K., Nguyen, T.V., Nguyen, T.N., Massacci, F., Phung, P.H.. A convolutional transformation network for malware classification. *Proceedings of 6th NAFOSTED Conference on Information and Computer Science*, NICS 2020 art. no. 9023876, pp. 234-239.

C6. Vu, D.L., Pashchenko, I., Massacci, F., Plate, H., Sabetta, A. Towards Using Source Code Repositories to Identify Software Supply Chain Attacks. *Poster at Proceedings of the ACM Conference on Computer and Communications Security*, pp. 2093-2095.

C7. Vu, D.-L., Pashchenko, I., Massacci, F., Plate, H., Sabetta, A. Typosquatting and Combosquatting Attacks on the Python Ecosystem. Proceedings - *5th IEEE European Symposium on Security and Privacy Workshops*, Euro S&PW 2020, art. no. 9229803, pp. 509-514 (2020)

C8. Battaiola, E., Massacci, F., Ngo, C.N., Sterlini, P. Blockchain-based invoice factoring: From business requirements to commitments. Proc. of the Distributed Ledger Technology Workshop (DLT'19). CEUR Workshop Proceedings.

C9. Friolo, D., Massacci, F., Ngo, C.N., Venturi, D. Affordable security or big guy vs small guy: Does the depth of your pockets impact your protocols? *Proceedings of the International Security Protocols Workshop*. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 12287 LNCS, pp. 135-147.

C10. Geretto, E., Tessier, C., Massacci, F. QBDI-based fuzzer taming magic bytes. *Proc. of ITASEC* 2019. CEUR Workshop Proceedings 2019

C11. Giaretta, A., Dragoni, N., Massacci, F. Protecting the Internet of Things with Security-by-Contract and Fog Computing. IEEE 5th World Forum on Internet of Things, WF-IoT 2019 - Conference Proceedings, (2019).

C12. Uuganbayar, G., Massacci, F., Yautsiukhin, A., Martinelli, F. Cyber insurance and time-to-compromise: An integrated approach. International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2019, art. no. 8899442,

C13. Allodi, L., Cremonini, M., Massacci, F., Shim, W. et al. "The Effect of Security Education and Expertise on Security Assessments: the Case of Software Vulnerabilities." *Workshop on Economics of Information Security* (WEIS) 2018.

C14. Massacci, F., Ngo, C. N., Nie, J., Venturi, D., & Williams, J. FuturesMEX: secure distributed futures market exchange. ***Proceedings of IEEE Symposium on Security and Privacy***. *2018*.

C15. F Massacci, CN Ngo, D Venturi, J Williams. Non-monotonic Security Protocols and Failures in Financial Intermediation. *Proceedings of the International Security Protocols Workshop* 2018

C16. Pashchenko, I., Plate, H., Ponta, S. E., Sabetta, A., & Massacci, F. Vulnerable open source dependencies: counting those that matter. In ***Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*** **ESEM** 2018

C17. Allodi L, Massacci F. "Attack Potential in Impact and Complexity." *Proceedings of the 12th International Conference on Availability, Reliability and Security*. ACM, 2017.

C18. Allodi L, Massacci F, Williams J. The Work-Averse Cyber Attacker Model. Evidence from two million attack signatures. *Presented at WEIS 2017.*

C19. Labunets, K., Massacci, F., & Tedeschi, A.. Graphical vs. tabular notations for risk models: On the role of textual labels and complexity. ***Proceedings of the 12th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement ESEM'17***, 2017.

C20. Massacci, F., Ngo, C. N., Nie, J., Venturi, D., & Williams, J. (2017). The seconomics (security-economics) vulnerabilities of decentralized autonomous organizations. *Proceedings of SPW'17*.

