Luca Allodi

Universitair Docent (Assistant Professor)
Security Cluster
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 (1.8M TU/e), and of `DEFRAUDIfy`, an **ITEA3** project on cybercrime and fraud identification (approx 540k Euro at TU/e). I am also PI of SeReNiTy, an **NWO Cybersecurity** project on Security Operation Centers operation. I have been shortlisted for the 2018 NWO VENI interview round with a proposal on cybercrime economics.

Standard setting (2014-2020) 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 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

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 *Proceedings of the International Conference on Availability, Reliability, and Security (ARES)*. 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 *Proceedings of the EuroS&P Workshop on Attackers and Cyber-Crime Operations (WACCO)*. IEEE, 2019
Amber van der Hijden (MSc stud.)	2019	Cognitive evaluation of phishing attacks.	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 **16% acceptance rate**.
Tzouliano Chotza (Internship)	2019	Countermeasures for phishing attacks	L. Allodi, T. Chotza, E. Panina, and N. Zannone. The need for new antiphishing measures against spear-phishing attacks. *IEEE Security Privacy*, 18(2):23–34, 2020. `doi:10.1109/MSEC.2019.2940952`
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 *IFIP/IEEE International Symposium on Integrated Network Management*, 2019
Tho Le Phouc (MSc stud.)	2018	DNSSEC measurements and the effect of economic incentives on *quality* vs *quantity* 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 *Proceedings of the 16th IEEE/IFIP Network Operations and Management Symposium (NOMS 2018)*. 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 marketeers learned. *IEEE Transactions on Emerging Topics in Computing*, 4(1):35–46, Jan 2016. `doi:10.1109/TETC.2015.2397395`

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

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.

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 supervise two PhD students.

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, Fabio Massacci, and Julian Williams. The work-averse cyber attacker model. evidence from two million attack signatures. *Risk Analysis*, 2021 (to appear) **Impact factor: 3.137**.

3. Luca Allodi, Marco Cremonini, Fabio Massacci, and Woohyun Shim. Measuring the accuracy of software vulnerability assessments: experiments with students and professionals. *Empirical Software Engineering*, 2020. URL: `https://doi.org/10.1007/s10664-019-09797-4`, `doi:10.1007/s10664-019-09797-4` **Impact factor: 5.61** (2019 Scopus CiteScore).

4. Luca Allodi and Fabio Massacci. Security events and vulnerability data for cyber security risk estimation. *Risk Analysis*, 37(8), 2017 **Impact factor: 2.225**, ISI Journal Citation Reports Ranking: 2015: 6/49 (Social Sciences Mathematical Methods); 17/101 (Mathematics Interdisciplinary Applications).

5. L. Allodi, M. Corradin, and F. Massacci. Then and now: On the maturity of the cybercrime markets the lesson that black-hat marketeers 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).

6. 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.

Policy (white) papers

7. Winnona DeSombre, James Shires, JD Work, Robert Morgus, Patrick Howell ONeill, Luca Allodi, and Trey Herr. Countering cyber proliferation: Zeroing in on Access-as-a-Service. *Atlantic Council, 2021. Available on the Atlantic Councils website.*

8. Winnona DeSombre, Michele Campobasso, Luca Allodi, Dr. James Shires, JD Work, Robert Morgus, Patrick Howell ONeill, and Dr. Trey Herr. A primer on the proliferation of offensive cyber capabilities. *Atlantic Council, 2021. Available on the Atlantic Councils website.*

Conferences and peer-reviewed publications

9. Simone Pirocca, Luca Allodi, and Nicola Zannone. A toolkit for security awareness training against targeted phishing. In *International Conference on Information Systems Security*, pages 137–159. Springer, 2020

10. Martin Rosso, Michele Campobasso, Ganduulga Gankhuyag, and Luca Allodi. Saibersoc: Synthetic attack injection to benchmark and evaluate the performance of security operation centers. In *Annual Computer Security Applications Conference*, pages 141–153, 2020 **Best paper award with artifact. 23% acceptance rate.**

11. Michele Campobasso and Luca Allodi. Impersonation-as-a-service: Characterizing the emerging criminal infrastructure for user impersonation at scale. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 1665–1680, 2020 **17% acceptance rate.**

12. Pavlo Burda, Luca Allodi, and Nicola Zannone. Dont forget the human: a crowdsourced approach to automate response and containment against spear phishing attacks. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 471–476. IEEE, 2020

13. Giorgio Di Tizio, Fabio Massacci, Luca Allodi, Stanislav Dashevskyi, and Jelena Mirkovic. An experimental approach for estimating cyber risk: a proposal building upon cyber ranges and capture the flags. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 56–65. IEEE, 2020

14. Pavlo Burda, Tzouliano Chotza, Luca Allodi, and Nicola Zannone. Testing the effectiveness of tailored phishing techniques in industry and academia: a field experiment. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pages 1–10, 2020

15. L. Allodi, T. Chotza, E. Panina, and N. Zannone. The need for new antiphishing measures against spear-phishing attacks. *IEEE Security Privacy*, 18(2):23–34, 2020. doi:10.1109/MSEC.2019.2940952

16. 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 **16% acceptance rate.**

17. 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

18. 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

19. 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

20. 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

21. 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

22. 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.**

23. 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.**

24. 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.**

25. Luca Allodi, Sebastian Banescu, Henning Femmer, and Kristian Beckers. 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

26. 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

27. 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` **Acc. rate 18%. Only accepted single author paper (of 33 submitted).**

28. 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`

29. 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`

30. 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

31. 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`

32. 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`

33. 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`

34. Luca Allodi and Fabio Massacci. How cvss is dossing your patching policy (and wasting your money). BlackHat USA 2013 arXiv:1301.1275 [cs.CR], 2013

35. 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**)

36. 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**)

37. 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

38. 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/

39. 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

40. 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

41. Luca Allodi, Vadim Kotov, and Fabio Massacci. Malwarelab: Experimentation with cybercrime 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

42. 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

43. 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

44. 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

45. Luca Allodi and Fabio Massacci. Poster: Analysis of exploits in the wild. In *IEEE 2013 Symposium on Security & Privacy*, 2013

46. 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 **Workshop on Attackers and Cyber-Crime Operations (WACCO)**, periodically held with IEEE EuroS&P. www.wacco-workshop.org. My co-chairs include Alice Hutchings at the University of Cambridge, and Sergio Pastrana at University Carlos III of Madrid.

Teaching

I am the responsible lecturer for the 2IC80 course on Offensive Computer Security (OCS). I am also co-lecturer of the course *Cyber-attacks, Crime, and Defenses* in 2019, held jointly with Prof. S. Etalle. Both courses receive excellent scores from students across iterations.

Invited presentations and seminars

Criminal Excellence in (Cyber) La La Land. Cambridge University, UK.

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: us- ing 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, Californa, 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.

Other activities

PC Member of RAID 2021; Invited reviewer for: MIS Quarterly; ACM TISSEC/TOPS; ACM DTRAP; IEEE TSE; ESEM; Risk Analysis; IEEE TDSCSI; Elsevier COSE; International Journal of Information Security.