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

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 assessment. I authored a modification to the standard for the main metric, the Base Score, which has been approved by the SIG and is now officially part of CVSSv3. 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.

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 prestigeous *Risk Analysis* journal, the flagship journal of the Society for Risk Analysis. I have a

single-author paper in *ESSoS 2015* and in *Usenix LEET 2013*. 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*.

Funding and involvement in research projects (2011-Pres.) I recently wrote a research proposal on attack economics for the CISCO Research Center funding programme. As a Ph.D. student I won several travel grants from international associations such as Usenix, ACM, and IEEE. I have also been granted unconditional funding from the University of Trento for my Ph.D. studies. During my Ph.D. I worked on the FP7 project SECONOMICS on social, cyber and physical security, and on the Italian PRIN TENACE project on security of critical infrastructures. Additionally, I have participated in the drafting of two European Projects.

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.

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`).

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`.

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 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).

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

5. Luca Allodi and Fabio Massacci. Attack potential in impact and complexity. In *To appear in the Proceedings of ARES 2017*, 2017

6. Luca Allodi, Fabio Massacci, and Julian Williams. The work-averse cyber attacker model. evidence from two million attack signatures. In *Published in WEIS 2017. Available at https://ssrn.com/abstract=2862299*, 2017

7. 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

8. 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

9. 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

10. 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

11. 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**)

12. 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**)

13. 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

14. 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/

15. 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

16. 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

17. 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`

18. 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`

19. 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`

20. 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`

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

22. 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

Work in progress

Identifying Relevant Information Cues for Vulnerability Assessment Using CVSS. L. Allodi, K. Beckers, S. Banescu, H. Femmer.
Using Security Event and Vulnerability Data for Quantitative Cyber Security Risk. With F. Massacci, and an undisclosed industry partner (financial organization).
The Work-Averse attacker model. Journal version. With F. Massacci and J. Williams.
An Empirical Analysis of the Impact of Security Knowledge in the Performance of Vulnerability Assessments Using CVSS v3. With F. Massacci, W. Shim, M. Cremonini.
Incomplete contracts, bounded rationality and the shadow of the future: Qualitative evidence from Russian hacker markets, with F. Massacci and J. Williams. (*In preparation*).

Grants

Participation Grant for BlackHat USA 2013 - $1500 (2013).

IEEE Travel Grant for the 2013 IEEE Symp. on Security and Privacy - $1500 (2013).

Usenix Travel Grant for the 2013 Usenix Security Conference - $300 (2013).

ACM Travel Grant for the ACM CCS 2012 Conference - $500 (2012).

UNITN Ph.D. Scholarship for my doctorate studies - €44200 (2011).

Student supervision

Zhongying Qiao (MSc Thesis). *Security impact modelling and analysis using quantitative incident data for large financial institutions.* University of Trento.

Martin Pozdena (MSc Thesis). *Collecting Actionable Threat Intelligence from Digital Underground.* University of Trento.

Marco Corradin (MSc Thesis). *Then and now: On the maturity of cybercrime markets.* University of Twente.

Francesco La Spina (MSc Project). *Applied Security Project - Exploiting Vulnerabilities in Firefox* (12 credits) University of Trento. `https://securitylab.disi.unitn.it/doku.php?id=course_on_offensive_technologies_2014`

Davide Martintoni (MSc Project). *Applied Security Project - Exploiting Vulnerabilities in Firefox* (6 credits course) University of Trento. `https://securitylab.disi.unitn.it/doku.php?id=course_on_offensive_technologies_2014`

Gabor Stefanik (MSc Project). *Testing software diversity with blackhat markets attack tools.* (18 credits 450 hours) University of Trento.

Luca Chiodi (BSc Thesis, in italian). *Comunicazione e conoscenza in reti sociali complesse: modellazione, simulazione ed analisi.* University of Milan.

Teaching courses and lectures

Courses

Network Security (Lecturer). *University of Trento.* `https://securitylab.disi.unitn.it/doku.php?id=course_netsec_2016` (2015-2016)

Security training for the Information Security Department of the Italian Republic (Lecturer). *Dates, location and material undisclosed.*

CVSSv3 training for professionals (Lecturer). *Oracle offices, Milan.* `https://securitylab.disi.unitn.it/doku.php?id=teaching_activities:cvss` (2016)

Cyber Security Management (Lecturer). *CINI Master in Cyber Security, Univ. of Cosenza.* (2015)

Offensive Technologies (TA). *University of Trento.* `https://securitylab.disi.unitn.it/doku.php?id=course_on_offensive_technologies` (2014-2017)

ICT Innovation (TA). *University of Trento.* `https://securitylab.disi.unitn.it/doku.php?`

`id=ict_innovation` (2014-2016)

Other lectures

Knowing the Attackers. Governmental Malware and Cybercrime. *Lecture at University of Trento, Italy.* (2014)

A techno-economic review of the Cybercrime black markets. *Lecture at University of Trento, Italy.* (2014)

Validation of an industry standard. Or: how compliance makes risk unaffordable. *Lecture at University of Milan, Italy.* (2013)

Risk metrics for vulnerabilities exploited in the wild. *Lecture at University of Milan DTI.* (2013)

Exploitation in the wild: what attackers really do, and what we should worry about. *Lecture at University of Rome Tor Vergata.* (2013)

Dynamic Social Networks. Modeling Trust, Shocks and Hype. *Lecture at University of Bologna. Engineering department of Cesena, Italy.* (2011)

Teaching module experience. Computer, Network and Software Security; IT risk management, assessment and compliance.

