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 **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

Senior Lecturer (Associate Professor) in Cybersecurity   **Dept. Informatics, King's College London (KCL), UK** 🇬🇧
Research and Education in Computer Science, with focus on Cybersecurity   *since Aug 2023*
- **Deputy Head of Cybersecurity Group**   *since Sep 2022*
- **Programme Leader of MSc Cyber Security**   *since Fall 2020*

PREVIOUS EMPLOYMENT

Lecturer (Assistant Professor) in Cybersecurity   **Dept. Informatics, King's College London (KCL), UK** 🇬🇧
Research and Education in Computer Science, with focus on Cybersecurity   *Sep 2019–July 2023*
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)   *Jun 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*

RESEARCH TEAM

Current Ph.D. students (First Supervisor)

Jacopo Cortellazzi Problem-space Adversarial Robustness, King's College London, UK   Started Fall 2019; defense expected Sep 2024

Zeliang Mark Kan Concept drift anticipation, King's College London, UK   Started Fall 2019; defense expected Sep 2024
Mohamed Abouhashem Federated Learning Security, King's College London, UK   Started Summer 2021
Theo Hoifung Chow Explainability and Adversarial Robustness, King's College London, UK   Started Fall 2021
Shae McFadden Security of Deep Reinforcement Learning, King's College London, UK   Started Fall 2023
Xin Fan Guo Model-driven IoT intrusion detection, King's College London, UK   Started Fall 2023

Research Visitors

Alessandro Sanna Ph.D. Student, University of Cagliari, Italy   Feb 2024–May 2024
Hamid Bostani Ph.D. Student, Radboud University, Netherlands   Oct 2023–Mar 2024
Marcello Maugeri Ph.D. Student, University of Catania, Italy   Oct 2023–Mar 2024
Feng Wei Ph.D. Student, University at Buffalo, USA   Oct 2023–Mar 2024
Mario D'Onghia Ph.D. Student, University of Milan, Italy   May–Nov 2023

Malik Al-Essa Ph.D. student, University of Bari, Italy   Mar–Sep 2023
Dr. Daniel Arp PostDoctoral Researcher, TU Berlin, Germany   Sep 2022–Jun 2023
Ilias Tsingenopoulos Ph.D. student, KU Leuven, Belgium   Jan–Apr 2023
Giuseppina Andresini Ph.D. student, University of Bari, Italy   2021
Harivallabha Rangarajan MSci student, BITS Pilani, Hyderabad Campus, India   2021

Ph.D. Alumni as Second Supervisor

Feargus Pendlebury Limitations of ML for Security, UCL & Royal Holloway, University of London, UK   2017–2021

PUBLICATIONS

Conference Papers

ICRA24 Wenxi Wu, Fabio Pierazzi, Yali Du, Martim Brandao, "*Characterizing Physical Adversarial Attacks on Robot Motion Planners*", IEEE International Conference on Robotics and Automation (ICRA), 2024

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 (Position Paper, 26 pages) Giovanni Apruzzese, Hyrum S. Anderson, Savino Dambra, David Freeman, Fabio Pierazzi, Kevin A. Roundy, "*"Real Attackers Don't Compute Gradients": Bridging the Gap Between Adversarial ML Research and Practice*", IEEE Conference on Secure and Trustworthy Machine Learning, 2023

IMC22 (Short Paper, 7 pages) Jide Edu, Cliona Mulligan, Fabio Pierazzi, Jason Polakis, Guillermo Suarez-Tangil, Jose Such, "*Exploring the Security and Privacy Risks of Chatbots in Messaging Services*", ACM Internet Measurement Conference (IMC), 2022 — 26.4% Acceptance Rate

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 in the Presence of Concept Drift*", 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**

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, 2013 — **Best Paper Award**

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 Characterization 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

DLSP24 Shae McFadden, Marcello Maugeri, Chris Hicks, Vasilis Mavroudis, and Fabio Pierazzi, "*Wendigo: Deep Reinforcement Learning for Denial-of-Service Query Discovery in GraphQL*", In Proc. of the IEEE Workshop on Deep Learning Security and Privacy (DLSP), 2024

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

CCS23-Poster Shae McFadden, Zeliang Kan, Lorenzo Cavallaro, Fabio Pierazzi, "*Poster: RPAL-Recovering Malware Classifiers from Data Poisoning using Active Learning*", Proceedings of ACM CCS 2023 (poster paper).

DLSP23 Zhi Chen, Zhenning Zhang, Zeliang Kan, Limin Yang, Jacopo Cortellazzi, Feargus Pendlebury, Fabio Pierazzi, Lorenzo Cavallaro, Gang Wang, *Is It Overkill? Analyzing Feature-Space Concept Drift in Malware Detectors*, Deep Learning Security & Privacy Workshop (co-located with IEEE S&P), 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.

