CURRICULUM VITAE - DR FABIO PIERAZZI

Office BH(N)7.16, King's College London, UK | +44 020 7848 2390 | fabio.pierazzi@kcl.ac.uk | https://fabio.pierazzi.com

RESEARCH INTERESTS

Dr Fabio Pierazzi is a Lecturer (Assistant Professor) in Cybersecurity at King's College London, where is also a member of the Cybersecurity group (CYS) and Systems Security Research Lab (S2Lab), and Programme Leader of the MSc in Cyber Security to ensure its quality and relevance. He has a strong track record of AI & security publications in peer-reviewed venues, including top journals and top conferences in the field (e.g., USENIX Security, IEEE S&P, IEEE TIFS, IEEE TDSC), and also serves in Program Committees of well-known venues including AAAI, IJCAI, ICML, ICLR, DLS, AISec, DIMVA, and ARES, plus served as journal reviewer in multiple occasions for IEEE TIFS and ACM TOPS among others. He has worked on cybersecurity since 2011, when he started his MSc thesis in applied cryptography for cloud database security. During his Ph.D. (2014–2017), he then focused on statistical methods for the detection of advanced attackers in large networks. Fabio's research interests now focus on behavioral modeling for anomaly detection, with particular emphasis on: machine learning for systems security (mostly malware analysis and network intrusion detection), adversarial machine learning, and adaptive attackers in highly non-stationary contexts. Moreover, Fabio has delivered many teaching and mentoring activities in security in different countries (mostly UK and Italy).

PROFESSIONAL EMPLOYMENT

Lecturer (Assistant Professor) in Cybersecurity — **Dept. Informatics, King's College London (KCL), UK** 🇬🇧
Research and Teaching in Computer Science, with focus on Cybersecurity — *Sept 2019 to present*

PostDoctoral Researcher — **Systems Security Research Lab (S2Lab), RHUL & KCL, UK** 🇬🇧
Working on Concept Drift and Adversarial ML (w/ Prof. Lorenzo Cavallaro and Prof. Johannes Kinder) — *Oct 2017 to Sep 2019*

PostDoctoral Researcher — **WEBLab, University of Modena, Italy** 🇮🇹
Working on Big Data Security Analytics for Network Intrusion Detection (w/ Prof. Michele Colajanni) — *Jan 2017 to Sep 2017*

Visiting Research Scholar — **Dept. Computer Science, University of Maryland - College Park, USA** 🇺🇸
Working on Cyber Deception and ML-based Malware Detection (w/ Prof. V.S. Subrahmanian) — *Jan 2016 to Nov 2016*

Research Assistant — **WEBLab, University of Modena, Italy** 🇮🇹
Working on Applied Cryptography for Cloud Database Security (w/ Prof. Michele Colajanni) — *June 2013 to Dec 2013*

EDUCATION

Ph.D. in Computer Science — **University of Modena, Italy** 🇮🇹
Thesis: Security analytics for prevention and detection of advanced cyberattacks (advisor: Prof. Colajanni) — *Jan 2014 to Mar 2017*

MSc in Computer Engineering and Science (110/110 cum laude) — **University of Modena, Italy** 🇮🇹
Average exam score (similar to GPA, in Italy): **29.9/30.0** — *Sep 2010 to Apr 2013*

- Thesis: Data confidentiality through adaptive encryption for cloud DataBase as a Service

BSc in Computer Engineering and Science (110/110 cum laude) — **University of Modena, Italy** 🇮🇹
Average exam score (similar to GPA, in Italy): **29.0/30.0** — *Sep 2007 to Nov 2010*

High School Scientific Diploma — **Liceo Scientifico Statale "A. Tassoni", Modena, Italy** 🇮🇹
Graduation score: **100/100** — *Sep 2002 to July 2007*

PUBLICATIONS

Conference Papers

S&P20 Fabio Pierazzi*, Feargus Pendlebury*, Jacopo Cortellazzi, Lorenzo Cavallaro, "*Intriguing Properties of Adversarial ML Attacks in the Problem-Space*", IEEE Symp. Security & Privacy (Oakland), 2020 — **12.3% Acceptance Rate**

USENIXSec19 Feargus Pendlebury*, Fabio Pierazzi*, Roberto Jordaney, Johannes Kinder, Lorenzo Cavallaro, "*TESSERACT: Eliminating Experimental Bias in Malware Classification across Space and Time*", USENIX Security, 2019 — **16% Acceptance Rate**

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 (CyCon), 2017.