Presentations and seminars

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.

Research & professional experience

May 2015-Pres.: 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: ACM TISSEC/TOPS; IEEE TSE; Risk Analysis; IEEE TDSCSI; Elsevier COSE; International Journal of Information Security; ICIS 2016; MMM-ACNS-2012; PST-2012;

PC Member: IFIP Sec 2015, 2016; CRiSIS-2016.

Referees

Prof. Fabio Massacci. Full Professor, University of Trento, Italy.
email: fabio.massacci@unitn.it
phone: +39 0461 282086

Prof. Julian Williams. Chair of Finance, University of Durham, UK.
email: julian.williams@durham.ac.uk
phone: +44 (0) 191 33 45301

Prof. Marco Cremonini. Professor, University of Milan, Italy.
email: marco.cremonini@unimi.it
phone: +39 02 503 02503-30093

Darius Wiles. Vice Chair of FIRST's Common Vulnerability Scoring System Special Interest Group.
Senior Principal Security Analyst, Oracle
email: darius.wiles@oracle.com

Abstract of selected publications

The typical cyber attacker is assumed to be all powerful and to exploit all possible vulnerabilities. In this paper we present, and empirically validate, a novel and more realistic attacker model. The intuition of our model is that an attacker will optimally choose whether to act and weaponize a new vulnerability, or keep using existing toolkits if there are enough vulnerable users. The model predicts that attackers may i) exploit only one vulnerability per software version, ii) include only vulnerabilities with low attack complexity, and iii) be slow at introducing new vulnerabilities into their arsenal. We empirically test these predictions by conducting a natural experiment on attack data collected against more than one million real systems from Symantec's WINE platform. Our analysis shows that mass attackers' fixed costs are indeed significant and that substantial efficiency gains can be made by individuals and organizations by accounting for this effect.

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`
(U.S.) Rule-based policies for mitigating software risk suggest using the CVSS score to measure the risk of an individual vulnerability and act accordingly. A key issue is whether the danger score does actually match the risk of exploitation in the wild, and if and how such a score could be improved. To address this question, we propose using a case-control study methodology similar to the procedure used to link lung cancer and smoking in the 1950s. A case-control study allows the researcher to draw conclusions on the relation between some risk factor (e.g., smoking) and an effect (e.g., cancer) by looking backward at the cases (e.g., patients) and comparing them with controls (e.g., randomly selected patients with similar characteristics). The methodology allows us to quantify the risk reduction achievable by acting on the risk factor. We illustrate the methodology by using publicly available data on vulnerabilities, exploits, and exploits in the wild to (1) evaluate the performances of the current risk factor in the industry, the CVSS base score; (2) determine whether it can be improved by considering additional factors such the existence of a proof-of-concept exploit, or of an exploit in the black markets. Our analysis reveals that (a) fixing a vulnerability just because it was assigned a high CVSS score is equivalent to randomly picking vulnerabilities to fix; (b) the existence of proof-of-concept exploits is a significantly better risk factor; (c) fixing in response to exploit presence in black markets yields the largest risk reduction.

Cybercrime activities are supported by infrastructures and services originating from an underground economy. The current understanding of this phenomenon is that the cybercrime economy ought to be fraught with information asymmetry and adverse selection problems. They should make the effects that we observe every day impossible to sustain. In this paper we show that the market structure and design used by cyber criminals have evolved towards a market design that is similar to legitimate, thriving, on-line forum markets such as eBay. We illustrate this evolution by comparing the 'market regulatory mechanisms' of two underground forum markets: a failed market for credit cards and other illegal goods and another, extremely active marketplace for vulnerabilities, exploits, and cyber attacks in general. The comparison shows that cybercrime markets evolved from unruly, 'scam for scammers' market mechanisms to mature, regulated mechanisms that greatly favors trade

efficiency.

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`
Cybercrime attack tools (i.e. Exploit Kits) are reportedly responsible for the majority of attacks affecting home users. Exploit kits are traded in the black markets at different prices and advertising different capabilities and functionalities. In this paper we present our experimental approach in testing 10 exploit kits leaked from the markets that we deployed in an isolated environment, our *MalwareLab*. The purpose of this experiment is to test these tools in terms of resiliency against changing software configurations in time. We present our experiment design and implementation, discuss challenges, lesson learned and open problems, and present a preliminary analysis of the results.