C21. Pashchenko, I., Dashevskyi, S., & Massacci, F. (2017). Delta-bench: Differential benchmark for static analysis security testing tools. ***Proceedings of ESEM'17***

C22. Labunets, K., Massacci, F. On the Equivalence Between Graphical and Tabular Representations for Security Risk Assessment. *In Proc. of the 23rd Internat. Conf. on Requirements Engineering: Foundation for Software Quality (REFSQ).* 2017

C23. Davanian, A., Massacci, F., & Allodi, L. (2017). Diversity: A poor man's solution to drone takeover. Paper presented at Proceedings of PECCS 2017.

C24. Dashevskyi, S., Brucker, A.D., Massacci, F. On the security cost of using a free and open source component in a proprietary product. *Proceedings of ESSO'16.* LNCS 9639, pp. 190-206 (2016) . Revised and extended version in Proceedings of WEIS'18

C25. Allodi L, Massacci F. The Work-Averse Attacker Model. In *Proceedings of the 2015 European Conference on Information Systems (ECIS)*. 2015

C26. de Gramatica M, Labunets K, Massacci F, Paci F, Tedeschi A. The Role of Catalogues of Threats and Security Controls in Security Risk Assessment: An Empirical Study with ATM Professionals. *In Proceedings of the 21st Internat. Conf. on Requirements Engineering: Foundation for Software Quality (REFSQ).* 2015

C27. Labunets, K., Paci, F., Massacci, F. Which security catalogue is better for novices? *Proceedings of 5th International Workshop on Empirical Requirements Engineering, EmpiRE 2015* (2016).

C28. Ngo M., Massacci F., Milushev D., Piessens F.. "Runtime Enforcement of Security Policies on Black Box Reactive Programs". *In* ***Proceedings of the 42nd Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)***. 2015

C29. Zhauniarovich Y, Ahmad M, Gadyatskaya O, Crispo B, Massacci F. StaDynA: Addressing the Problem of Dynamic Code Updates in the Security Analysis of Android Applications. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy (CODASPY)*. 2015

C30. Dashevskyi S, Dos Santos DR, Massacci F, Sabetta A. TestRex: a Testbed for Repeatable Exploits. In *Proceedings of the 7th Usenix Workshop on Cyber Security Experimentation and Test (CSET)*. 2014. This work has been protected by a IPCT Patent Application by SAP AG.

C31. De Groef W, Massacci F, Piessens F. NodeSentry: least-privilege library integration for server-side JavaScript. In *Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC)*. 2014

C32. Giacalone M, Mammoliti R, Massacci F, Paci F, Perugino R, Selli C. Security triage: an industrial case study on the effectiveness of a lean methodology to identify security requirements. In ***Proceedings of the 8th ACM/IEEE International Symposium on Empirical Software Engineering (ESEM)***. 2014

C33. Giacalone M, Massacci F, Paci F, Mammoliti R. Perugino R, Selli C. Security triage: A report of a lean security requirements methodology for cost-effective security analysis. *Proceedings of the 4th IEEE International Workshop on Empirical Requirements Engineering (EmpiRE)* 2014.

C34. Labunets K, Paci F, Massacci F, Ruprai RS. An experiment on comparing textual vs. visual industrial methods for security risk assessment. In *Proceedings of the 4th IEEE International Workshop on Empirical Requirements Engineering (EmpiRE)*. 2014

C35. Massacci F, Paci F, Solhaug B, Tedeschi A. EMFASE - An Empirical Framework for Security Design and Economic Trade-off. *Proceedings of the 9th International Conference on Availability, Reliability and Security (ARES)*. 2014.

C36. Shim W, Massacci F, Tedeschi A, Pollini A. A Relative Cost-Benefit Approach for Evaluating Alternative Airport Security Policies. In *Proceedings of the 9th International Conference on Availability, Reliability and Security (ARES)*. 2014.