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.

FUNDING

Funding as PI

PI: £60k fEC – Project with ATI's DARe   Research Project on "ML Model Vulnerabilities in Systems Security" with Alan Turing Institute's Defence Artificial Intelligence Research Centre   Oct 2023–Mar 2024

PI: £120k incl. VAT – Project with ATI's AICD   Advisory Consultancy with Alan Turing Institute's AI centre for Cyber Defense on "Open Challenges of Security of Deep Reinforcement Learning"   Apr 2023–Mar 2024

PI: £393k fEC – EPSRC NIA   EPSRC New Investigator Award (NIA) on "XAdv: Robust Explanations for Malware detection"
                                                                                                                                       Oct 2023–Sep 2026

PI: £124k fEC – EPSRC-Toshiba iCASE   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

Funding as Co-I

Co-I: £349k fEC – InnovateUK's KTP between KCL and ControlPlane   Project: "KTP - KubeSec-AFM: Kubernetes Security Assurance Through Formal Methods", led by Prof. Luca Viganò (KCL), and with ControlPlane (`https://control-plane.io`).
                                                                                               accepted Jan 2024; start date TBC (duration: 2 years)

ACADEMIC SERVICE

Service-related Awards

- **Notable Reviewer at IEEE SaTML 2023**
- **Top Reviewer ACM CCS 2022** (Top 30 out of 300+ reviewers; automatically invited to ACM CCS 2023 TPC)
- **NeurIPS 2021 Outstanding Reviewer Award** (Top 8% of reviewers)
- **Top 10 Reviewers at DIMVA 2021 conference**
- **Outstanding Reviewer Award at DIMVA 2020 conference**
- **Distinguished Program Committee Member at IJCAI-ECAI 2018**

Founder and Program Co-Chair

2024 3nd Workshop on Rethinking Malware Analysis (WoRMA), co-located with IEEE EuroS&P 2024 – `https://worma.gitlab.io/2024/`

2023 2nd Workshop on Robust Malware Analysis (WoRMA), co-located with IEEE EuroS&P 2023

2022 1st Workshop on Robust Malware Analysis (WoRMA), co-located with ACM AsiaCCS 2022

Workshop Chair

2023 IEEE EuroS&P

Program committees

2024 IEEE S&P (Oakland), USENIX Security, IEEE SaTML, ML4Cyber Workshop (co-located with ICDM), DIMVA, DLSP workshop

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, SYSTOR, AI4Cyber/MLHat (co-located KDD), AISec (CCS Workshop), IEEE NCA

2021 NeurIPS, AAAI, ICLR, ICML, DIMVA, ARES, DLS Workshop, DSN-DSML Workshop, EuroSec Workshop, KDD-MLHat Workshop, AISec, IEEE NCA

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)

Artifact Evaluation PC

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

Distinguished Reviewers Committee (Journals)

2021–2024 ACM TOPS

Journal Reviewing (selected)

2016–2024 ACM TOPS (2019-2024), IEEE TIFS (2017-2024), IEEE TDSC (2022), 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 (Invited in the PC discussion for at least one paper)

2021 USENIX Security

Sub-Reviewing

2020 ACSAC

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

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 ACM CCS 2023 in the "Language Models & Verification" session — Nov 2023
- **Session Chair** at IEEE S&P 2022 in the "Attack Investigations" session — May 2022
- **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

Ph.D. Thesis External Reviewer

- Angelo Sotgiu, University of Cagliari, Italy — Nov 2022
- Maura Pintor, University of Cagliari, Italy — Nov 2021
- Francesco Crecchi, University of Cagliari, Italy — Feb 2021

Ph.D. Defense Committee (External Examiner)

- Sergio Esposito, Royal Holloway, University of London, UK — Jul 18, 2023
- Marcos Tileria Palacios, Royal Holloway, University of London, UK — Apr 21, 2023
- Angelo Sotgiu (and other students), University of Cagliari, Italy — Feb 16, 2023
- Marco Melis, Michele Scalas, Diego Deplano, Stefano Sonedda, University of Cagliari, Italy — Mar 9, 2021

TALKS, SEMINARS AND COLLOQUIUMS (SELECTED)

Public Engagement and Dissemination

- Interview at TG2 (≈Italian BBC2) on my research on malware analysis with machine learning 🇮🇹 — June 2023
- King's AI Festival – Demonstration titled "AI for Malware Detection: How Machine Learning Can Keep Your Computer Safe" (https://www.kcl.ac.uk/events/ai-malware-detection) 🇬🇧 — 27 May 2023
- Robust Intelligence Webinar on IEEE SaTML 2023 paper 🇺🇸 — Feb 2023
- Computerphile YouTube video on "Machine Learning & Malware Analysis" 🇬🇧 — Jan 2023
- Official CyBOK Webinar for "Malware and Attack Technologies" Knowledge Area, UK 🇬🇧 — Mar 2021

