

Luca Allodi

Universitair Docent (Assistant Professor)

Security Group

Department of Mathematics and Computer Science

Eindhoven Technical University

P.O. Box 513, 5600 MB Eindhoven, the Netherlands

Email: l.allodi@tue.nl

Homepage: <http://www.win.tue.nl/~lallodi>

Education

Apr. 2015 **Ph.D.** in Information Security, *DISI, University of Trento, Italy*.

Awarded best PhD Thesis at DISI, for A.Y. 2013/2014.

Jul. 2011 **MSc** Information Security, University of Milan, Italy.

Jun. 2009 **BSc** Computer Science, University of Milan, Italy.

Research interests

System and software security management

Standard setting and policies for information security

Vulnerability exploitation and cyberattacks

Underground cybercrime markets' economy and activities

Previous positions

May 2015-Jan 2015. Postdoctoral Research Fellow at the University of Trento, DISI.

Apr 2014-Sept 2014 Visiting University of Durham Business School, UK.

Sep 2011-Apr 2015 PhD Student at University of Trento (UNITN Scholarship).

Jun 2006-Aug 2011 Co-Founder, Executive Director of Area-Software of BRT Solutions (Brescia, IT).

Research impact and achievements

Funding and involvement in research projects (2017-Pres.) I am an investigator and among the main proponents of INTERSECT, a 2019 **NWA-NWO** 10M, 8 years project on IoT security (1.2M TU/e), and of DEFRAUDify, an **ITEA3** project on cybercrime and fraud identification (approx 540k Euro for TU/e). I am also PI of a proposal for the **NWO Cybersecurity** call at the start of 2019 (granting decision yet to be taken), and have worked as the initiator of an H2020 proposal whose second incarnation is now led by ATOS (granting decision yet to be taken). I have been shortlisted for the 2018 NWO VENI interview round with a proposal on cybercrime economics, and am submitting to the NWO VIDI in 2019.

Standard setting (2014-Pres.) I am an acknowledged contributing author of the third version of the *Common Vulnerability Scoring System (CVSS)*, the worldwide standard for vulnerability assessment promoted by NIST and US CERT. I've been invited to join the *First.org* Special Interest Group (SIG) for the development of the standard as a result of my work on vulnerability risk

Student	Year	Topic	Published in
Pavlo Burda (PhD stud.)	2019	Redundancy of TOR systems.	Pavlo Burda, Cohen Boot, and Luca Allodi. Characterizing the redundancy of darkweb .onion services. In <i>Proceedings of the International Conference on Availability, Reliability, and Security (ARES)</i> . ACM, 2019
Michele Campobasso (MSc stud.), Pavlo Burda (PhD stud.)	2019	Stealth monitoring of underground activities in adversarial conditions	Michele Campobasso, Pavlo Burda, and Luca Allodi. Caronte: Crawling adversarial resources over non-trusted, high-profile environments. In <i>Proceedings of the EuroS&P Workshop on Attackers and Cyber-Crime Operations (WACCO)</i> . IEEE, 2019
Amber van der Heijden (MSc stud.)	2019	Cognitive evaluation of phishing attacks.	Amber van der Heijden and Luca Allodi. Cognitive triaging of phishing attacks. In <i>28th USENIX Security Symposium (USENIX Security 19)</i> , pages 1309–1326, Santa Clara, CA, August 2019. USENIX Association Top-3 cybersecurity conference. 16% acceptance rate.
Tzouliano Chotza (Internship)	2019	Countermeasures for phishing attacks	Luca Allodi, Tzouliano Chotza, Ekaterina Panina, and Nicola Zannone. On the need for new anti-phishing measures against spear phishing attacks. <i>To appear in IEEE Security & Privacy</i> , 2019
Gijs Rijnders (MSc stud.)	2019	Privacy-aware detection and reporting of Indicators of Compromise in operative settings using BLOOM filters	Roland van Rijswijk-Deij, Gijs Rijnders, Matthijs Bomhoff, and Luca Allodi. Privacy-conscious threat intelligence using dnsbloom. In <i>IFIP/IEEE International Symposium on Integrated Network Management</i> , 2019
Tho Le Phouc (MSc stud.)	2018	DNSSEC measurements and the effect of economic incentives on <i>quality</i> vs <i>quantity</i> of adoption. Together with	Tho Le, Roland van Rijswijk-Deij, Luca Allodi, and Nicola Zannone. Economic incentives on dnssec deployment: Time to move from quantity to quality. In <i>Proceedings of the 16th IEEE/IFIP Network Operations and Management Symposium (NOMS 2018)</i> . IEEE, 2018. Provided recommendations to the Swedish Internet registry Internetstiftelsen i Sverige (IIS), and the registry operator for the Netherlands, SIDN, on future development of DNSSEC policies.
Marco Corradin (UNITN, MSc stud.)	2016	Investigation on the maturity of underground marketplaces. With University of Twente.	L. Allodi, M. Corradin, and F. Massacci. Then and now: On the maturity of the cybercrime markets the lesson that black-hat marketers learned. <i>IEEE Transactions on Emerging Topics in Computing</i> , 4(1):35–46, Jan 2016. doi:10.1109/TETC.2015.2397395