C37. Ngo M, Massacci F. Programmable enforcement framework of information flow policies. In *Proceedings of the*

15th Italian Conference on Theoretical Computer Science (ICTCS). 2014

C38. Tran LMS, Massacci F. An Approach for Decision Support on the Uncertainty in Feature Model Evolution. In ***Proceedings of the 22nd International Requirements Engineering Conference*** *(RE)*, 2014 IEEE, 93-102. 2014

C39. Labunets K, Massacci F, Paci F., Tran LMS. An Experimental Comparison of Two Risk-Based Security Methods. *In* ***Proceedings of the ACM/IEEE International Empirical Software Engineering and Measurement*** *(ESEM)*, 2013

C40. Allodi L, Massacci F.. HoW CVSS is DoSSing your patching policy and wasting your money. ***BlackHat USA 2013***. Whitepaper available as ArXiv report

C41. Gadyatskaya, O., Massacci, F. Controlling application interactions on the novel smart cards with security-by-contract (2013), 7866 LNCS, pp. 197-215.

C42. Kotov, V., Massacci, F. Anatomy of exploit kits: Preliminary analysis of exploit kits as software artefacts. *Proc. of ESSOS*, 7781 LNCS, pp. 181-196. 2013.

C43. Labunets, K., Massacci, F., Paci, F., Tran, L.M.S. An experimental comparison of two risk-based security methods. ***Proc. of International Symposium on Empirical Software Engineering and Measurement*** *(ESEM)*, pp. 163-172. (2013).

C44. Nguyen, V.H., Massacci, F. The (un)reliability of NVD vulnerable versions data: An empirical experiment on Google Chrome vulnerabilities (2013) *Proceedings of ASIA CCS 2013*, pp. 493-498.

C45. Shim, W., Massacci, F., De Gramatica, M., Tedeschi, A., Pollini, A. Evaluation of airport security training programs: Perspectives and issues. *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*, pp. 753-758.

C46. Allodi, L., Massacci, F. A preliminary analysis of vulnerability scores for attacks in wild: The EKITS and SYM datasets (2012) *Proceedings of the BADGERS' Workshop, ACM Conference on Computer and Communications Security*, pp. 17-24.

C47. Allodi, L., Massacci, F. The dark side of vulnerability exploitation: A proposal for a research analysis (2012) *CEUR Workshop Proceedings*, 834, pp. 71-76.

C48. Massacci, F., Paci, F. How to select a security requirements method? A comparative study with students and practitioners (2012) *Proc. of NordSec*, 7617 LNCS, pp. 89-104.

C49. Gadyatskaya, O., Massacci, F., Philippov, A. Security-by-contract for the OSGi platform (2012) Proc. of *IFI-SEC*, 376 AICT, pp. 364-375.

C50. Paci, F., Massacci, F., Bouquet, F., Debricon, S. Managing evolution by orchestrating requirements and testing engineering processes (2012) *Workshop Proceedings - IEEE 5th International Conference on Software Testing, Verification and Validation, ICST 2012*, pp. 834-841.

C51. Massacci, F., Nagaraj, D., Paci, F., Tran, L.M.S., Tedeschi, A. Assessing a requirements evolution approach: Empirical studies in the Air Traffic Management domain (2012) 2012 *2nd IEEE International Workshop on Empirical Requirements Engineering, EmpiRE 2012 - Proceedings*, pp. 49-56.

C52. Nguyen, V.H., Massacci, F. An independent validation of vulnerability discovery models. (2012) *ASIACCS 2012*, pp. 6-7.

C53. Philippov, A., Gadyatskaya, O., Massacci, F. Security of the OSGi platform (2012) *CEUR Workshop Proceedings*, 834, pp. 11-16.

C54. Shim, W., Allodi, L., Massacci, F. Crime pays if you are just an average hacker (2013) *Proceedings of the 2012 ASE/IEEE International Conference on Cyber Security, CyberSecurity 2012*, art. no. 6542527, pp. 62-68.

C55. Asnar Y., Li T., Massacci F., Paci F.: Computer Aided Threat Identification. *Proc. of CEC'11*. p. 145-152. IEEE 2011.

C56. Bergmann G., Massacci F., Paci F., Tun T.T., Varró D., Yu Y.: A Tool for Managing Evolving Security Requirements. *Proc. of CAiSE Forum'11*. p. 49-56. Springer LNBIP 2011.

