

Luca Arnaboldi

SECURITY RESEARCHER · FORMAL METHODOLOGIST

☎ (+44) 7784435092 | ✉ luca.arnaboldi@ed.ac.uk | 🏠 www.arnaboldiluca.eu | 📺 yiergot | 📄 luca-arnaboldi-829083b2 | 🎓 Luca Arnaboldi

Summary

I am a researcher currently focusing on security of autonomous systems, explainable AI and formal verification of machine learning algorithms. My general research interests lie in the **use and development of formal modelling techniques** for adaptive security solutions in the context of ubiquitous distributed systems. I am particularly interested in the area of **automated verification of security protocols**, to which end I have co-developed a one of a kind tool for the automated translation from a graphical design interface to a formal specification of the protocols as well as working correct by design implementations, MetaCP. My other areas of interest are the application of formal modelling techniques to the area of **white box anomaly based intrusion detection** in the Internet of Things (IoT), and the development of **testing suites for security solutions** for constrained and disadvantaged environments.

Education

Newcastle University, Secure & Resilient Systems

Newcastle Upon Tyne, UK

PHD IN COMPUTER SCIENCE

Oct. 2016 - Dec. 2020

- **Thesis:** *A Methodology for the Quantitative Evaluation of Attacks and Mitigations in IoT Systems*
industry partner: ARM Ltd. **Supervisor:** C. Morisset, **Examiners:** Prof. S. Etalle and Prof. A. van Moorsel
- Extra MSc Modules Attended: System Validation (CS8105), System Evaluation (CSC8106), High Integrity Software Development (CSC8204), 1st class honors (all)

Newcastle University

Newcastle Upon Tyne, UK

BSC IN COMPUTER SCIENCE, 1ST CLASS

Sep. 2013 - June. 2016

- **Dissertation:** *Feature Engineering For an Industrial Data Mining Challenge*
industry partner: XACT Ltd.
- **Security Specialisation**, courses included: network security, databases, server side programming, formal system analysis, formal verification, model checking, algorithms, machine learning etc..

Work Experience

Januus

Edinburgh, UK

CHAIR OF ADVISORY BOARD

Mar. 2022 - now

- Chairing advisory board tackling regulations, ethics and security of blockchain data

University of Edinburgh

Edinburgh, UK

UNIVERSITY TEACHER

Jan. 2022 - May 2022

- Module Leader for Msc Course on Secure Programming
- Topics: Attack and defence practice for real world cyber security and static analysis tools for security verification

Heriot Watt University

Edinburgh, UK

VISITING SCHOLAR

Aug. 2021 - now

- Leading team in construction of autonomous research vehicle
- Co-supervising Msc projects focusing on algorithmic racing, AI explainability, vehicle data analysis, vehicle control

University of Edinburgh

Edinburgh, UK

RESEARCH ASSOCIATE

Dec. 2020 - now

- Working on Security of Autonomous Systems
- Collaborating with PL and Verification researchers to create an AI verification tool
- Creating novel risk assessments for security safety scenarios in autonomous vehicles

ARM, Ltd.

Cambridge, UK

RESEARCH INTERN

Aug. 2018 - Dec. 2018

- Worked on security analysis and formal verification of cryptographic protocols
- Created first formal model of the full ACE-OAuth implementation, using formal tool Tamarin published at OAuth workshop 2019

ARM, Ltd.

Cambridge, UK

RESEARCH INTERN

Aug. 2017 - 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 (common in IoT deployments) through proof of freshness

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

Automating Cryptographic Protocol Language Generation from Structured Specifications

*FormaliSE: International Conference
on Formal Methods in Software
Engineering*
May 2022

AUTHOR

- Create one of a kind tool allowing specification of cryptographic protocols
- Automatically translates to two formal languages as well as c++ implementations

Vehicle: Interfacing Neural Network Verifiers with Interactive Theorem Provers

In Submission (POPL)
June 2022

AUTHOR

- Created a dependently typed specification language for neural network verification properties
- Connects the neural network verifier Marabou to Agda and then formally verifying that a car steered by a neural network never leaves the road

Modelling Load-Changing Attacks in Cyber-Physical Systems

*Electronic Notes in Theoretical
Computer Science*
Nov 2021

AUTHOR

- Modelled distributed load changing attacks on smart grid infrastructures using markov chains
- Ran quantitative assessment of attack impact

Teaching

Secure Programming (MSc) INFR11098

University of Edinburgh
Jan 2022 - May 2022

MODULE LEADER

- 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."

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

(UG) Uni. of Edi.

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

(MSc) HW Uni.

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

(MSc) CSC8207

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

(MSc) CSC8102

2016-2020 **Teaching Assistant**, Cryptography

(UG) CSC3621

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

(UG) CSC3124

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

(UG) CSC2021

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

(UG) CSC3324

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

(UG) CSC3422

My Research & Pedagogical Tools

Vehicle: Neural Network Verification

Edinburgh

COLLABORATOR

Jan 2021 - Ongoing

- Vehicle is a high-level dependently-typed domain-specific language for enforcing logical specifications for neural networks.

