

Luca Arnaboldi

RESEARCH ASSOCIATE · SECURITY RESEARCHER

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

Summary

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 - Oct. 2020

- Thesis: A Methodology For The Automated Deployment of Attack Detection Systems in the IoT
- 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" in cooperation with XACT Ltd.
- **Security Specialisation**, courses included: network security, databases, server side programming, formal system analysis, algorithms, machine learning etc..

Courses & Training

Cyber Security Winter School

Newcastle Upon Tyne, UK

SPECIALISED RESEARCH COURSE

January 13 2020 - January 16 2020

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

RISE Hardware Security

Surrey, UK

SPECIALISED SECURITY COURSE

March 11 2019 - March 14 2019

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

School on Foundations of Probabilistic Programming and Software systems.

Braga, Portugal

SPECIALISED RESEARCH COURSE

May 28 2017 - June 4 2017

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

Introduction to Learning and Teaching in Higher Education (IHLE)

Newcastle Upon Tyne, UK

TEACHING TRAINING

October 2016

- practical skills to enable teaching in HE

COBOL and Agile Java Programming

Newcastle Upon Tyne, UK

NEWCASTLE COLLEGE

July 13 2015 - August 13 2015

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

Work Experience

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 the work in a paper 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.
- Documented several vulnerabilities in current approaches.
- 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](#)

Towards a Data Centric Approach for the Design and Verification of Cryptographic Protocols

ACM CCS - Poster Session

DEMO AUTHOR

November 2019

- Demo of MetaCP, tool for the design, formalisation and specification of cryptographic protocols

Generating Synthetic Data for Real World Detection of DoS Attacks in the IoT

DATAMOD

AUTHOR

June 2018

- Proposed new approach for deploying IDSs in constrained systems

Quantitative Analysis of DoS Attacks and Client Puzzles in IoT systems

Security & Trust Management

AUTHOR

Sep 2017

- Proposed a modelling approach for the evaluation of IoT systems under strain of DoS
- Showcased approach with use of case study looking a Crypto Puzzles as a mitigation to DoS attacks

Talks & Presentations

Designing a Secure Protocol Using Formal Methods - Tutorial Session

Stuttgart, Germany

FOURTH ANNUAL OAUTH WORKSHOP (OSW)

Mar. 2019

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

Building Secure IoT Systems - Guest Lecture

Newcastle University

SOFTWARE ENGINEERING PROFESSIONAL (CSC1023)

Mar. 2019

- First years Bsc lecture on my research work.
- Tought a class of 200 students about IoT security, challenges, and discussed my work in how to improve IoT security.

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

Cambridge, UK

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

Sep. 2018

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

Program Committees

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

Newcastle Upon

Tyne, UK

2019-2021 **Artifact Review Committee**, Privacy Enhancing Technologies Symposium - PETS

Skills

Security	Protocols, Intrusion Detection, DoS, Security Modelling	●●●●●●
Formal Modelling	PRISM Model Checker, Markov Chains, VDM, PEPA, SPIN, SPARK	●●●●●●
Programming	JavaScript, Python, JAVA, C, COBOL	●●●●●●
Formal Verification	Tamarin, Scyther, Isabelle	●●●●○
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	●●●●●●

Tools

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
- Involved: PHP, MySQL, Java, JUnit

CTF Competition Coursework Submission Tool

Newcastle University, CSC3124

DEVELOPER

January. 2019, January 2020

- Developed Coursework Tool for Capture The Flag
- Generated Unique Security challenges for students
- Created virtual security environments for security testing
- Involved: C, Java, python, NodeJS, virtual machines, networking

Teaching

2019-now Teaching Assistant , Security Analysis of Complex Systems	(MSc) CSC8207
2019-now Teaching Assistant , System Security	(MSc) CSC8102
2016-now Teaching Assistant , Cryptography	(UG) CSC3621
2016-now Teaching Assistant , System and Network Security	(UG) CSC3124
2016-now Teaching Assistant , Software Engineering	(UG) CSC2021
2016-now Teaching Assistant , Understanding Concurrency	(UG) CSC3324
2016-2017 Teaching Assistant , Website Construction and Management (Server-side)	(UG) CSC3422

Honors & Awards

- 2019 **Awarded**, NCL+ Award - For Work in Leadership and Peer Representation
- 2019 **Short List**, Best Postgraduate School Representative of The Year:
- 2018 **First Place**, Action for Impact Competition - Designing Sustainable Smart Cities

Extracurricular Activity

CTF Competition Team

Newcastle University

CO-FOUNDER & MEMBER

April. 2017 - Ongoing

- 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.

Student Staff Committee

Newcastle University

STUDENT STAFF COMMITTEE CHAIR, COMPUTING

September 2019 - Ongoing

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

Graduate School Committee

Newcastle University

SCHOOL OF COMPUTING PGR REPRESENTATIVE

September 2018 - 2019

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

Technology and Computing Society NUCATS

Newcastle University

POSTGRADUATE REPRESENTATIVE & MEMBER

Sep. 2018 - Jun. 2018

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

Student Staff Committee

Newcastle University

GROUP REPRESENTATIVE

September 2017 - 2018

- Represented SRS group PhDs at the School student staff committee.

Hack NE - 24 hour programming event

Major League Hacking (MLH)

ORGANISED AND RAN HACKATHON

November 2014

- 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

References

To Be Provided Upon Request