Luca Allodi

Universitair Hoofddocent (Associate Professor)
Head of Threat Analysis group, 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: https://lallodi.github.io/

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.

PhD students

Pavlo Burda (2018-01/24 (exp))	Advanced Social Engineering.
Michele Campobasso (2019-03/24 (exp))	Cybercrime Threats Evolution.
Leon Kersten (2021 -)	Decision Support for Security Analysis.
Koen Teuwen (2022 -)	Automated Methods for Threat Intelligence.

Past positions and current roles

Sep 2022 -	Scientific Director at Eindhoven Security Hub.
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, ED 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, and co-applicant for the **NWO/NWA CATRIN project** on threat intelligence. I am now leading efforts for an application to an Horizon Europe project proposal centred around the TUe M&CS Security Operation Center (ESH-SOC), and am involved in the drafting of an ITEA4 project and an NWO-NWA project. I have been shortlisted for the 2018 NWO VENI interview round with a proposal on cybercrime economics.

Eindhoven Security Hub - Security Operation Center (2020-) I have led the initial technical efforts to bring up the backbone of the ESH-SOC infrastructure. I have been and am **coordinating education** within the SOC and its collaboration with Fontys for a total of more than **60 students** since 2020 with roughly a 50-50 split between TUe and Fontys students. Since September 2022 I

Student	Year	Topic	Published in
Marin Ioana	2023	Phishing reporting	Ioana Marin, Pavlo Burda, Luca Allodi, and Nicola Zannone. The influence of human factors on the intention to report phishing emails. In *Proceddings of the 2023 ACM Conference on Human Factors in Computing Systems*, 2023
Martino Tommasini	2022	Attacks on Building Automation Systems.	Martino Tommasini, Martin Rosso, Emmanuele Zambon, Luca Allodi, and Jerry den Hartog. Characterizing building automation system attacks and attackers. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 139–149. IEEE, 2022
Meijaard, Yoram	2021	Models for disruptive malware attacks.	Yoram Meijaard, Peter-Paul Meiler, and Luca Allodi. Modelling disruptive apts targeting critical infrastructure using military theory. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 178–190. IEEE, 2021
Simone Pirocca	2020	Toolkit for automated spear phishing experimentation	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
Amber van der Hijden	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`, **IEEE best paper award**.

Table 1: Selection (6/13) of supervised students whose MSc projects are published in peer-reviewed venues requiring no additional work or data collection.

am the **scientific director of the ESH-SOC**, coordinating joint work between the ESH-SOC and the SECurity cluster, and integrating the ESH-SOC in wider research projects. Currently 2 PhD students are active in ESH-SOC; ESH-SOC is involved in 2 national projects, and is at the core of an HE project proposal being drafted.

Policy impact (2021) Our work on cybercrime threat modelling and measurement resulted in key contributions (together with PhD student Michele Campobasso, expected to graduate in 2023 under my supervision) in two publications from the Atlantic Council on the proliferation of offensive cyber-capabilities (see publication list below). These publications resulted in **hearings from US State, Microsoft, the Cyber Peace Institute**, as well as discussion with a member of the EU parliament, and were part of the broader discussion that led to resolutions from the *US Department of Commerce* to amend the US Export Administration Regulations in relation to specific cybersecurity actors.

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 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.

Student supervision and outcomes

Table 1 reports a summary of selected outcomes from MSc pprojects I have supervised.

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. Pavlo Burda, Luca Allodi, and Nicola Zannone. Cognition in social engineering empirical research: a systematic literature. *ACM Transactions on Computer-Human Interaction (to appear)*, 2024

3. Luca Allodi, Fabio Massacci, and Julian Williams. The work-averse cyberattacker model: theory and evidence from two million attack signatures. *Risk Analysis*, 42(8):1623–1642, 2022

4. Laura Genga, Luca Allodi, and Nicola Zannone. Association rule mining meets regression analysis: An automated approach to unveil systematic biases in decision-making processes. *Journal of Cybersecurity and Privacy*, 2(1):191–219, 2022.

5. 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` Software 62/398.