MetaCP - Cryptographic Protocol Design Tool for Formal Verification

MetaCP

CO-INVENTOR & DEVELOPER

June 2019 - Ongoing

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

Coursework Automatic Judge System and Marking Tool

Newcastle University, CSC3621

LEAD DEVELOPER

October. 2019

- Made a submission and marking website for Cryptography
- Automated judge system evaluating code quality and structure
- Automated marking of coursework through testcases and automated feedback system

CTF Competition Coursework Submission Tool

Newcastle University, CSC3124

DEVELOPER

January. 2019, January 2020

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

Talks & Presentations

Intrusion Detection in the IoT

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

Building Secure IoT Systems - Guest Lecture

SOFTWARE ENGINEERING PROFESSIONAL (CSC1023)

- First years Bsc lecture on my research work
- Taught a class of 200 students about IoT security challenges
- Discussed my work in how to improve IoT security

Newcastle University

Mar. 2019

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

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

Outreach & Public Engagement

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

April 6th, 2021

Short interview published - “Is the Dream of Self-Driving Cars Dead?”

INTERVIEW WITH ADAM TURNER

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

Media Interview

October 26, 2021

National Robotarium Daytime Demo Exhibition: Autonomous Racing Car

NATIONAL ROBOTARIUM SCIENCE EXHIBIT

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

Edinburgh Science Festival

April 14th 2022

Program Committees

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

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

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

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

Courses & Training

Cyber Security Winter School

SPECIALISED RESEARCH COURSE

- School on Cyber Security
- UK PhD Winter School on Cyber Security focussing on real-world large-scale current and future problems

Newcastle Upon Tyne, UK

January 13 2020 - January 16 2020

RISE Hardware Security

SPECIALISED SECURITY COURSE

- Introduction to hacking embedded systems
- Courses that covered the following topics: JTAG, UART, SPI, Firmware hacking, hardware reconnaissance

Surrey, UK

March 11 2019 - March 14 2019

School on Foundations of Probabilistic Programming and Software systems.

SPECIALISED RESEARCH COURSE

- School on Probabilistic Programming and Modelling
- Courses that covered the following topics: semantics, analysis, verification, privacy, and security.

Braga, Portugal

May 28 2017 - June 4 2017

Introduction to Learning and Teaching in Higher Education (IHLE)

TEACHING TRAINING

- Practical skills to enable teaching in HE

Newcastle Upon Tyne, UK

October 2016

- Specialised course converting COBOL programs to JAVA
- Full course on COBOL language and AGILE Java development

Skills

Machine Learning	Data Analysis, Interpretable AI, Anomaly Detection
Security	Protocols, Intrusion Detection, DoS, Security Modelling
Formal Modelling	PRISM Model Checker, Markov Chains, PEPA, SPIN
Programming	JavaScript, Python, JAVA, C, COBOL
Formal Verification	Tamarin, Scyther, Isabelle, Ada SPARK, VDM SL
Networks	VSphere, VMware, Hypervisors, VirtualBox, Network Management
Embedded Systems	ARM mbed, Mbed OS, C, JTAG, UART
Back-end	Express, PHP, REST API, SQL
Front-end	Hugo, Redux, React, HTML5
Languages	English, Italian

Honors & Awards

- 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

Extracurricular Activity

Edinburgh Science Festival

TEAM LEAD

- Presenting demo of our research autonomous vehicle
- Teaching children ages 8-12 how to program an autonomous vehicle

Edinburgh

April 2022

CTF Competition Team

CO-FOUNDER & MEMBER

- Founded Newcastle University first Capture The Flag team
- Participated in several CTF competitions across the UK
- Set up cyber incident room for CTF competition training

Newcastle University

Apr. 2017 - Dec. 2020

Student Staff Committee

STUDENT STAFF COMMITTEE CHAIR, COMPUTING

- Organised, Chaired and represented the SSC at the school level

Newcastle University

Sep. 2019 - Dec. 2020

Graduate School Committee

SCHOOL OF COMPUTING PGR REPRESENTATIVE

- Represented School of Computing at University Level
- Elected as PGR Representative at *University Education Committee*
- Elected as PGR representative at *University PGR Committee*

Newcastle University

Sep. 2018 - Sep. 2019

Technology and Computing Society NUCATS

POSTGRADUATE REPRESENTATIVE & MEMBER

- Focused on hackathons and coding events
- Created marketing and network opportunities

Newcastle University

Sep. 2018 - Jun. 2018

Student Staff Committee

GROUP REPRESENTATIVE

- Represented SRS group PhDs at the School student staff committee

Newcastle University

Sep. 2017 - Sep. 2018

Hack NE - 24 hour programming event

ORGANISED AND RAN HACKATHON

- With two friends organised the largest coding Hackathon in the North East (at the time) [Link Here](#)
- In cooperation with Major League Hacking and sponsors:
Bede Gaming, Bloomberg, PayPal, Braintree, SendGrid, Capital One and namecheap

Major League Hacking (MLH)

November 2014