Table 1: Selection of supervised students and outcomes of their projects

assessment. I have contributed and authored several modifications of the standard, including single-handedly proposing and drafting (jointly with Microsoft) a major change to the new upcoming standard version (4.0). I am the only European member of the consortium, and one of the only two academics in the SIG. Other members of the consortium include Oracle, Microsoft, IBM, Juniper, Intel, NIST, US CERT/CC, and others.

Students (2016-Pres.) I have supervised or am currently supervising fourteen MSc thesis at TU/e. Five are currently completed; four of these resulted in a scientific publication aimed at

highly-regarded or top venues in the field of networks and security. I currently have one PhD student, Pavlo Burda (started Spring 2018) and a second one, Michele Campobasso is joining the group in October 2019. Two more positions will be opened starting in November.

Publications (2012-Pres.) My work on vulnerability management has been published in a top Information System Security journal, *ACM Transactions on Information and System Security* (best non-crypto security journal according to Microsoft Academic Research), and I published in the prestigious *Risk Analysis* journal, the flagship journal of the Society for Risk Analysis. I have a single-author paper in *ACM CCS 2017*, *ESSoS 2015* and in *Usenix LEET 2013*. The work of one of my MSc students has been published in *Usenix Security 2019*, one of the top four Computer Security venues. I further published, among other venues, in the new *IEEE Transactions on Emerging Topics in Computing* and in the Rank-A Information System conference *ECIS 2015*.

Research visibility with industry and practitioners. (2013-Pres.) My work on vulnerability management and prioritisation has been presented at *BlackHat USA 2013*, the leading industry conference in Information Security counting more than 7.5 thousand attendees. The results of my work and my participation in the CVSSv3 team created several contacts with industry leaders such as SAP, Symantec, and Qualys. I am an invited lecturer for the 2019 **Lorentz Center** seminar on *Cyber Insurance and its Contribution to Cyber Risk Mitigation* with a lecture on the link between cybercrime economics and risk measurement. In August 2019 I have been invited to give a seminar at Google's headquarters in Mountain View, CA, on phishing.

RAND Corporation report on cybercrime. (2013) My work on cybercrime underground markets has been acknowledged by the RAND Corporation, that contacted me as a domain expert for the RAND report "Markets for Cybercrime Tools and Stolen Data" (<http://tinyurl.com/mtmnhte>) released in October 2013. My work on vulnerabilities has also been covered by the specialised media in a DarkReading article (<http://tinyurl.com/lv2pbxo>).