C57. Bergmann G:, Massacci F., Paci F., Tun T.T., Varró D., Yu Y.: SeCMER: A Tool to Gain Control of Security Requirements Evolution. *Proc. of ServiceWave'11*: Springer. pp 321-322

C58. Bielova N., Devriese D.,Massacci F., Piessens F.: Reactive non-interference for a browser model. *Proc. of NSS'11*. p 97-104. IEEE 2011.

C59. Bielova N., Massacci F.: Computer-Aided Generation of Enforcement Mechanisms for Error-Tolerant Policies. ***Proc. of POLICY'11***. p. 89-96. IEEE 2011.

C60. Bielova N., Massacci F.: Predictability of Enforcement. In *Proc. of ESSoS'11*. Springer p 73-86

C61. Dragoni N., Lostal E., Gadyatskaya O., Massacci F., Paci F.: A Load Time Policy Checker for Open Multi-application Smart Cards. *Proc. of POLICY'11*. p. 153-156. IEEE 2011.

C62. Gadyatskaya O., Lostal E., Massacci F.: Load Time Security Verification. *Proc. of ICISS'11*. p 250-264. Springer 2011

C63. Joosen W., Lopez J., Martinelli F., Massacci F.: Engineering Secure Future Internet Services. *Proc. of Future Internet Assembly'11*. pp. 177-192. IOS Press 2011.

C64. Massacci F., Bouquet F., Fourneret E., Jürjens J., Lund M.S., Madelénat S., Muehlberg J.T., Paci F., Paul S., Piessens F., Solhaug B., Wenzel S.: Orchestrating Security and System Engineering for Evolving Systems -

(Invited Paper). *Proc. of ServiceWave'11*: pp. 134-143

C65. Massacci F., Mylopoulos J., Paci F., Thein T. T., Yijun Y.: An Extended Ontology for Security Requirements. *Proc. of CAiSE Workshops'11*. p. 622-636. Springer LNBIP 2011.

C66. Massacci F., Neuhaus S., Nguyen V.H.: After-Life Vulnerabilities: A Study on Firefox Evolution, Its Vulnerabilities, and Fixes. In *Proc. of ESSoS'11*. Springer p 195-208, 2011

C67. Tran L.M.S., Massacci F.: Dealing with Known Unknowns: Towards a Game-Theoretic Foundation for Software Requirement Evolution. ***Proc. of CAiSE'11***. p. 62-76. Springer 2011.

C68. Massacci F., Mylopoulos J., Zannone Z.: Security Requirements Engineering: The SI* Modeling Language and the Secure Tropos Methodology. In *Advances in Intelligent Information Systems 2010*. p. 147-174. Springer 2010.

C69. Dragoni N., Gadyatskaya O., Massacci F.: Can We Support Applications' Evolution in Multi-application Smart Cards by Security-by-Contract? In *Proc. of WISTP'10*. pp.221-228 . Springer 2010.

C70. Asnar Y., Felici M., Massacci F., Tedeschi A., Yautsiukhin A.. Quantitative assessment for organisational security & dependability. *Proc. of DEPEND'09*. p. 40-45, 2009.

C71. Bielova N., Massacci F., Micheletti A.: Towards Practical Enforcement Theories. *Proc. of NordSec'09* p. 239-254, Springer 2009.

C72. Desmet L., Joosen W., Massacci F., Naliuka K., Philippaerts P., Piessens F., Vanoverberghe D.. The S3MS.NET Run Time Monitor. Tool Demonstration. *ENTCS* 253(5):153-159, 2009.

C73. Krausova A., Massacci F., Saidane A.. How to capture and use legal patterns in IT. *Proc. of ICAIL'09.* p. 228-229, ACM Press, 2009.

C74. L.A. Lopez, F. Massacci, N. Zannone. Goal-equivalent secure business process re-engineering. *Proc. of . SemSOC*. LNCS 4907, p. 212-223, Springer 2009.