6. Luca Allodi and Fabio Massacci. Security events and vulnerability data for cyber security risk estimation. *Risk Analysis*, 37(8), 2017

7. 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`

8. 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

Policy (white) papers

9. 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.*

10. 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

11. Michele Campobasso and Luca Allodi. You can tell a cybercriminal by the company they keep: A framework to infer the relevance of underground communities to the threat landscape. *Presented at the 22nd Workshop on the Economics of Information Security (WEIS'23)*, 2023

12. Michele Campobasso and Luca Allodi. Know your cybercriminal: Evaluating attacker preferences by measuring profile sales on an active, leading criminal market for user impersonation at scale. In *Proceedings of Usenix Security 2023*, 2023

13. Leon Kersten, Tom Mulders, Emmanuele Zambon, Chris Snijders, and Luca Allodi. 'give me structure': Synthesis and evaluation of a (network) threat analysis process supporting tier 1 investigations in a security operation center. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 97–111, 2023

14. Ioana Marin, Pavlo Burda, Luca Allodi, and Nicola Zannone. The influence of human factors on the intention to report phishing emails. In *Proceddings of the 2023 ACM Conference on Human Factors in Computing Systems*, 2023

15. Pavlo Burda, Abdul Malek Altawekji, Luca Allodi, and Nicola Zannone. The peculiar case of tailored phishing against smes: Detection and collective defensemechanisms at a small it company. In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 232–243. IEEE, 2023

16. Leon Kersten, Pavlo Burda, Luca Allodi, and Nicola Zannone. Investigating the effect of phishing believability on phishing reporting. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 117–128. IEEE, 2022

17. Michele Campobasso and Luca Allodi. Threat/crawl: a trainable, highly-reusable, and extensible automated method and tool to crawl criminal underground forums. In *APWG eCrime 2022*, 2022

18. Max Meijer, Giacomo Tommaso Petrucci, Matthijs Schotsman, Luca Morgese, Thijs van Ede, Andrea Continella, Ganduulga Gankhuyag, Luca Allodi, and Savio Sciancalepore. Federated lab (fedlab): An open-source distributed platform for internet of things (iot) research and experimentation. In *IEEE World Forum on IoT*, 2022

19. Luca Morgese Zangrandi, Thijs Van Ede, Tim Booij, Savio Sciancalepore, Luca Allodi, and Andrea Continella. Stepping out of the mud: Contextual threat information for iot devices with manufacturer-provided behaviour profiles. In *Annual Computer Security Applications Conference, ACSAC 2022*, 2022 **23.8% acceptance rate.**

20. Leon Kersten, Pavlo Burda, Luca Allodi, and Nicola Zannone. Investigating the effect of phishing believability on phishing reporting. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 117–128. IEEE, 2022

21. Martino Tommasini, Martin Rosso, Emmanuele Zambon, Luca Allodi, and Jerry den Hartog. Characterizing building automation system attacks and attackers. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 139–149. IEEE, 2022

22. Pavlo Burda, Luca Allodi, and Nicola Zannone. A decision-support tool for experimentation on zero-hour phishing detection. In *International Symposium on Foundations and Practice of Security*, pages 443–452. Springer, 2022

23. Yoram Meijaard, Peter-Paul Meiler, and Luca Allodi. Modelling disruptive apts targeting critical infrastructure using military theory. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 178–190. IEEE, 2021

24. Pavlo Burda, Luca Allodi, and Nicola Zannone. Dissecting social engineering attacks through the lenses of cognition. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 149–160. IEEE, 2021

25. Bram Van Dooremaal, Pavlo Burda, Luca Allodi, and Nicola Zannone. Combining text and visual features to improve the identification of cloned webpages for early phishing detection. In *The 16th International Conference on Availability, Reliability and Security*, pages 1–10, 2021

26. 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

27. 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.**

28. 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.**

29. 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

30. 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

31. 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

32. 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` **Winner of the 2020 Best Paper Award for IEEE Security & Privacy**

33. 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.**

34. 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

35. 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

36. 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

37. 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

38. 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

39. 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.**

40. 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.**

41. 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.**

42. 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

43. 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

44. 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).**

45. 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`

46. 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`

47. 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

48. 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`

49. 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`

50. 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`

51. 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

52. 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**)

53. 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**)

54. 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

Other publications

55. 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/

56. 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

57. 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

58. 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

59. 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

60. 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

61. 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

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

63. 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 and committees

Since 2019 I am the Chair of the **Workshop on Attackers and Cyber-Crime Operations (WACCO)**, annually 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. I represent TUe in the IPN (ICT-research Platform Netherlands) Special Interest Group on Cyber Security (SIG-CS).

Teaching

I am the responsible lecturer for the 2IC80 course on Offensive Computer Security (OCS). I am also co-lecturer of the course *2IMS20 - Cyber-attacks, Crime, and Defenses* in 2019, held jointly with Prof. S. Etalle and the course *2IMS40 - Intrusion Detection Laboratory*, starting in Q3 2022/23, that I co-lecture with Dr. Emmanuele Zambon.

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, 2022; Invited reviewer for, among many others: MIS Quarterly; ACM TISSEC/TOPS; ACM DTRAP; IEEE TSE; ESEM; Risk Analysis; IEEE TDSCSI; Elsevier COSE; International Journal of Information Security.