Student supervision and outcomes

Table 1 reports a summary of selected outcomes from the students I have supervised in the last year. Since my arrival at TU/e I have supervised or am currently supervising 14 (and counting) MSc theses. I currently have one PhD student, Pavlo Burda. A second one (Michele Campobasso) is joining the group in October 2019.

Publications

International standards

1. First.org CVSS Special Interest Group (Authoring member). Common Vulnerability Scoring System (CVSS) v3. *Published at <http://www.first.org/cvss>. Only EU representative and only academic in the standard body next to CMU.*

Journals

2. Luca Allodi and Fabio Massacci. Security events and vulnerability data for cyber security risk estimation. *Risk Analysis (to appear)*, 37(8), 2017 **Impact factor: 2.225**, ISI Journal

Citation Reports Ranking: 2015: 6/49 (Social Sciences Mathematical Methods); 17/101 (Mathematics Interdisciplinary Applications).

3. L. Allodi, M. Corradin, and F. Massacci. Then and now: On the maturity of the cybercrime markets the lesson that black-hat marketers learned. *IEEE Transactions on Emerging Topics in Computing*, 4(1):35–46, Jan 2016. doi:10.1109/TETC.2015.2397395 **Impact factor: 4.12** (2016 Scopus CiteScore).
4. Luca Allodi and Fabio Massacci. Comparing vulnerability severity and exploits using case-control studies. *ACM Transactions on Information and System Security*, 17(1):1:1–1:20, August 2014. doi:10.1145/2630069 **Impact factor: 3.45** (2014 Scopus CiteScore); flagship ACM journal on security.

Conferences and peer-reviewed publications

5. Luca Allodi, Tzouliano Chotza, Ekaterina Panina, and Nicola Zannone. On the need for new anti-phishing measures against spear phishing attacks. *To appear in IEEE Security & Privacy*, 2019
6. Amber van der Heijden and Luca Allodi. Cognitive triaging of phishing attacks. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1309–1326, Santa Clara, CA, August 2019. USENIX Association **Top-3 cybersecurity conference. MSc thesis. 16% acceptance rate.**
7. Laura Genga, Luca Allodi, and Nicola Zannone. Unveiling systematic biases in decisional processes: an application to discrimination discovery. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pages 67–72. ACM, 2019
8. Pavlo Burda, Cohen Boot, and Luca Allodi. Characterizing the redundancy of darkweb .onion services. In *Proceedings of the International Conference on Availability, Reliability, and Security (ARES)*. ACM, 2019
9. Donatello Luna, Luca Allodi, and Marco Cremonini. Productivity and patterns of activity in bug bounty programs: Analysis of hackerone and google vulnerability research. In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, page 67. ACM, 2019
10. Michele Campobasso, Pavlo Burda, and Luca Allodi. Caronte: Crawling adversarial resources over non-trusted, high-profile environments. In *Proceedings of the EuroS&P Workshop on Attackers and Cyber-Crime Operations (WACCO)*. IEEE, 2019
11. Roland van Rijswijk-Deij, Gijs Rijnders, Matthijs Bomhoff, and Luca Allodi. Privacy-conscious threat intelligence using dnsbloom. In *IFIP/IEEE International Symposium on Integrated Network Management*, 2019
12. Luca Allodi. Underground economics for vulnerability risk. *Published in Usenix ;login:*, 43(1), 2018. URL: <https://www.usenix.org/publications/login/spring2018/allodi> **Invited article.**