Invited Talks

- Summer School on "Security and Privacy in the Age of AI", KU Leuven — September 2023
- MLSec Seminars organized by University of Cagliari 🇮🇹 — April 2022
- Software Engineering Ph.D./PostDoc Winter School, Berlin, Germany 🇩🇪 — Mar 2021
- ACE-CSR Winter Ph.D. School, UK 🇬🇧 — Dec 2020
- 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
- ISG Seminars at Royal Holloway, University of London, UK 🇬🇧 — Feb 2020
- "*Network security analytics for detection of advanced cyberattacks*", Dartmouth College, USA 🇺🇸 — Nov 2017

Discussion Colloquiums

- Robust Intelligence Webinar on IEEE SaTML 2023 paper 🇺🇸 — Feb 2023
- Panel Member on AI Security at "Deep Learning for Security" (DLS) workshop, co-located with IEEE S&P 🇺🇸 — May 2022
- Dagstuhl Seminar on Security of Machine Learning 🇩🇪 — Jul 2022
- Security Data Science Colloquium (SDSC) organized by Microsoft 🇺🇸 — Jun 2021

- AISecAI, King's College London, UK 🇬🇧   Jan 2020

SELECTED HONORS, SCHOLARSHIPS AND AWARDS

- Notable Reviewer at IEEE SaTML 2023   Feb 2023
- Top Reviewer at ACM CCS 2022   Nov 2022
- Distinguished Paper Award @ USENIX Security Symposium   Aug 2022
- NeurIPS 2021: Outstanding Reviewer Award (Top 8% Reviewers)   Oct 2021
- Top-10 reviewers of DIMVA 2021   Jul 2021
- 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 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
- 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

Education-related Roles

- **Programme Leader of MSc in Cyber Security**   **MSc in Cyber Security, King's College London, UK** 🇬🇧
  Responsible of ensuring that the content is of quality and up-to-date, and meets NCSC certification criteria.   *Since Fall 2020*
- **NCSC Certification Lead**   **MSc in Cyber Security, King's College London, UK** 🇬🇧
  I have been the leader of the application for NCSC certification for MSc *with general, broad foundation in Cyber Security for the King's College London's* MSc in Cyber Security, *successfully awarded in Spring 2021.*   *Since Fall 2019*
- **Mitigating Circumstances Board**   **Computer Science Programmes, King's College London, UK** 🇬🇧
  Review and approval for students assessment mitigations.   *Fall 2019–Summer 2021*

Module Leader/Creator

- **Security Testing (7CCSMSCT)**   **MSc in Cyber Security, King's College London, UK** 🇬🇧
  Module Leader and Module Creator   *Spring 2020, 2021, 2022, 2023, 2024*
- **Security Testing (7CCSONST)**   **MSc in Advanced Cyber Security (Online MSc), King's College London, UK** 🇬🇧
  Module Creator   *Spring 2022*

Dissertation Supervisor

King's College London, UK Supervised 19 MSc and 21 BSc dissertations.   2019–ongoing
Royal Holloway, University of London Second supervisor of 1 MSc dissertation.   2018
University of Modena, Italy Second supervision of 4 MSc dissertation, and 1 BSc dissertation.   2015–2017

Guest Lectures and Short Courses

- **Risk Assessment of Machine Learning for Cybersecurity**   **University of Bologna, Italy** 🇮🇹
  Short Ph.D. course   *May 2023, April 2024*
- **Robust Machine Learning for Cybersecurity**   **University of Cagliari, Italy** 🇮🇹
  Short Ph.D. course   *June 2023*
- **Security Monitoring I: Malware Anaylsis and Detection**   **Specialization Course, University of Bologna, Italy** 🇮🇹
  Guest Lectures on static analysis, dynamic analysis, ML-based malware detection   *Spring 2020, 2021, 2022, 2023, 2024*
- **Cybersecurity**   **MSc Computer Science, University of Bologna, Italy** 🇮🇹
  Guest Lecture on "Trends and Challenges in Automated Malware Detection"   *Fall 2021, 2022*
- **Machine Learning for Security**   **MSc Computer Science, Karlsruhe Institute of Technology (KIT), Germany** 🇩🇪
  Guest Lecture on "Concept Drift for Malware Classification"   *Summer 2020, 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*

LANGUAGES

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

Date: **March 27, 2024**