

Luca Arnaboldi

RESEARCHER IN VERIFIABLY SECURE ML SYSTEMS ·✦· COMPUTING PEDAGOGIST

✉ l.arnaboldi@bham.ac.uk | 🏠 www.arnaboldiluca.eu | 🗣 yiergot | 📠 luca-arnaboldi-829083b2 | 🎓 Luca Arnaboldi

Summary

I am a researcher and educator specializing in the security of autonomous systems, and the formal verification of machine learning algorithms, with a strong focus on delivering real-world impact through innovation and industry engagement. My work has contributed to the development of internationally adopted tools, and two internally shortlisted REF impact case studies. I have secured competitive grants, including two EPSRC IAA's and Innovate UK funding, to bridge academic research and practical applications. In collaboration with industry partners, I have addressed critical challenges in secure software development, IoT security, and automated verification, with outcomes influencing best practices and regulatory standards. As an award-winning educator, I employ hybrid and blended teaching methods to inspire the next generation of computing professionals. My ongoing efforts include translating cutting-edge research into two academic spinouts, ensuring my work continues to drive innovation and societal benefit.

Academic Experience

University of Birmingham

Birmingham, UK

ASSISTANT PROFESSOR

Feb. 2023 - now

- **Leading research in:** Verification, Security and AI
- **Grants:** over £1.2 million secured as PI across diverse competitive funding sources (EPSRC, DSTL, Innovate UK, ARIA etc)
- **Teaching:** Co-lead Malware, Forensics and Penetration Testing (MSc) and Networks and System Security (UG2)
- **Supervision:** four PhD students on applied and theoretical AI/Security and eleven research assistants (grant funded)
- **Governance:** QS Lead and Director of PGR Experience for the school
- **Impact:** Two internally shortlisted Impact Case Studies for REF 2029, two expected academic spinouts (as outcome of funding), accepted into CyberASAP Pathfinder 2025 (Innovate UK), various media appearances and invited talks

University of Edinburgh

Edinburgh, UK

UNIVERSITY TEACHER (PART TIME)

Jan. 2022 - May 2022

- Module Leader for Msc Course on Secure Programming
- 100% Strongly Agree ratings for module leadership and course content
- Informatics Staff Award

Heriot Watt University

Edinburgh, UK

VISITING SCHOLAR (PART TIME)

Aug. 2021 - Dec. 2022

- Researching and co-supervising Msc projects on Autonomous Systems
- Impact: Media interviews and Showcase at the Edinburgh Science Festival

University of Edinburgh

Edinburgh, UK

RESEARCH ASSOCIATE

Dec. 2020 - Feb. 2023

- Working on Security and Verification of Autonomous Systems
- Output: several papers incl. one Q1 journal and two core ranked conferences (one A and one B), Internationally recognised research tool, media and industry engagements

Industry (R&D) Experience

Zeroth Research

Birmingham, UK

FOUNDER AND DIRECTOR (PART TIME)

Jul. 2025 - now

- Running a company focused on AI Safeguarding (grant funded).

DSTL (via BAE Systems)

Edinburgh, UK

SECURITY RESEARCH CONSULTANT (PART TIME)

Jul. 2022 - Feb. 2023

- Consulting in the area of software protection via automated rewriting.

ARM, Ltd.

Cambridge, UK

RESEARCH INTERN

Aug. - Dec. 2018

- First formal model of the ACE-OAuth implementation, using formal tool Tamarin published at OAuth workshop 2019
- Impact: Designated Expert for Internet Engineering Task Force (IETF) Authentication for Constrained Environments (ACE) WG

ARM, Ltd.

Cambridge, UK

RESEARCH INTERN

Aug. - Nov. 2017

- Ran in depth threat modelling and risk assessment for firmware update protocols in IoT, found and fixed flaws
- Proposed first of its kind scheme to protect against update reuse through proof of freshness

Education

Newcastle University, Secure & Resilient Systems

PHD IN COMPUTER SCIENCE

Newcastle upon Tyne, UK

Oct. 2016 - Dec. 2020

- **Thesis:** *A Methodology for the Quantitative Evaluation of Attacks and Mitigations in IoT Systems*
industry partner: ARM Ltd. **Supervisor:** Dr. C. Morisset, **Examiners:** Prof. S. Etalle and Prof. A. van Moorsel

Newcastle University

BSc HONS IN COMPUTER SCIENCE, 1ST CLASS

Newcastle upon Tyne, UK

Sep. 2013 - June. 2016

- **Dissertation:** *Feature Engineering For an Industrial Data Mining Challenge*
industry partner: XACT Ltd. **Supervisor:** Dr. J. Bacardit