13. Luca Allodi, Marco Cremonini, Fabio Massacci, and Woohuyn Shim. The effect of security education and expertise on security assessments: the case of software vulnerabilities. In *Presented at the Workshop on Economics of Information Security.*, 2018 **Top venue in cybersecurity economics.**
14. Jukka Ruohonen and Luca Allodi. A bug bounty perspective on the disclosure of web vulnerabilities. In *Presented at the Workshop on Economics of Information Security.*, 2018 **Top venue in cybersecurity economics.**
15. Luca Allodi, Sebastian Banescu, Henning Femmer, and Kristian Beekers. Identifying relevant information cues for vulnerability assessment using cvss. In *The 8th ACM Conference on Data and Application Security and Privacy (CODASPY'18)*. ACM, 2018
16. Tho Le, Roland van Rijswijk-Deij, Luca Allodi, and Nicola Zannone. Economic incentives on dnssec deployment: Time to move from quantity to quality. In *Proceedings of the 16th IEEE/IFIP Network Operations and Management Symposium (NOMS 2018)*. IEEE, 2018
17. Luca Allodi. Economic factors of vulnerability trade and exploitation. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS '17*, pages 1483–1499, New York, NY, USA, 2017. ACM. URL: <http://doi.acm.org/10.1145/3133956.3133960>, doi:10.1145/3133956.3133960 **Top-3 cybersecurity conference. Acc. rate 18%. Only accepted single author paper (of 33 submitted).**
18. Luca Allodi and Sandro Etalle. Towards realistic threat modeling: Attack commodification, irrelevant vulnerabilities, and unrealistic assumptions. In *Proceedings of the 2017 Workshop on Automated Decision Making for Active Cyber Defense, SafeConfig '17*, pages 23–26, New York, NY, USA, 2017. ACM. URL: <http://doi.acm.org/10.1145/3140368.3140372>, doi:10.1145/3140368.3140372
19. Luca Allodi and Fabio Massacci. Attack potential in impact and complexity. In *Proceedings of the 12th International Conference on Availability, Reliability and Security, ARES '17*, pages 32:1–32:6, New York, NY, USA, 2017. ACM. URL: <http://doi.acm.org/10.1145/3098954.3098965>, doi:10.1145/3098954.3098965
20. Luca Allodi, Fabio Massacci, and Julian Williams. The work-averse cyber attacker model. evidence from two million attack signatures. In *Presented at the Workshop on Economics of Information Security. Available at <https://ssrn.com/abstract=2862299>*, 2017
21. Luca Allodi and Fabio Massacci. The work-averse attacker model. In *Proceedings of the European Conference on Information Systems (ECIS) 2015. Paper 7.*, 2015. doi:10.18151/7217264
22. Luca Allodi. The heavy tails of vulnerability exploitation. In *Engineering Secure Software and Systems*, volume 8978 of *Lecture Notes in Computer Science*, pages 133–148. Springer International Publishing, 2015. doi:10.1007/978-3-319-15618-7_11
23. Luca Allodi, Luca Chiodi, and Marco Cremonini. Self-organizing techniques for knowledge diffusion in dynamic social networks. In *Complex Networks V*, volume 549 of *Studies in*

- Computational Intelligence*, pages 75–86. Springer International Publishing, 2014. doi:10.1007/978-3-319-05401-8_8
24. Luca Allodi and Fabio Massacci. How cvss is dosing your patching policy (and wasting your money). *BlackHat USA 2013* arXiv:1301.1275 [cs.CR], 2013
 25. Woohyun Shim, L. Allodi, and F. Massacci. Crime pays if you are just an average hacker. In *2012 International Conference on Cyber Security (CyberSecurity)*, pages 62–68, Dec 2012. doi:10.1109/CyberSecurity.2012.15 (**Best paper award**)
 26. Luca Allodi, Luca Chiodi, and Marco Cremonini. The asymmetric diffusion of trust between communities: Simulations in dynamic social networks. In *Proceedings of the Winter Simulation Conference*, WSC '11, pages 3146–3157. Winter Simulation Conference, 2011. URL: <http://dl.acm.org/citation.cfm?id=2431518.2431891> (**Finalist best theoretical paper award**)
 27. Luca Allodi, Luca Chiodi, and Marco Cremonini. Modifying trust dynamics through cooperation and defection in evolving social networks. In *Trust and Trustworthy Computing*, volume 6740 of *Lecture Notes in Computer Science*, pages 131–145. Springer Berlin Heidelberg, 2011. doi:10.1007/978-3-642-21599-5_10