C75. D. Marino, F. Massacci, A.Micheletti, N. Rassadko, S. Neuhaus: Satisfaction of Control Objectives by Control Processes. *Proc. of ICSOC/ServiceWave'09*: 531-545, ACM Press, 2009

C76. F. Massacci, K. Naliuka: Towards practical security monitors of UML policies for mobile applications. *Proc. of ARES Workshops'08*. p. 1112-1119, 2008.

C77. F. Massacci, F. Piessens, I. Siahaan: Security-by-contract for the future internet. *Proc. of FIS'09*. LNCS 5468. p. 29-43, Springer 2009.

C78. F. Massacci, G. Tsudik, A. Yautsiukhin: Logging key assurance indicators in business processes. *Proc. of ASIACCS'09*. p 364-367, ACM Press, 2009.

C79. A. Benameur, F. Massacci, N. Rassadko. Security views for outsourced business processes. *Proc. of SWS'08*. p. 45-52, ACM Press 2008.

C80. N. Bielova, F. Massacci: Do you really mean what you actually enforced? : Edit automata revisited. *Proc. of FAST'08*. LNCS 5491, p. 287-301, Springer 2009.

C81. N. Dragoni, F. Massacci, K. Naliuka: An inline monitoring system for .NET mobile devices. *Proc. of IFIPTM'08*. 363-366, 2008.

C82. F. Massacci, I. Siahaan. Simulating Midlet's Security Claims with Automata Modulo Theory. In *Proc. of PLAS'08*. May 2008 Tucson (USA), p 1-19, ACM Press, 2008.

C83. F. Massacci, N. Zannone. A model-driven approach for the specification and analysis of access control policies. In *Proc. of OTM Conferences'08*, vol.2, LNCS 5332, p1087-1103, Springer 2008.

C84. Y. Asnar, R. Bonato, P. Giorgini, F. Massacci, V. Meduri, C. Ricucci and A. Saidane, Secure and Dependable Patterns in Organizations: An Empirical Approach. In ***Proc. of IEEE RE'07 – Industry Paper Track***, October 2007, New Delhi (IN), pp. 287-292 IEEE Press 2007.

C85. Y. Asnar, P. Giorgini, F. Massacci, N. Zannone: From Trust to Dependability through Risk Analysis. In *Proc. of ARES'07*. p. 19-26 IEEE Press 2007.

C86. G. Bella, S. Bistarelli, F. Massacci. Retaliation: Can We Live with Flaws? In *Proc. of NATO Advanced Research Workshop in Security*, IOS Press, 2007.

C87. L. Compagna, P. El Khoury, F. Massacci, R. Thomas, N. Zannone: How to capture, model, and verify the knowledge of legal, security, and privacy experts: a pattern-based approach. In *Proc. of ICAIL'07*, p. 149-154. ACM Press, 2007.

C88. L. Desmet, W. Joosen, F. Massacci, K. Naliuka, P. Philippaerts, F. Piessens, D. Vanoverbergh: A flexible security architecture to support third-party applications on mobile devices. In *Proc. of CSAW'07*. p. 19-28 ACM Press 2007.

C89. N. Dragoni, F. Massacci: Security-by-contract for web services. In *Proc. of SWS'07*. p. 90-98 ACM Press 2007.

C90. N. Dragoni, F. Massacci, K. Naliuka, I. Siahaan: Security-by-Contract: Toward a Semantics for Digital Signatures on Mobile Code. In *Proc. of EuroPKI 2007*. LNCS, 4582, p. 297-312 Springer, 2007.

C91. N. Dragoni, F. Massacci, C. Schaefer, T. Walter, E. Vetillard. A Security-by-Contracts Architecture for Pervasive Services. In *Proc. of SecPerU'07*. p 49 – 54, IEEE Press 2007.

C92. S. Etalle, F. Massacci, A. Yautsiukhin: The Meaning of Logs. In *Proc. of TrustBus'07*. LNCS 4657, p. 145-154, Springer 2007.