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 (CyCon), 2016.

NCCA15 Fabio Pierazzi, Andrea Balboni, Alessandro Guido, Mirco Marchetti, "*The network perspective of cloud security*", IEEE Network Cloud Computing and Applications, 2015.

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, 2014.

SECURWARE13 Luca Ferretti, Fabio Pierazzi, Michele Colajanni, Mirco Marchetti, "*Security and confidentiality solutions for public cloud database services*", Conf. Emerging Security Information, System and Technology, Aug 2013 — ***Best Paper Award***

Journal Papers

TIFS20 Fabio Pierazzi, Stefano Cristalli, Danilo Bruschi, Michele Colajanni, Mirco Marchetti, Andrea Lanzi, "*GLYPH: Efficient ML-based Detection of Heap Spraying Attacks*", IEEE Trans. Information Forensics & Security (TIFS), 2020

TMIS20 Fabio Pierazzi, Ghita Mezzour, Qian Han, Michele Colajanni, V.S. Subrahmanian, "*A Data-Driven Analysis of Modern Android Spyware*", ACM Trans. Management Information Systems, 2020.

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.

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), 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.

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.

CoSe16 Fabio Pierazzi, Sara Casolari, Michele Colajanni, Mirco Marchetti, "*Exploratory security analytics for anomaly detection*", Elsevier Computers & Security, Feb 2016.

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 (TCC), 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 (TCC), 2014.

Workshop & Poster Papers

USENIXSec19-Poster Fabio Pierazzi*, Feargus Pendlebury*, Jacopo Cortellazzi, Lorenzo Cavallaro. "*POSTER: Realistic Adversarial ML Attacks in the Problem-Space*", USENIX Security Symposium (poster), 2019.

CCS18-Poster Feargus Pendlebury*, Fabio Pierazzi*, Roberto Jordaney, Johannes Kinder, Lorenzo Cavallaro, "*POSTER: Enabling Fair ML Evaluations for Security*", Proceedings of ACM CCS 2018 (poster paper).

HPCS14-LSAUC Marcello Missiroli, Fabio Pierazzi, Michele Colajanni, "*Security and privacy of location-based services for in-vehicle device systems*", International Workshop on Location-based Services and Applications in Ubiquitous Computing (LSAUC), as part of Proc. IEEE HPCS, 2014.

ACADEMIC SERVICE

Awards

- Outstanding Reviewer Award at DIMVA conference 2020
- Distinguished Program Committee Member at IJCAI-ECAI 2018

Program committees

2022 IEEE S&P (Oakland)

2021 AAAI, ICLR, ICML, DIMVA, ARES, DLS Workshop, DSN-DSML Workshop, EuroSec Workshop

2020 ICML, AAAI, IJCAI, DLS (S&P Workshop), DSML (DSN Workshop), DIMVA, MLCS (ECML-PKDD Workshop), EuroSec Workshop, ARES, SafeML (ECAI workshop), IEEE TrustCom, AISec (CCS Workshop), IEEE NCA, Poster/Demo Track of ACM CCS

2019 AAAI, IJCAI, AISec (CCS Workshop), Poster Track of IEEE S&P (Oakland), IEEE NCA, CARDS, Shadow PC of IEEE S&P (Oakland)

2018 IJCAI, IEEE Smart Industries Workshop, IEEE BDAA Workshop, Shadow PC of IEEE S&P (Oakland)

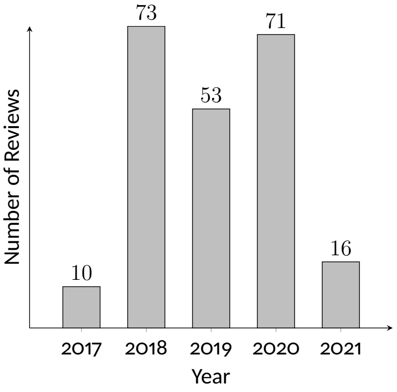

Figure 1: Papers reviewed from Nov 1, 2017 to Feb 15, 2021.