Workshops, tutorials, and posters

22. Luca Allodi, Fabio Massacci, Matteo Giacalone, Andrea Volponi, and Rocco Mammoliti. Using historic attack data and internal vulnerability assessments to estimate IT risk. Application to a large italian organization. In *Society for Risk Analysis Europe Conference 2016*, 2016. URL: <http://programme.exordo.com/sra2016/delegates/presentation/25/>
23. Luca Allodi and Fabio Massacci. Tutorial: Effective security management: a tutorial on cvss v3 and using case control studies to measure vulnerability risk. In *Proceedings of the 2015 Engineering Secure Software and Systems Conference (ESSoS'15)*, 2015
24. Luca Allodi and Fabio Massacci. Tutorial: Effective security management: using case control studies to measure vulnerability risk. In *25th IEEE International Symposium on Software Reliability Engineering (ISSRE)*, 2014
25. Luca Allodi, Vadim Kotov, and Fabio Massacci. Malwarelab: Experimentation with cyber-crime attack tools. In *Presented as part of the 6th Workshop on Cyber Security Experimentation and Test*, Berkeley, CA, 2013. USENIX. URL: <https://www.usenix.org/conference/cset13/workshop-program/presentation/Allodi>
26. L. Allodi, Woohyun Shim, and F. Massacci. Quantitative assessment of risk reduction with cybercrime black market monitoring. In *Security and Privacy Workshops (SPW), 2013 IEEE*, pages 165–172, May 2013. doi:10.1109/SPW.2013.16
27. Luca Allodi and Fabio Massacci. A preliminary analysis of vulnerability scores for attacks in wild: The ekits and sym datasets. In *Proceedings of the 2012 ACM Workshop on Building Analysis Datasets and Gathering Experience Returns for Security*, BADGERS '12, pages 17–24. ACM, 2012. doi:10.1145/2382416.2382427

28. Luca Allodi. Attacker economics for internet-scale vulnerability risk assessment. In *Presented as part of the 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats*. USENIX, 2013. URL: <https://www.usenix.org/conference/leet13/workshop-program/presentation/Allodi>
29. Luca Allodi and Fabio Massacci. Poster: Analysis of exploits in the wild. In *IEEE 2013 Symposium on Security & Privacy*, 2013
30. Luca Allodi. The dark side of vulnerability exploitation: a research proposal. In *Proceedings of the 2012 Engineering Secure Software and Systems Conference Doctoral Symposium*, 2012

Event organization

I am the Chair of the first Euro Security & Privacy Workshop on Attackers and Cyber-Crime Operations (WACCO) (<https://www.ieee-security.org/TC/EuroSP2019/events.php>); co-organizers are colleagues from Cambridge (UK), UC Berkeley (US), Univ. of New Mexico (US), and Univ. of Trento (IT).

Teaching

I am the responsible lecturer for the 2IC80 course on Offensive Computer Security (bachelor elective in security package). I designed the course from scratch in 2018; the course obtained excellent results. From 2018 evaluation: overall score (**9.1/10**); course structure, content, organization, material (**4.5/5**); evaluation of lecturer (**4.9/5**). Sample of comments: “*Best lecturer, excellent strucutre (sic.), interesting materials, no issues*”; “*I loved the material, definitely the most interesting course content so far in the whole computer science bachelor*”; “*Very enthusiastic lecturer that had a great way of teaching*”. I am also co-lecturer of the course *Cyber-attacks, Crime, and Defenses* in 2019, held jointly with Prof. S. Etalle (evaluation not in yet).

Invited presentations and seminars

Towards Fully-Automated Response to Phishing Attacks. Google. Mountain View, CA.

Quantitative Estimations of Attack Threats. Lorentz Center. NL.

Cognitive Triaging of Phishing Attacks. High-Tech Police Headq. for *NoMorePhish* project, NL.

The Work-Averse Attacker Model. Seminar at Technical University of Munich, Munich, Germany.