C93. Y. Karabulut, F. Kerschbaum, F. Massacci, P. Robinson, A. Yautsiukhin: Security and Trust in IT Business Outsourcing: a Manifesto. In *Proc. of STM'06*. September 2006, Hamburg, ENTCS, p. 47-58 Elsevier, 2007.

C94. F. Massacci, K. Naliuka: Towards Practical Security Monitors of UML Policies for Mobile Applications. In ***Proc. of Policy 2007***, p. 278-278. , IEEE Press.
C95. F. Massacci, I. Siahaan. Matching Midlet's Security Claims with a Platform Security Policy using Automata Modulo Theory. In *Proc. of NordSec'07*. 2007.
C96. F. Massacci, A. Yautsiukhin. Modelling Quality of Protection in Outsourced Business Processes. In *Proc. of IAS'07*, p. 247-252 IEEE Press 2007.
C97. F. Massacci, A. Yautsiukhin. An Algorithm for the Appraisal of Assurance Indicators for Complex Business Processes. In *Proc. of QoP'07*, p. 22-27 ACM Press 2007.
C98. A. Pretschner, F. Massacci, M. Hilty: Usage Control in Service-Oriented Architectures. In *Proc. of TrustBus'07*, LNCS 4657 p. 83-93, Springer 2007.

C99. V. Bryl, F. Massacci, J. Mylopoulos and N. Zannone. Designing Security Requirements Models through Planning. In ***Proc. of CAiSE'06***, June 2006, Luxembourg, LNCS 4001, p. 33-47, Springer-Verlag 2006.
C100. P. Giorgini, F. Massacci, J. Mylopoulos and N. Zannone. Detecting Conflicts of Interest. In ***Proc. of IEEE RE'06***. September 2006, Minneapolis/St. Paul (USA), p. 308-311, IEEE Press, 2006.

C101. P. Giorgini, F. Massacci, J. Mylopoulos, N. Zannone: Modeling Security Requirements Through Ownership, Permission and Delegation. In ***Proc. of IEEE RE'05***, p. 167-176, IEEE Press 2005. **Ten Years Most Influential Paper Award in 2015**.
C102. P. Giorgini, F. Massacci, J. Mylopoulos, N. Zannone: Modeling Social and Individual Trust in Requirements Engineering Methodologies. In *Proc. of iTrust'05*, LNCS 3477, p. 161-176, Springer 2005.
C103. H. Koshutanski, F. Massacci: Interactive Credential Negotiation for Stateful Business Processes. In *Proc. of iTrust'05* May 2005, Paris (FR), LNCS 3477, LNCS 256-272, Springer 2005.
C104. G. M. Kuper, F. Massacci, N. Rassadko: Generalized XML security views. In *Proc. of SACMAT'05*. p. 77-84, ACM Press, 2005.
C105. F. Massacci, J. Mylopoulos, N. Zannone: Minimal Disclosure in Hierarchical Hippocratic Databases with Delegation. In *Proc. of ESORICS'05*, LNCS 3679, p. 438-454, Springer 2005.
C106. N. Zannone, S. Jajodia, F. Massacci and D. Wijesekera. Maintaining Privacy on Derived Objects. In *Proc. of WPES'05*, p. 10-19. ACM Press, 2005.