Artifact Evaluation PC

2018–2020 USENIX Security Symposium (2020), ACSAC (2018, 2019), SOSP (2019), USENIX WOOT Workshop (2019)

Guest Editor

2021-2022 Special Issue on "Offensive Machine Learning", ACM DTRAP journal

2021– Research Topic[1] on "Distributed Fog/Edge computing architectures for IoT applications" for *Frontiers in Communication and Networks* journal.

Editorial Board

2020– Frontiers in Communications and Networks

Journal Reviewing (selected)

2016–2021 ACM TOPS (2019-2021), IEEE TIFS (2017-2021), IEEE TNNLS (2017-2020), Elsevier JISA (2017-2020), IEEE TBD (2019), IEEE TCSS (2016), IEEE CIM (2019,2020), IEEE TETCI (2018), Elsevier ComNet (2018), Elsevier ESWA (2017), Elsevier FGCS (2019, 2021)

Publons Verified Reviews https://publons.com/researcher/3086392/fabio-pierazzi/

External Reviewer[2]

2021 USENIX Security

Sub-Reviewing

2020 ACSAC

2019 RAID, DIMVA, ACM WWW (TheWebConf), IEEE EuroS&P

[1] Similar to special issue, but without fixed deadlines and open-eded submission pool.

[2] Invited in the PC discussion for at least one paper

2018 ACM CCS, ACSAC, DLS (S&P Workshop), ACM CODASPY, ARES
2015–2017 IEEE TCC (2017), IEEE ICC (2016), IEEE NetSciCom (2016), Elsevier EWMA (2015), IEEE NCA (2015)

Other

• **Session Chair** at NCA 2020 in the “Network Security” session	Nov 2020
• **Session Chair** at ARES 2020 in the “ML for Cybersecurity” session	Aug 2020
• **Workshop Chair** of CARDS conference	2019

Ph.D. Thesis External Reviewer

• Francesco Crecchi, University of Cagliari, Italy	Feb 28, 2021

Ph.D. Defense Committee

• Marco Melis, Thesis in Computer Science, University of Cagliari, Italy	March 9, 2021
• Michele Scalas, Thesis in Computer Science, University of Cagliari, Italy	March 9, 2021
• Diego Deplano, Thesis in Automatic Control, University of Cagliari, Italy	March 9, 2021
• Stefano Sonedda, Thesis in Electronics, University of Cagliari, Italy	March 9, 2021

TALKS AND SEMINARS (SELECTED)

• Invited Talk (virtual) at Software Engineering Ph.D./PostDoc Winter School, Berlin, Germany 🇩🇪	Mar 2021
• ACE-CSR Winter Ph.D. School, UK 🇬🇧	Dec 2020
• Invited Talk (virtual) at Computing Colloquium of Boise State University, USA 🇺🇸	Oct 2020
• (peer-reviewed) Talk at AVAST’s CyberSec&AI workshop about TIFS20 paper, London/SF/Prague 🇬🇧 🇺🇸 🇨🇿	Oct 2020
• (invited) Dagstuhl Seminar on Security of Machine Learning (cancelled; postponed due to covid19) 🇩🇪	Aug 2020
• Invited Talk (virtual) at SoSySec seminar at INRIA, Rennes, France 🇫🇷	Jun 2020
• Invited Talk (virtual) at InfoSec Seminars at University College London, UK 🇬🇧	May 2020
• Invited Talk at ISG Seminars at Royal Holloway, University of London, UK 🇬🇧	Feb 2020
• Paper presentation of TESSERACT at USENIX Security Symposium, Santa Clara, USA 🇺🇸	Aug 2019
• Invited Talk “*Network security analytics for detection of advanced cyberattacks*”, Dartmouth College, USA 🇺🇸	Nov 2017

