Curriculum Vitae – Fabio Pierazzi, Ph.D.

Contact information:
System Security Research Lab (S2Lab)
King's College London, Department of Informatics
Bush House, Strand, London, WC2R 1ES

Homepage: `https://fabio.pierazzi.com`
Email: `fabio.pierazzi@kcl.ac.uk`

Research Interests:
– machine learning for systems security and malware analysis
– adversarial machine learning and concept-drift detection
– anomaly detection in large traffic networks

Current:

Visiting Research Associate at KCL 09/2018 – *current*
Systems Security Research Lab (S2Lab)
King's College London (KCL), UK
Supervisor: Prof. Lorenzo Cavallaro

PostDoctoral Research Assistant at RHUL 10/2017 – *current*
Systems Security Research Lab (S2Lab)
Royal Holloway, University of London, UK
Supervisors: Prof. Lorenzo Cavallaro and Prof. Johannes Kinder

Experience:

Research Grant on Big Data Security Analytics 01/2017 – 09/2017
CRIS and Department of Engineering "Enzo Ferrari"
University of Modena and Reggio Emilia, Italy
Supervisor: Prof. Michele Colajanni

Visiting Research Scholar at UMD 01/2016 – 11/2016
Department of Computer Science
University of Maryland, College Park, MD, USA
Supervisor: Prof. V.S. Subrahmanian

Research Grant on Cloud Security 06/2013 – 12/2013
Department of Engineering "Enzo Ferrari"
University of Modena and Reggio Emilia, Italy
Supervisor: Prof. Michele Colajanni

Education:

Ph.D. in Computer Science 01/2014 – 03/2017
University of Modena and Reggio Emilia, Italy
Advisor: Prof. Michele Colajanni

MSc in Computer Engineering and Science 2010 – 2013
University of Modena and Reggio Emilia, Italy
Graduation score: **summa cum laude**
Average exam score (similar to GPA, in Italy): **29.9/30.0**

BSc in Computer Engineering and Science 2007 – 2010
Department of Engineering "Enzo Ferrari"
University of Modena and Reggio Emilia, Italy
Graduation score: **summa cum laude**
Average exam score (similar to GPA, in Italy): **29.0/30.0**

High school scientific diploma, Italy 2002 – 2007
Graduation score: **100 out of 100**

Selected honors, scholarships and awards:

- Distinguished PC Member at IJCAI-ECAI 2018
- My Ph.D. Dissertation has been selected as the best among the Computer Science Ph.D. theses defended in 2017 in my alma mater, UniMoRe 05/2018
- Ranked 1st in the Admission list for the PhD program in ICT in UniMoRe, Italy 12/2013
  - Received 3-year scholarship for the period 01/2014–12/2016
- Best Paper Award @ SECURWARE 2013 08/2013
- Passed the public exam to practice as *Computer Engineer* in Italy 07/2013
- Award for outstanding MSc study achievements– UniMoRe, Italy a.y. 2011/2012

Publications:

- [USESec19] Feargus Pendlebury*, Fabio Pierazzi*, Roberto Jordaney, Johannes Kinder, Lorenzo Cavallaro, *TESSERACT: Eliminating Experimental Bias in Malware Classification across Space and Time*, **USENIX Security Symposium 2019**.
- [TDSC19] Chongyang Bai, Qian Han, Ghita Mezzour, Fabio Pierazzi, and V.S. Subrahmanian, *DBank: Predictive Behavioral Analysis of Recent Android Banking Trojans*, IEEE Transactions on Dependable and Secure Computing (TDSC), 2019.
- [CCS18-Poster] Feargus Pendlebury*, Fabio Pierazzi*, Roberto Jordaney, Johannes Kinder, Lorenzo Cavallaro, *POSTER: Enabling Fair ML Evaluations for Security*, **ACM CCS 2018 (poster)**.
- [TETC17] Giovanni Apruzzese, Fabio Pierazzi, Michele Colajanni, Mirco Marchetti, *Detection and threat prioritization of pivoting attacks in large networks*, IEEE Transactions on Emerging Topics in Computing (TETC), Special Issue on Cyber Security Threats and Defense Advances, 2017.
- [TDSC17] Tanmoy Chakraborty, Fabio Pierazzi, V.S. Subrahmanian, *EC2: Ensemble Clustering & Classification for predicting Android malware families*, IEEE Transactions on Dependable and Secure Computing (TDSC), 2017.
- [TIFS17] Sushil Jajodia, Noseong Park, Fabio Pierazzi, Andrea Pugliese, Edoardo Serra, Gerardo Simari, V.S. Subrahmanian, *A probabilistic logic for cyber deception*, IEEE Transactions on Information Forensics and Security, Nov. 2017.
- [CyCon17] Fabio Pierazzi, Giovanni Apruzzese, Michele Colajanni, Alessandro Guido, Mirco Marchetti, *Scalable architecture for online prioritisation of cyber threats*, IEEE International Conference on Cyber Conflicts, Tallinn, Estonia, Jun 2017.
- [ComNet16] Mirco Marchetti, Fabio Pierazzi, Michele Colajanni, Alessandro Guido, *Analysis of high volumes of network traffic for Advanced Persistent Threat detection*, Elsevier Computer Networks Journal, Jun 2016
- [CyCon16] Mirco Marchetti, Fabio Pierazzi, Alessandro Guido, Michele Colajanni, *Countering Advanced Persistent Threats through security intelligence and big data analytics*, IEEE International Conference on Cyber Conflicts, Tallinn, Estonia, Jun 2016
- [CoSe16] Fabio Pierazzi, Sara Casolari, Michele Colajanni, Mirco Marchetti, *Exploratory security analytics for anomaly detection*, Elsevier Computers & Security Journal, Feb 2016
- [NCCA15] Fabio Pierazzi, Andrea Balboni, Alessandro Guido, Mirco Marchetti, *The network perspective of cloud security*, IEEE Network Cloud Computing and Applications, Munich, Germany, Jun 2015
- [TCC14] Luca Ferretti, Fabio Pierazzi, Michele Colajanni, Mirco Marchetti, *Scalable architecture for multi-user encrypted SQL operations on cloud database services*, IEEE Transactions on Cloud Computing, Oct-Dec 2014.

- [HPCS14-LSAUC] Marcello Missiroli, Fabio Pierazzi, Michele Colajanni, *Security and privacy of location-based services for in-vehicle device systems*, IEEE High Performance Computing and Simulation (HPCS) – International Workshop on Location-based Services and Applications in Ubiquitous Computing, Bologna, Italy, Jul 2014.
- [TCC14] Luca Ferretti, Fabio Pierazzi, Michele Colajanni, Mirco Marchetti, *Performance and cost evaluation of an adaptive encryption architecture for cloud databases*, *IEEE Transactions on Cloud Computing*, Apr-Jun 2014
- [ISCC14] Luca Ferretti, Fabio Pierazzi, Michele Colajanni, Mirco Marchetti, Marcello Missiroli, *Efficient detection of unauthorized data modification in cloud databases*, IEEE Symposium Computers and Communications, Madeira, Portugal, Jun 2014
- [SECURWARE13] Luca Ferretti, Fabio Pierazzi, Michele Colajanni, Mirco Marchetti, *Security and confidentiality solutions for public cloud database services*, Conference Emerging Security Information, System and Technonology, Barcelona, Spain, Aug 2013
  Best Paper Award

Talks:

- (upcoming) Presentation of TESSERACT paper at USENIX Security Symposium, Santa Clara, USA, Aug 2019
- (invited) *Network security analytics for detection of advanced cyberattacks*[1], Dartmouth College, US, Nov 2017

Teaching:

- [RHUL (BSc)] Seminars on Machine Learning for Security as part of "*Malicious Software*" class, BSc Computer Science, Royal Holloway University of London, UK 2019
- [KCL (MSc)] Seminar on Authentication and Access Control for the "*Security Engineering*" class, MSc Computer Science, King's College London, UK 2018
- [RHUL (BSc)] Seminars and T.A. for the "*Malicious Software*" class (IY3840), BSc in Information Security, Royal Holloway, University of London, UK 2018
- [UNIMORE (MSc)] Several lectures and lab tutor for part of the "*Network Systems and Applications*" class, MSc in Computer Engineering, University of Modena and Reggio Emilia, Italy 2017
- [UNIMORE (MSc)] Seminars and T.A. for the "*Computer Security*" class, MSc in Computer Engineering, University of Modena and Reggio Emilia, Italy 2016
- [UNIMORE (MSc)] Several lectures and lab tutor for part of the "*Network Systems and Applications*" class, MSc in Computer Engineering, University of Modena and Reggio Emilia, Italy 2015
- [UNIMORE (MSc)] Seminars and T.A. for the "*Computer Security*" class, MSc in Computer Engineering, University of Modena and Reggio Emilia, Italy 2015
- [UNIMORE (MSc)] Seminars and T.A. for "*Network Systems and Applications*" class, MSc in Computer Engineering, University of Modena and Reggio Emilia, Italy 2014

Academic Service:

Technical Program Committee:

– IJCAI 2019
– AAAI 2019
– Poster track of IEEE Symp. S&P (Oakland) 2019
– IEEE Network Computing and Applications (NCA) 2019
– CARDS conference 2019
– IJCAI-ECAI — **Distinguished PC Member**[2] 2018
– IEEE Big Data Principles, Architectures & Applications Workshop 2018

[1] http://news.dartmouth.edu/events/event?event=49292
[2] https://www.ijcai-18.org/distinguished-members/

– IEEE Smart Industries Workshop (co-located with IEEE SmartComp 2018) 2018
– IEEE Network Computing and Applications (NCA) 2017

Shadow Technical Program Committee:
– IEEE Symp. Security & Privacy (S&P), *Oakland* 2019
– IEEE Symp. Security & Privacy (S&P), *Oakland* 2018

Workshop Chair:
– CARDS conference 2019

Artifact Evaluation PC:
– ACSAC 2018

Review service:
– IEEE Transactions on Information Forensics and Security (TIFS) 2017,2018,2019
– IEEE Transactions on Neural Networks and Learning Systems (TNNLS) 2018,2019
– IEEE Computational Intelligence Magazine (CIM) 2019
– Springer UK book Review 2019
– IEEE Transactions on Emerging Topics in Computational Intelligence (TETCI) 2018
– Elsevier Computer Networks Journal 2018
– Elsevier Journal of Information Security and Applications 2017,2018
– International Journal of Machine Learning and Cybernetics (JMLC) 2018
– Elsevier Expert Systems With Applications 2017
– IEEE Transactions on Computational Social Systems (TCSS) 2016

Sub-review service:
– USENIX Security Symposium 2019
– ACM WWW (TheWebConf) 2019
– IEEE Euro S&P 2019
– ACM CCS 2018
– ACSAC 2018
– Deep Learning for Security workshop (co-located IEEE S&P 2018) 2018
– ACM CODASPY 2018
– ARES Conference 2018
– IEEE Transactions on Cloud Computing (TCC) 2017
– IEEE International Conference on Communications (ICC) 2016
– IEEE NetSciCom 2016
– Elsevier Expert Systems With Applications 2015
– IEEE Network Computing and Applications (NCA) 2015

Participation to European projects:
– HORIZON2020: Analysis System for Gathered Raw Data (ASGARD) 2016,2017

Technical skills:

Security analytics:
– Python data science libraries, including pandas, scipy, scikit-learn, matplotlib, PyTorch
– Familiarity with R and Matlab for statistical analysis
– Collection and analysis of IDS alerts (Snort, Suricata, Bro) and IP netflows (nprobe)

Programming:
– Proficiency with Python and Java programming, GNU/Linux (Debian), Bash scripting
– Web programming (J2EE, AJAX, HTML, CSS, Javascript, API, OAuth, Google App Engine)
– Familiarity with C, C++, DBMS (MySQL, PostgreSQL)
– Experience of team development with code versioning (cvs, svn, git)

Languages: English: fluent
Italian: native speaker

Note: Academic references and full CV are available upon request.

Date: March 29, 2019