C107. G. Bella, S. Bistarelli, and F. Massacci. A protocol's life after attacks. In *Proc. of the 11th Int. Workshop on Security Protocols*, LNCS. Springer-Verlag, 2004.
C108. N. Chetcuti-Sperandio and F. Massacci. Semantique et raisonnement automatique pour une infrastructure a cles publiques. In Proc. of RFIA 2004, vol. 3, pages 1165-1174, 2004.
C109. P. Giorgini, F. Massacci, J. Mylopoulos, and N. Zannone. Requirements engineering meets trust management: model, methodology, and reasoning. In *Proc. of i-Trust 2004*, LNCS 2995 p. 176-190. Springer-Verlag, 2004.
C110. P. Giorgini, F. Massacci, J. Mylopoulous, and N. Zannone. Filling the gap between requirements engineering and public key/trust management infrastructures. In *Proc. of EuroPKI'04*, LNCS 3093 p. 15-24. Springer-Verlag, 2004.
C111. H. Koshutanski and F. Massacci. E pluribus unum: Deduction, abduction and induction, the reasoning services for access control in autonomic communication. In Proc. of WAC'04, LNCS.
C112. H. Koshutanski and F. Massacci. Interactive access control for Web Services. In *Proc. of SEC'04*, p. 151-166. Kluwer Academic Publishers, 2004.
C113. H. Koshutanski and F. Massacci. An interactive trust management and negotiation scheme. In *Proc. of FAST'04*, p. 139-152. Kluwer Academic Publishers, 2004.
C114. H. Koshutanski and F. Massacci. A system for interactive authorization for Business Processes for Web Services. In Proc. of ICWE '04, LNCS 3140, p. 521-525. Springer-Verlag Heidelberg, 2004.
C115. F. Massacci and N. Zannone. Privacy is linking permission to purpose: extended abstract. In *Proc. of the 12th International Workshop on Security Protocols*, LNCS. Springer-Verlag, 2004.

C116. L. Carlucci Aiello and F. Massacci. Attacking fair-exchange protocols: parallel models vstrace models. In *Proc. of Int Workshop on Logical Aspects of Crypto. Protocols Verif.*, ENTCS 55. Elsevier, 2003
C117. H. Koshutanski and F. Massacci. An access control framework for business processes for web services. In Proc. of XMLSEC-2003, p. 15-24. ACM Press, 2003.
C118. H. Koshutanski and F. Massacci. An access control system for business processes for web services. In Proc. of NordSec'03, Tech, Report. Gjovik University College, Norway., 2003.
C119. H. Koshutanski and F. Massacci. A logical model for security of Web Services. In *Proc. of FAST'03*, p. 1-8. Technical Report IIT TR-10/2003.
C120. N. Chetcuti-Sperandio and F. Massacci. Reasoning about credential-based systems. *In Proc.of FAST'03*, p. 23-38. Technical Report IIT TR-10/2003.
C121. N. Chetcuti-Sperandio and F. Massacci. A semantics and a calculi for reasoning about credential based systems. In *Proc. of M4M'03*, p. 61.76, 2003.
C122. P. Giorgini, F. Massacci, and J. Mylopoulos. Requirements engineering meets security: a case study on

modelling Secure electronic Transactions by VISA and Mastercard. In *Proc. of ER'03*. LNCS 2813 p. 263-276. Springer-Verlag, 2003.

C123. G. Bella, F. Massacci, and L. C. Paulson. The verification of an industrial payment protocol: The SET purchase phase. In ***Proc. of ACM CCS'02***, p. 12-20. ACM Press, 2002.

C124. F. M. Donini, P. Liberatore, F. Massacci, and M. Schaerf. Solving QBF with SMV. In *Proc. of KR'02*, pages 578-589, Morgan Kaufmann 2002.

C125. A. Fioravanti and F. Massacci. How to model (and simplify) the SET payment phase for automated verification. In *Proc. VERIFY '01*, p. 34-44, 2001. DII Technical Report 08/01, Univ. of Siena.

C126. F. Massacci. Decision procedures for expressive description logics with intersection, composition, converse of roles and role identity. In ***Proc. of IJCAI'01***, p. 193-198. Morgan-Kaufmann, 2001.

C127. P. Baumgartner and F. Massacci. The taming of the (X)OR. In *Computational Logic 2000*, LNCS 1861 p. 508-522. Springer-Verlag, 2000

C128. G. Bella, F. Massacci, L. Paulson, and T. Piero. Formal verication of Card-Holder Registration in SET. In *Proc of. ESORICS'00*, LNCS 1895 p. 159-174. Springer-Verlag Heidelberg, 2000

C129. G. Bella, F. Massacci, L. Paulson, and T. Piero. Making sense of specifications: the formalization of SET (extended abstract). In *Proc. of the 8th Int. Workshop on Security Protocols*, LNCS 2133 p 74-81. Springer-Verlag, 2000.