Grants – Total: £1.3million~

Zero Knowledge Attestation for AI Security

Foresight Research

PI (AWARDED)

Jan 2026

- Runs Formal Verification of AI models running on trusted enclaves
- Accountability for AI systems in critical environments
- **Value:** \$161,376.60

Formal Certification Technologies for AI Safety

Manifund Grants

CO-PI (AWARDED)

Nov 2025

- Formal proof certificates for complex specifications that define the safety of probabilistic cyber-physical systems
- Donation to create the future of safe AI
- **Value:** \$128,000

A Unified Theoretical and Assurance Framework for SNNs in Defence Contexts

Defence Science and Technology

Laboratory

PI (AWARDED)

October 2025

- A robust theoretical and practical framework for understanding, certifying, and safely deploying Spiking Neural Networks (SNNs) within Defence and Security (D&S) environments
- **Value:** £150,000

Infrastructure for Safeguarded AI Systems

ARIA Safeguarded AI Grant

PI (AWARDED)

Jul 2025

- Builds a verification stack for AI systems capable of producing and checking formal proof certificates.
- Combines SMT, BnB, and ITP methods for validating security and correctness of ML policies.
- **Value:** £994,552

Recovering ML Models from Partial Parameters

The Alan Turing Institute

Co PI (AWARDED)

Jan. 2025

- Looks at model stealing attacks and implications of partial recovery.
- **Value:** £13.416,36

Open Network for Secure, Ethical, and Sustainable AI for Manufacturing Excellence (Open-SESAME)

EPSRC Impact Acceleration Awards

PI (AWARDED)

Dec 2024

- Funds a workshop to build a multidisciplinary team addressing secure, ethical AI adoption in industry.
- Facilitates collaboration among academics, industry, and policymakers, fostering ideas for an EPSRC Network Grant application.
- **Value:** £5,000

HackRoom - Unlock Your Cyber Skills to Escape

Innovate UK - Cyber Local

ACADEMIC PI (AWARDED)

Oct. 2024

- Teaches practical cybersecurity skills through immersive, fun challenges in physical and virtual escape rooms.
- Promotes cybersecurity awareness, career exploration, and real-world skills in accessible, engaging formats.
- **Partners:** X-Seed, CycurFUZZ, ETAS **Value:** £80,497 (of which £32,051 to Academic PI)

AI Powered Knowledge Graph for Automotive and Mobility Sector

EPSRC Impact Acceleration Awards

PI (AWARDED)

Sep 2024

- Addresses challenges in the automotive and mobility sectors through AI-powered knowledge graph technology.
- Identifies skill gaps, fosters stakeholder collaboration, and aligns workforce development with industry transformation needs.
- **Value:** £18,513.38

Selected Publications - Full list available on: [Google Scholar](#)

NLP Verification: Towards a General Methodology for Certifying Robustness

*European Journal of Applied
Mathematics*

AUTHOR

Feb 2025

- Created first framework for end to end NLP verification (Neural Network Based)
- Analysed trends and limitations of this approach

Tactics for Account Access Graphs

*European Symposium on Research
in Computer Security (ESORICS)*

AUTHOR

Sep 2023

- Created a mathematical framework for studying account takeover attacks
- Provided a case study showing attacks on iPhones and selected android devices

The Vehicle Tutorial: Neural Network Verification with Vehicle

*Workshop on Formal Methods for
ML-Enabled Autonomous Systems*

AUTHOR

May 2023

- Created one of a kind tool allowing specification of neural network verification properties
- Automatically translates to a state of the art verification tool (Marabou) as well as interactive theorem prover (Agda)

Teaching

Networks and System Security (UG)

University of Birmingham

CO MODULE LEADER

Feb. 2024 - now

- Gave lectures, created coursework and exam, marked coursework and exam, led TAs and practicals

Malware, Forensics and Penetration Testing (MSc)

University of Birmingham

CO MODULE LEADER

Feb. 2023 - now

- Gave lectures, created coursework and exam, marked coursework and exam, led TAs and practicals
- 95% student rated the module Very good (top grade) for both Lecturer and Module content

Secure Programming (MSc)

University of Edinburgh

MODULE LEADER

Jan. 2022 - May 2023

- Gave lectures, created coursework and exam, marked coursework and exam, led TAs and practicals
- Sample Feedback:

Student oaUJ: "Please encourage all lecturers to use Piazza as effectively as Dr Arnaboldi."

Student zAQT: "BEST COURSE IN INFORMATICS PERIOD"

Student qpHn: "I knew very little about security before this course, and I believe I learnt a lot."