SELECTED HONORS, SCHOLARSHIPS AND AWARDS

• Outstanding Reviewer Award at DIMVA conference 2020	Jul 2020
• Distinguished Program Committee Member at IJCAI-ECAI 2018	Spring 2018
• Ph.D. Dissertation selected as the best among the dissertations of my UniMoRe CS cohort	2017
• Ranked 1st and awarded 3-year scholarship for CS Ph.D. at the University of Modena, Italy	From Jan 2014 to Dec 2016
• Best Paper Award @ SECURWARE 2013	Aug 2013
• Passed the public exam to practice as *Computer Engineer* in Italy	Jul 2013
• Award for outstanding MSc study achievements at University of Modena, Italy	a.y. 2011/2012

TEACHING EXPERIENCE

Module Leader/Creator

- **Security Testing (7CCSONST)** **MSc in Advanced Cyber Security (Online MSc), King’s College London, UK** 🇬🇧
  Module Creator *Spring 2022*
- **Security Testing (7CCSMSCT)** **MSc in Cyber Security, King’s College London, UK** 🇬🇧
  Module Leader and Module Creator *Spring 2020, Spring 2021*

Guest Lectures

- **Machine Learning for Security** **MSc Computer Science, Karlsruhe Institute of Technology (KIT), Germany** 🇩🇪
  Guest Lecture on “Concept Drift for Malware Classification” *Summer 2020*
- **Security Monitoring I: Malware Anaylsis and Detection** **Security Specialization Course, University of Bologna, Italy** 🇮🇹
  Guest lectures on static analysis, dynamic analysis, ML-based malware detection *Spring 2020, Spring 2021*
- **Machine Learning for Malware Analysis** **Cyber Academy, Specialization Course, University of Modena, Italy** 🇮🇹
  Guest lectures on ML-based malware detection *Spring 2019*
- **Malicious Software** **BSc Computer Science, Royal Holloway, University of London, UK** 🇬🇧
  Guest Lectures on “Machine learning for malware analysis” *Spring 2018, Spring 2019*
- **Security Engineering (7CCSMSEN)** **MSc Computer Science, King’s College London, UK** 🇬🇧
  Guest Lecture on “Authentication and Access Control” *Fall 2018*
- **Computer Security** **MSc Computer Engineering, University of Modena, Italy** 🇮🇹
  Guest Lectures on Network Security and Web Security, and Lab TAing *Fall 2015, Fall 2016*
- **Network Systems and Applications** **MSc Computer Engineering, University of Modena, Italy** 🇮🇹
  Several Guest Lectures on Cloud Computing, and Lab Design and TAing *Spring 2014, Spring 2015, Spring 2017*

OTHER RELEVANT ACADEMIC ROLES

Programme Leader of KCL MSc in Cyber Security Responsible of ensuring that the content is of quality and up-to-date, and meets NCSC accreditation criteria, while coordinating with the MSc programmes director for any challenge (KCL has one director for all MSc programmes). Since Oct 2020

TECHNICAL SKILLS IN SECURITY (SELECTED)

- Traffic and malware analysis with python data science libraries, including pandas, scipy, scikit-learn, matplotlib, PyTorch
- Advanced Penetration Testing of Web Applications (e.g., SQL injections, XSS, CSRF)
- Collection and analysis of Network IDS alerts (Snort, Suricata, Bro) and IP netflows (nprobe)
- Hands-on experience on monitoring real-world networks (up to 10k hosts)
- Malware execution and log analysis in Cuckoo sandbox (e.g., ransomaware)
- Web Security and Penetration Testing

LANGUAGES

- **English**: fluent
- **Italian**: native speaker

REFERENCES

Available upon request.

Date: March 5, 2021