







# CURRICULUM VITAE - DR FABIO PIERAZZI

Office BH(N)7.16, King's College London, UK | <https://fabio.pierazzi.com>




## RESEARCH INTERESTS

Dr Fabio Pierazzi is **Senior Lecturer (Associate Professor) in Cybersecurity** at King's College London (KCL), where he is also **Deputy Head of the Cybersecurity group** (since Sep 2022), and **Programme Leader of the MSc in Cyber Security** (since Fall 2020) to ensure its quality and relevance. He closely collaborates with the Systems Security Research Lab (S2Lab) at UCL. 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 IEEE S&P (Oakland), USENIX Security, ACM CCS, 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), and has taken the leadership in the application for NCSC Certification of KCL's MSc in Cyber Security, which in Spring 2021 resulted in a successful outcome.

## PROFESSIONAL EMPLOYMENT

<b>Senior Lecturer (Associate Professor) in Cybersecurity</b> <i>Research and Education in Computer Science, with focus on Cybersecurity</i>	<b>Dept. Informatics, King's College London (KCL), UK</b> 	<i>since Aug 2023</i>
<ul style="list-style-type: none"><li>• <b>Deputy Head of Cybersecurity Group</b></li><li>• <b>Programme Leader of MSc Cyber Security</b></li></ul>		<i>since Sep 2022</i> <i>since Fall 2020</i>
<b>Lecturer (Assistant Professor) in Cybersecurity</b> <i>Research and Education in Computer Science, with focus on Cybersecurity</i>	<b>Dept. Informatics, King's College London (KCL), UK</b> 	<i>Sep 2019–Jul 2023</i>
<b>Postdoctoral Researcher</b> <i>Working on Concept Drift and Adversarial ML</i>	<b>Systems Security Research Lab (S2Lab), RHUL &amp; KCL, UK</b> 	<i>Oct 2017 to Sep 2019</i>
<b>Postdoctoral Researcher</b> <i>Working on Big Data Security Analytics for Network Intrusion Detection</i>	<b>WEBLab, University of Modena, Italy</b> 	<i>Jan 2017 to Sep 2017</i>
<b>Visiting Research Scholar</b> <i>Working on Cyber Deception and ML-based Malware Detection</i>	<b>Dept. Computer Science, University of Maryland - College Park, USA</b> 	<i>Jan 2016 to Nov 2016</i>
<b>Research Assistant</b> <i>Working on Applied Cryptography for Cloud Database Security</i>	<b>WEBLab, University of Modena, Italy</b> 	<i>Jun 2013 to Dec 2013</i>

## EDUCATION

<b>Ph.D. in Computer Science</b> <i>Thesis: Security analytics for prevention and detection of advanced cyberattacks (advisor: Prof. Colajanni)</i>	<b>University of Modena, Italy</b> 	<i>Jan 2014 to Mar 2017</i>
<b>MSc in Computer Engineering and Science (110/110 cum laude)</b> <i>Average exam score (similar to GPA, in Italy): 29.9/30.0</i>	<b>University of Modena, Italy</b> 	<i>Sep 2010 to Apr 2013</i>
<b>BSc in Computer Engineering and Science (110/110 cum laude)</b> <i>Average exam score (similar to GPA, in Italy): 29.0/30.0</i>	<b>University of Modena, Italy</b> 	<i>Sep 2007 to Nov 2010</i>

## PUBLICATIONS (SELECTED)

Full list: <https://fabio.pierazzi.com/publications/>

### Journal Papers

- TIFS21** 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), 2021
- 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.
- 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.

### Conference Papers

- S&P23** Limin Yang, Zhi Chen, Jacopo Cortellazzi, Feargus Pendlebury, Kevin Tu, Fabio Pierazzi, Lorenzo Cavallaro, Gang Wang, "Jigsaw Puzzle: Selective Backdoor Attack to Subvert Malware Classifiers.", IEEE Symposium on Security & Privacy (Oakland), 2023
- SaTML23** Giovanni Apruzzese, Hyrum S. Anderson, Savino Dambra, David Freeman, Fabio Pierazzi, Kevin A. Roundy, "Position: "Real Attackers Don't Compute Gradients": Bridging the Gap Between Adversarial ML Research and Practice", IEEE Conference on Secure and Trustworthy Machine Learning, 2023

- USENIXSec22** Daniel Arp, Erwin Quiring, Feargus Pendlebury, Alexander Warnecke, Fabio Pierazzi, Christian Wressnegger, Lorenzo Cavallaro, Konrad Rieck. "Dos and Don'ts of Machine Learning in Computer Security", USENIX Security Symposium, 2022 — **16% Acceptance Rate** — **Distinguished Paper Award**
- S&P22** Federico Barbero\*, Feargus Pendlebury\*, Fabio Pierazzi, Lorenzo Cavallaro. "Transcending Transcend: Revisiting Malware Classification with Conformal Evaluation", IEEE Symp. Security and Privacy (Oakland), 2022 — **14.5% Acceptance Rate**
- 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 Symposium, 2019 — **16% Acceptance Rate**