2023-now **UG/MSc Supervisor**, Wide array of Verification/Security/ML Subjects

2022-2023 **UG Co-Supervisor x3**, "Automated Identification of Connected Autonomous Vehicle Risk Scenarios"

2021-2022 **MSc Co-Supervisor**, "Evaluating the Performance of RL Methods for Autonomous Racing"

2019-2020 **Teaching Assistant**, Security Analysis of Complex Systems

2019-2020 **Teaching Assistant**, System Security

2016-2020 **Teaching Assistant**, Cryptography

2016-2020 **Teaching Assistant**, System and Network Security

2016-2020 **Teaching Assistant**, Software Engineering

2016-2020 **Teaching Assistant**, Understanding Concurrency

2016-2017 **Teaching Assistant**, Website Construction and Management (Server-side)

Uni. of Birmingham.

(UG) Uni. of Edi.

(MSc) Heriot-Watt U.

(MSc) Newcastle U.

(MSc) Newcastle U.

(UG) Newcastle Uni.

(UG) Newcastle Uni.

(UG) Newcastle Uni.

(UG) Newcastle Uni.

(UG) Newcastle Uni.

Invited Talks & Presentations

Towards Verifiable NLP – Keynote Speaker

Zagreb, Croatia

SYMPOSIUM ON AI VERIFICATION (AIVERIFICATION.ORG)

July. 2025

- Delivered keynote on NLP verification challenges and emerging methods, with a focus on embedding-space reasoning.

Cybersecurity in the Age of Responsible AI – Invited Speaker

London

RESPONSIBLE AI LAB – BUSINESS IN THE COMMUNITY

May 2025

- Spoke on AI cybersecurity challenges and best practices for UK businesses at the Responsible AI Lab event.

A High-Level Language for Neural Network Verification... and more! - Invited Talk

Oxford, UK

OXFORD VERIFICATION SEMINARS MEETING

Nov. 2024

- Talk at the verification group at Oxford on Neural Network Verification

Inside the Mind of a Hacker: Unraveling the Tactics Behind Account Takeover Attacks - Invited Talk

DURHAM UNIVERSITY AIHS SEMINARS

- Talk at the AIHS group at Durham on Account Takeover attacks

Durham, UK

Nov. 2024

Attacks on Autonomous Vehicle Sensors and AI Reasoning - Invited Talk

SURREY CYBER CLUSTER

- Presented to the Surrey Cyber Security Cluster work on Attacks on AI

Camberley, UK

May. 2024

Future of AI - Invited Expert

UK-CANADA FRONTIERS OF SCIENCE MEETING - AI

- Meet with experts in AI to discuss future risks and challenges

Ottawa, Canada

Feb. 2024

Future of AI : Benefits, Risks & Responsibilities - Invited Talk

UKC3 PAN CLUSTER EVENT

- Presented to the UK Cyber Security Clusters on how to ensure safe deployment of AI in their businesses and what risks there are

Birmingham, UK

Oct. 2023

Verifiably Secure AI in Autonomous Vehicles

THIRD CONFERENCE ON RESILIENT AND ROBUST SENSING FOR AUTONOMOUS VEHICLES - INVITED TALK

- Discussed my research on ensuring AI safety and security in Autonomous Vehicles

Warwick, UK

Jun. 2023

Intrusion Detection in the IoT - Invited Talk

LAB FOR AI VERIFICATION

- Discussed state of the art of intrusion detection in IoT systems
- Presented my explainable approach to IDS

Edinburgh, UK

Jan. 2021

Designing a Secure Protocol Using Formal Methods - Tutorial Session

FOURTH ANNUAL OAUTH WORKSHOP (OSW)

- Designed and presented a 4 hour tutorial on formal protocol verification
- Audience of 30 industry and academic security experts

Stuttgart, Germany

Mar. 2019

A Modelling Approach for DoS Detection in Low-Powered IoT Systems

SIXTH WORKSHOP ON FORMAL METHODS AND TOOLS FOR SECURITY (FMATS)

- Lightning presentation on my work in intrusion detection
- Presented my proposed methodology to industry and academic experts present

Cambridge, UK

Sep. 2018

Program Committees

2024-now **Artifact Committee**, International Conference on Computer-Aided Verification

2024-now **Program Committee**, Third Workshop on Safety for Conversational AI @ LREC/COLING

2022-now **Program Committee**, Security Track at the ACM Symposium on Applied Computing (SAC)

2022-2023 **Artifact Review Committee**, International Conference on Cyber-Physical Systems

2021-now **Organisation Committee Chair**, UK-SPS: Cyber Security & Privacy Seminar Series