The Common Vulnerability Scoring System v3. Seminar at University of Milan, Italy.

The Work-Averse Attacker Model. Presentation at ECIS 2015, Muenster, Germany.

The Heavy Tails of Vulnerability Exploitation. Presentation at ESSoS 2015, Milan, Italy.

Advanced Vulnerability Management. Full day tutorial at ESSoS 2015, Milan, Italy.

Tutorial: Effective security management: using case control studies to measure vulnerability risk. Half day tutorial at ISSRE 2014, Naples, Italy.

Vulnerability criticality assessment and efficient software security management. Two days (6 hours)

seminar at University of Milan, Italy.

Efficient Vulnerability Management: Measuring Vulnerabilities and Exploits for Better Security Strategies. Seminar on Road-Mapping Cybersecurity Research and Innovation, Florence, IT.

My Software has a vulnerability, should I Worry? An empirical validation of an industry standard. Seminar at Durham University, UK and Accenture, Washington D.C., USA.

Attacker Economics for Internet-scale vulnerability Risk Assessment (Extended Abstract). 2013 Usenix Security LEET Workshop. Washington D.C., USA.

My Software has a vulnerability, should I Worry? An empirical validation of an industry standard. Seminar at George Mason University, Fairfax, USA.

Economics of cybercrime. Seminar, Joint meeting with Ufa State Aviation University, Russia. Trento, Italy.

MalwareLab: Experimenting with Cybercrime Attack Tools. 2013 Usenix Security CSET Workshop. Washington D.C., USA.

Luca Allodi and Fabio Massacci. How CVSS is DOSSing your patching policy (and wasting your money). BlackHat USA 2013. Las Vegas, Nevada, USA.

Quantitative assessment of risk reduction with cybercrime black market monitoring. IEEE SS&P IWCC 2013. San Francisco, California, USA.

Analysis of exploits in the wild. Or, do Cybersecurity standards make sense? IEEE SS&P 2013 Poster session. San Francisco, California, USA.

Crime pays if you are just an average hacker. IEEE/ASE 2012 Conference on Cyber Security. Alexandria, Virginia, USA.

A preliminary analysis of CVSS scores in the Wild. ACM CCS BADGERS Workshop. Raleigh, North Carolina, USA.

A quick analysis on data quality for risk evaluation. Rump session at WEIS 2012. Berlin, Germany.

Some preliminary analysis of the economics of malware kits and traffic brokers. Workshop on Collaborative Security and Privacy Technologies. Berlin, Germany.

The dark side of vulnerability exploitation. 2012 ESSoS Conference, Doctoral Symposium session. Eindhoven, The Netherlands.

Research & professional experience

May 2015-2017: Research fellow at DISI, University of Trento.

Oct 2013-Pres.: Authoring member of the standard body for the definition of the Common Vulnerability Scoring System (CVSS) v3 worldwide standard for vulnerability assessment. I worked with CISCO, IBM, JUNIPER and others on its definition.

Apr 2014-Sep 2014.: Visiting Ph.D. Student at University of Durham, UK. Modelling of under- ground cybercrime economy and trust relationships.

Sep 2011-Apr 2015.: Ph.D. Student at University of Trento, Italy. Worked on FP7 project SECONOMICS and PRIN Project TENACE.

Nov 2009-Aug 2011: Project Manager at BRT Solutions (Brescia, Italy), ED As a team leader I coordinated small groups of people (5+) with different expertise and backgrounds.

Jun 2006-Oct 2009: Design Manager at BRT Solutions (Brescia, Italy), ED I worked on web-site design and development. Occasionally I led a group of two people devoted to the design and programming of interfaces.

Other activities

Invited reviewer for: MIS Quarterly; ACM TISSEC/TOPS; IEEE TSE; ESEM; Risk Analysis; IEEE TDSCSI; Elsevier COSE; International Journal of Information Security; ICIS 2016; MMM-ACNS-2012; PST-2012.