Professor Dr Lorenzo Cavallaro September

Professor of Computer Science
WWW https://s2lab.cs.ucl.ac.uk/people/sullivan
Systems Security Research Lab https://s2lab.cs.ucl.ac.uk
Google Scholar Profile https://scholar.google.co.uk/citations?user=oWT7fIYAAAAJ&hl=en
Department of Computer Science, UCL Euston Road, London, UK

Research Vision

My research vision is to develop **learning-based methods** that are **robust against adversaries**. We can achieve this by understanding the **interplay program analysis, representations, and machine learning models** play towards realizing **Trustworthy AI for Systems Security**.

Education

PhD in Computer Science **University of Milan**
Supervisors: Professor R. Sekar (Stony Brook University) and Professor Danilo Bruschi (University of Milan) Apr
BSc/MSc in Computer Science (-year integrated, **Summa Cum Laude**) **University of Milan**
Advisor: Professor Danilo Bruschi (University of Milan) Feb

Employment and Experience (Selected)

Professor of Computer Science **UCL**
Full Professor Aug –
Adjunct Professor **Zhejiang University**
Adjunct Professor Jun –
Professor of Computer Science, Chair in Cybersecurity (Systems & Security) **King's College London**
Full Professor Sep –Jul
Professor of Information Security **Royal Holloway, University of London**
Full Professor Jan –Aug
Reader in Information Security (Associate Professor) **Royal Holloway, University of London**
Equivalent to tenured Associate Professor++ Jan –Dec
Senior Lecturer in Information Security **Royal Holloway, University of London**
Equivalent to tenured Associate Professor-- Jan –Dec
Lecturer **Royal Holloway, University of London**
Equivalent to tenured Assistant Professor Jan –Dec

Awards (Selected)

Distinguished Paper Award **USENIX Security**
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
Outstanding Reviewer Award **NeurIPS**
(Top % Reviewers)

Research Grants (Selected)

Unrestricted Gift (Principal Investigator) Jun –present
Google ASPIRE Award ,000
Unrestricted Gift (Principal Investigator) ,000
AVAST Jan –present
EPSRC iCASE PhD Studentship (Principal Investigator) ,000
Toshiba Oct –Sep
NCSC ACE-CSR Small Grants (Principal Investigator) ,000
Workshop on AI for Security and the Security of AI Jun –Mar
(guests from UCL, Imperial College London, King's, University of Toronto, University of Cagliari, Google, Facebook, Huawei, AVAST)

MobSec: Malware and Security in the Mobile Age (Principal Investigator) ,
BACCHUS Call Nov –Nov
EPSRC Research Grant at KCL https://gow.epsrc.ukri.org/NGBOViewGrant.aspx?GrantRef=EP/L022710/2
EPSRC Research Grant at RHUL https://gow.epsrc.ukri.org/NGBOViewGrant.aspx?GrantRef=EP/L022710/1

NCSC ACE-CSR Small Grants (Principal Investigator) ,000
SLab Research Infrastructure Dec –Jan

NCSC ACE-CSR Small Grants (Principal Investigator) ,
SLab Research Infrastructure Dec –Jan

Mining the Network Behaviour of Bots (Principal Investigator) ,
CERES Call Jun –Dec
EPSRC Research Grant http://gow.epsrc.ac.uk/NGBOViewGrant.aspx?GrantRef=EP/K033344/1

Publications (Selected)

[IEEE S&P 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.** th IEEE Symposium on Security and Privacy, May

[DLSP@IEEE S&P Zhi Chen and Zhenning Zhang and Zeliang Kan and Limin Yang and and Jacopo Cortellazzi and Feargus Pendlebury and Fabio Pierazzi and Lorenzo Cavallaro and Gang Wang. **Is It Overkill? Analyzing Feature-Space Concept Drift in Malware Detectors.** th Deep Learning Security and Privacy Workshop, May

[USENIX Sec Daniel Arp, Erwin Quiring, Feargus Pendlebury, Alexander Warnecke, Fabio Pierazzi, Christian Wressnegger, Lorenzo Cav- allaro, and Konrad Rieck. **Dos and Don'ts of Machine Learning in Computer Security.** nd USENIX Security Symposium – **Distinguished Paper Award** (top % of accepted papers), Aug

[IEEE S&P Federico Barbero, Feargus Pendlebury, Fabio Pierazzi, and Lorenzo Cavallaro. **Transcending Transcend: Revisiting Malware Classification in the Presence of Concept Drift.** rd IEEE Symposium on Security and Privacy, May

[AISec@CCS Zeliang Kan, Feargus Pendlebury, Fabio Pierazzi, and Lorenzo Cavallaro. **Investigating Labelless Drift Adaptation for Mal-ware Detection.** th ACM Workshop on Artificial Intelligence and Security, Nov

[IEEE S&P Fabio Pierazzi, Feargus Pendlebury, Jacopo Cortellazzi, and Lorenzo Cavallaro. **Intriguing Properties of ML Adversarial Attacksin the Problem Space.** st IEEE Symposium on Security and Privacy, May

[USENIX Sec Feargus Pendlebury, Fabio Pierazzi, Roberto Jordaney, Johannes Kinder, and Lorenzo Cavallaro. **TESSERACT: Eliminating Experimental Bias in Malware Classification across Space and Time.** th USENIX Security Symposium, Aug

Professional Service (Selected)

Steering Committee
DIMVA –present
NDSS –present

Associate Editor
ACM TOPS –present
Computer & Security –present

Program Co-Chair
DIMVA –
IEEE Deep Learning and Security (co-located with IEEE Symposium on Security and Privacy) –
ACM EuroSec (co-located with ACM EuroSys) –

Program Committees
USENIX Sec, NDSS
USENIX Sec, ICLR, SaTML, PATTERN, ACSAC, RAID
IEEE S&P, USENIX Sec, ACM CCS, RAID, ICLR, NeurIPS
IEEE S&P, USENIX Sec, NeurIPS, ICLR, ACM CCS, ESORICS, RAID

Keynotes and Invited Talks (Selected)

Trustworthy AI... for Systems Security
Keynote at Deep Learning Security and Privacy , co-located with IEEE S&P

Transcending Transcend: Revisiting Malware Classification in the Presence of Concept Drift
University of Luxembourg ()

Trustworthy ML for Systems Security
KASTEL Distinguished Lecture Series, Karlsruhe Institute of Technology (Jun), UCL ACE-CSR Open Day (Jun), Informal ML Security Symposium, Imperial (Jun), Ohio State University (May)

Dos and Don'ts of Machine Learning in Computer Security
Keynote Talk at HP Colloquium Day (Dec)