2020-2020 **Program Chair**, School of Computing, PGR Research Conference 2020

2019-2022 **Artifact Review Committee**, Privacy Enhancing Technologies Symposium - PETS

Outreach & Public Engagement

Expert Commentary - “Now cybersecurity experts say Brits should stop texting too - as the FBI issues an urgent warning to Americans about sending messages between Androids and iPhone”

DAILY MAIL

- Discussed potential threats of sms interceptions

Expert Commentary

Dec. 5, 2024

Industry Meetup - Launch Event & Automotive Digital Forensics and Cybersecurity Event

AUTOMOTIVE SECURITY RESEARCH GROUP (ASRG)

- Launched the West Midlands Chapter of ASRG in Collaboration with Industrial Partner
- Over 50 industry participants sharing insights into challenges in automotive cybersecurity

Industry Focused Meetup

May 2024 and Dec 2024

Media Article - “Researchers unveil new way to counter mobile phone ‘account takeover’ attacks”

BIRMINGHAM ENTERPRISE NETWORK

- Media Article on my publication studying account takeover attacks
- Shared internationally in over 20 media outlets, with combined readerships of **30 million readers**, such as MSN News, Tech Spark, Tech Times, Science Daily...

Media Piece on my Research

Jan. 22, 2024

Media Interview - “DON’T SPEAK Why your VOICE is no longer safe on social media as AI clones mimic speech to deceive family & break into bank accounts”

THE SUN

- Discussed potential threats of AI cloning

Media Interview

May 10, 2024

Radio Interview - “AI Safety (in relation to AI Safety Summit)”

FREE RADIO AND HITS RADIO NETWORK

- Discussed my view on AI Safety and Potential Mitigations

Media Interview

Oct. 30, 2023

Media Article - “Perfecting self-driving cars – can it be done?”

THE CONVERSATION

- **24,194 readers** (highest read article for any Heriot-Watt article no data for University of Edinburgh)
- Shared on – Yahoo News UK, Metro UK, Big News Network, Stuff (Australia), Robohub, and more...

Media Article

Apr. 6, 2021

Media Interview - “Is the Dream of Self-Driving Cars Dead?”

DIRECT INDUSTRY MAGAZINE

- Interview with industry targeted magazine with intent to share my work with practitioners

Media Interview

Oct. 26, 2021

Science Festival - National Robotarium Exhibition: Autonomous Racing Car

NATIONAL ROBOTARIUM SCIENCE EXHIBIT - EDINBURGH SCIENCE FESTIVAL

- Led team of colleagues from HW and showcased our research autonomous vehicle to a crowd of children and their families

Science Festival

Apr. 14, 2022

My Research & Pedagogical Tools

Vehicle: Neural Network Verification

COLLABORATOR

- Vehicle is a high-level dependently-typed domain-specific language for enforcing logical specifications for neural networks.
- Hosted Tutorials for industry and academia at international conferences and UK Cyber Security Institute
- available at: Tool: <https://github.com/vehicle-lang/vehicle>
Tutorial: <https://vehicle-lang.github.io/tutorial/>

Edinburgh

Jan. 2021 - Ongoing

MetaCP - Cryptographic Protocol Design Tool for Formal Verification

CO-INVENTOR & DEVELOPER

- Tool aiding the cryptographer throughout the process of designing and formally modelling a protocol
- Made in: ReactJS, ExpressJS, Redux, XSLT, DTD, XML
- Available at metacp.eu

MetaCP

Jun. 2019 - Ongoing

Coursework Automatic Judge System and Marking Tool

DEVELOPER

- Automated judge system evaluating code quality and structure
- Automated marking of coursework through testcases and automated feedback system

Newcastle University, Cryptography

Oct. 2019

CTF Competition Coursework Submission Tool

DEVELOPER

- Developed Coursework Tool for Capture The Flag (security competition)
- Generated Unique Security challenges for students

Newcastle University, CSC3124

Jan. 2019, Jan. 2020

Honors & Awards

- 2022 **Awarded**, Informatics Staff Award - For teaching Secure Programming MSc
- 2019 **Awarded**, NCL+ Award - For Work in Leadership and Peer Representation
- 2019 **Short List**, Best Postgraduate School Representative of The Year:
- 2018 **1st Place**, Action for Impact Competition - Designing Sustainable Smart Cities

Certifications & Continuous Professional Development

- 2024 **Pedagogical Practice Course – Learning and Teaching in Higher Education**,
- 2020 **Cyber Security Winter School**,
- 2019 **RISE Hardware Security**,
- 2017 **School on Foundations of Probabilistic Programming and Software Systems**,

Birmingham, UK

Newcastle, UK

Guildford, UK

Braga, Portugal