#### Workshop & Poster Papers

- AISec23** Theo Chow, Zeliang Kan, Lorenz Linhardt, Lorenzo Cavallaro, Daniel Arp, and Fabio Pierazzi, *Drift Forensics of Malware Classifiers*, In Prof. of the ACM Workshop on Artificial Intelligence and Security (AISec), 2023
- AISec21** Giuseppina Andresini, Feargus Pendlebury, Fabio Pierazzi, Corrado Loglisci, Annalisa Appice, Lorenzo Cavallaro. "INSOMNIA: Towards Concept-Drift Robustness in Network Intrusion Detection", AISec Workshop (co-located with ACM CCS), 2021.
- AISec21** Zeliang Mark Kan, Feargus Pendlebury, Fabio Pierazzi, Lorenzo Cavallaro. "Investigating Labelless Drift Adaptation for Malware Detection", AISec Workshop (co-located with ACM CCS), 2021.

#### FUNDING (SELECTED)

- PI of project with Turing AICD (£90k)** Advisory Consultancy with Turing AI centre for Cyber Defense on "Open Challenges of Security of Deep Reinforcement Learning" 2023
- PI of EPSRC NIA (£393k)** EPSRC New Investigator Award (NIA) on "XAdv: Robust Explanations for Malware detection" 2023–2026
- PI of EPSRC-Toshiba iCASE (£124k)** EPSRC Industrial CASE (iCASE) Ph.D. Studentship co-funded by *Toshiba Research Europe Limited* on the topic of "Concept drift in distributed IIoT networks" 2021–2025

#### ACADEMIC SERVICE

##### Program Chair

- 2023** 2nd Workshop on Robust Malware Analysis (WoRMA), co-located with IEEE EuroS&P 2023
- 2022** 1st ACM Workshop on Robust Malware Analysis (WoRMA), co-located with ACM AsiaCCS

##### Workshop Chair

- 2023** IEEE EuroS&P

##### Program committees (Selected)

- 2024** IEEE S&P (Oakland), USENIX Security, IEEE SaTML, ICLR, ML4Cyber Workshop (co-located with ICDM)
- 2023** IEEE S&P (Oakland), USENIX Security, ACM CCS, IEEE SaTML, EuroSec, DLSP, DIMVA
- 2022** IEEE S&P (Oakland), USENIX Security, ACM CCS, ICML, DIMVA, AI4Cyber/MLHat (co-located KDD), AISec (CCS Workshop)
- 2021** NeurIPS, AAAI, ICLR, ICML, DIMVA, ARES, DLS Workshop, EuroSec Workshop, KDD-MLHat Workshop, AISec
- 2020** ICML, AAAI, IJCAI, DLS (S&P Workshop), DIMVA, EuroSec Workshop, AISec (CCS Workshop), Poster/Demo Track of ACM CCS
- 2019** AAAI, IJCAI, AISec (CCS Workshop), Poster Track of IEEE S&P (Oakland), Shadow PC of IEEE S&P (Oakland)
- 2018** IJCAI, Shadow PC of IEEE S&P (Oakland)

##### Artifact Evaluation PC

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

#### TALKS, SEMINARS AND COLLOQUIUMS (SELECTED)

##### Invited Talks

- MLSec Seminars organized by University of Cagliari  April 2022
- Official CyBOK Webinar for "Malware and Attack Technologies" Knowledge Area, UK  Mar 2021
- Software Engineering Ph.D./PostDoc Winter School, Berlin, Germany  Mar 2021
- Computing Colloquium of Boise State University, USA  Oct 2020
- SoSySec seminar at INRIA, Rennes, France  Jun 2020
- InfoSec Seminars at University College London, UK  May 2020
- "Network security analytics for detection of advanced cyberattacks", Dartmouth College, USA  Nov 2017

##### Discussion Colloquiums

- Dagstuhl Seminar on Security of Machine Learning  Jul 2022
- AISecAI, King's College London, UK  Jan 2020

#### SELECTED HONORS, SCHOLARSHIPS AND AWARDS

- Distinguished Reviewer Awards at: CCS 2022, NeurIPS 2021, DIMVA 2020, DDIMVA 2021, IJCAI 2018 2018–2023
- Distinguished Paper Award @ USENIX Security Symposium Aug 2022
- Ph.D. Dissertation selected as the best among the dissertations of my computer science cohort at UniMoRe 2017
- Ranked 1st and awarded 3-year scholarship for CS Ph.D. at the University of Modena, Italy From Jan 2014 to Dec 2016

Date: **September 11, 2023**