C130. L. Carlucci Aiello and F. Massacci. An executable specification language for planning attacks to security protocols. In ***Proc. CSFW'00***. p. 88-103. IEEE Press, 2000.

C131. M. Hietalahti, F. Massacci, and I. Niemela. DES: a challenge problem for nonmonotonic reasoning systems. In Proc. of NMR-2000.

C132. F. Massacci. Reduction rules and universal variables for first order tableaux and DPLL. In *Proc. of KR'00*, pages 186-197. Morgan Kaufmann, 2000.

C133. F. Massacci. Using walk-SAT and rel-sat for cryptographic key search. In ***Proc. of IJCAI'99***, p. 290-295. Morgan Kaufmann, 1999.

C134. F. Massacci. Cook and Reckhow are wrong: subexponential tableau proofs for their family of formulae. In Proc. ECAI-98, p. 408-409. Morgan Kaufmann, 1998.

C135. F. Massacci. Anytime approximate modal reasoning. In ***Proc. of AAAI-98***, p. 274-279. AAAI Press/The MIT Press, 1998.

C136. F. Massacci. Tableaux methods for access control in distributed systems. In *Proc. of TABLEAUX-98*, LNAI 1227 p. 246-260. Springer-Verlag Heidelberg, 1997.

C137. F. Massacci. Breaking security protocols as an AI planning problem. In *Proc. of ECP'97*, LNAI 1348, p. 286-298. Springer-Verlag, 1997.

C138. F. Massacci. A proof theory for tractable approximations of propositional reasoning. In *Proc. Of AI*IA-97*, LNAI 1321p. 219-230. Springer-Verlag, 1997.

C139. F. Massacci. Simplification: A general constraint propagation technique for propositional and modal tableaux. In Proc. TABLEAUX-97, LNAI 1397 p. 217-231. Springer-Verlag, 1998.

C140. F. Massacci. Reasoning about security: a logic and a decision methods for role-based access control. In *Proc. of ECSQARU/FAPR'97*, LNAI 1244 p. 421-435. Springer-Verlag, 1997.

C141. G. De Giacomo and F. Massacci. Tableaux and algorithms for propositional dynamic logic with converse. In ***Proc. of CADE-96***, LNAI 1104 p. 613-628. Springer-Verlag 1996

C142. F. M. Donini, F. Massacci, D. Nardi, and R. Rosati. A uniform tableaux method for nonmonotonic modal logics. In Proc. of *JELIA-96*, LNCS 1126 p. 87-103. Springer-Verlag, 1996.

C143. F. Massacci. Contextual reasoning is NP-complete. In ***Proc. of AAAI-96***, p. 621-626. AAAI Press/The MIT Press, 1996.

C144. F. Massacci. Approximate reasoning for contextual databases. In *Proc. of ICTAI-96*, p. 308-315. IEEE Press, 1996.

C145. F. Massacci. Superficial tableaux for contextual reasoning. In *Proc. of the AAAI-95 FS on Formalizing Context"*, in AAAI Technical Report FS-95-02, p. 60-66. AAAI Press/The MIT Press, 1995.

C146. F. Massacci. k-clusters tableaux (a tool for modal logics and inconsistent belief sets). *AI*IA Notizie*, 4:23-33, 1994. Ex-aequo AI*IA award in 1994 for the best paper in Artificial Intelligence by master graduates.

C147. F. Massacci. Strongly analytic tableaux for normal modal logics. In ***Proc. of CADE-94***, LNAI 814 p. 723-737. Springer-Verlag, 1994

I autorize the processing of personal data included in my curriculum vitae according to the applicable norms and regulation.