Ilia Shumailov

is410@cam.ac.uk Tel:+44 7472 629757

PROFILE

Currently a PhD candidate at the University of Cambridge. My research interests lie primarily in the areas of Computer Security and Artificial Intelligence.

EDUCATION

PhD in Computer Science *Fitzwilliam College, University of Cambridge*
Oct 2017 - Oct 2021 Cambridge, UK

Supervisor(s): Prof Ross Anderson
Thesis: The power of a crowd: on behavioural manipulation of robotic herds
Funding: Department of Computer Science and Technology, University of Cambridge; Bosch Research Foundation (Bosch-Forschungsstiftung im Stifterverband)
Awarded College Senior Scholarship in recognition of academic achievements

MPhil in Advanced Computer Science (distinction) *Darwin College, University of Cambridge*
Cambridge, UK

Oct 2016 - Jun 2017

Supervisor(s): Prof Ross Anderson and Dr Laurent Simon
Thesis: Inferring smartphone PINs and text through acoustic side-channels (89%, top 2)
Classes: Computer Security – Principles and Foundations, Computer Security – Current Applications and Research, Advanced Operating Systems, Affective Computing, Advanced Topics in Computer Systems, Chip Multiprocessors (audit), Social and Technological Network Data Analytics (audit), Digital Signal Processing (audit).

Study Abroad *University of California San Diego*
Sep 2014 - Jun 2015 San Diego, CA, USA

Classes: Software Engineering, Theory of Computability, Database Systems Principles, Operation Systems, Artificial Intelligence, Computer Vision, Data Mining and Prediction Analytics, Search and Reasoning in Artificial Intelligence, Computer Security (audit).

BSc (Hons) in Computer Science *University of St Andrews*
Sep 2012 - June 2016 St Andrews, UK

Supervisor(s): Prof Simon Dobson
Thesis: Can Centrality Measures Adopted From Graph Theory Explain the Slowdown in Street Networks? (95%, top 2)
Classes: Object-Oriented Programming, Internet Programming, Foundation of Computation, Advanced Computer Science, Advanced Internet Programming, Advanced Programming Projects, Computer Architecture, Distributed Systems, Component Technology, Computer Security, Logic and Software Verification, Artificial Intelligence Practice (MSc-level course).

BSc in Engineering and Technology (dropped) *State University of Aerospace Instrumentation*
Sep 2010 - Aug 2011 St Petersburg, Russia

Classes: Mathematical Logic and Theory of Algorithms, Mathematical Analysis, Analytical Geometry, Discrete Mathematics, Information Theory, Computational Mathematics, Linear Mathematics, Physics, Programming foundations, Astronomy.
Received full scholarship.

PUBLICATIONS

Turning Up the Dial: the Evolution of a Cybercrime Market Through Set-up, Stable, and Covid-19 Eras with Anh Viet Vu, Jack Hughes, Ildiko Pete, Ben

Collier, Yi Ting Chua, and Alice Hutchings. Presented at ACM Internet Measurement Conference 2020 (IMC 2020).

Replay Attacks on Reinforcement Learning with Timothy Lazarus, Yiren Zhao and Robert Mullins. Currently under review.

Towards certifiable adversarial sample detection with Yiren Zhao, Robert Mullins and Ross Anderson. Currently under review.

Not My Deepfake: Towards Plausible Deniability for Machine-Generated Media with Baiwu Zhang, Jin Peng Zhou and Nicolas Papernot. Currently under review.

Sponge Examples: Energy-Latency Attacks on Neural Networks with Yiren Zhao, Daniel Bates, Nicolas Papernot, Robert Mullins and Ross Anderson. Currently under review.

BatNet: Data transmission between smartphones over ultrasound with Almos Zarandy and Ross Anderson. Currently under review.

Audio CAPTCHA with a couple of Cocktails with Fairooz Islam and Benjamin Maximilian Reinheimer. Presented at International Workshop on Security Protocols 2018 (SPW19).

Snitches Get Stitches: On the Difficulty of Whistleblowing with Mansoor Ahmed, Darija Halatova and Ross Anderson. Presented at International Workshop on Security Protocols 2018 (SPW19).

Blackbox Attacks on Reinforcement Learning Agents Using Approximated Temporal Information with Yiren Zhao, Robert Mullins and Ross Anderson. Presented at Dependable and Secure Machine Learning 2020 (DSML20).

Towards Automatic Discovery of Cybercrime Supply Chains with Rasika Bhalerao, Maxwell Aliapoulios, Sadia Afroz and Damon McCoy, Presented at eCrime 2019 (Acceptance rate $\tilde{4}4\%$). Received Honorable Mention.

Sitatapatra: Blocking the Transfer of Adversarial Samples with Xitong Gao, Yiren Zhao, Robert Mullins, Ross Anderson, Cheng-Zhong Xu.

The Taboo Trap: Behavioural Detection of Adversarial Samples with Yiren Zhao, Robert Mullins and Ross Anderson.

To compress or not to compress: Understanding the Interactions between Adversarial Attacks and Neural Network Compression with Yiren Zhao, Robert Mullins and Ross Anderson. Presented at SysML 19 (Acceptance rate $\tilde{1}6\%$).

Tendrils of Crime: Visualising the Diffusion of Stolen Bitcoins with Mansoor Ahmed and Ross Anderson. Presented at The Fifth International Workshop on Graphical Models for Security(GramSec 18).

Bitcoin Redux with Ross Anderson, Alessandro Rietmann and Mansoor Ahmed. Presented at 17th Annual Workshop on the Economics of Information Security (WEIS 18).

Hearing your touch (Poster) presented at Spring School on Hardware Security organised by the Research Institute in Secure Hardware and Embedded Systems (RISE 2018).

Making Bitcoin Legal with Ross Anderson and Mansoor Ahmed. Presented at International Workshop on Security Protocols 2018 (SPW18).

Hearing your touch: Inferring smartphone PINs and text through an acoustic side-channel with Laurent Simon, Jeff Yan and Ross Anderson.

Computational Analysis of Valence and Arousal in Virtual Reality Gaming using Lower Arm Electromyogram with Hatice Gunes. Presented at the Affective Computing and Intelligent Interaction 2017 Conference (ACII 17).

Comparing Relational and Graph Databases for Pedigree Datasets with Graham Kirby, Conrad de Kerckhove, Jamie Carson, Alan Dearly, Christopher Dibben, Lee Williamson. Presented at Population Reconstruction Workshop 2014 (PRW 14).

TEACHING

Supervisor for University of Cambridge Undergraduates — *University of Cambridge*
Jan 2018 - Present — Cambridge, UK

Supervision for Part IB 'Security', Part IA 'Software and Security Engineering', Part II 'Security II' and Part I 'Operating Systems'. Overall I did about 200 hours of supervisions.

Final project supervisor — *University of Cambridge*
Sep 2017 - Present — Cambridge, UK

Supervision of Part II (a.k.a Bachelors) and MPhil theses in the topics of Computer Security, DSP and Machine learning. To date I have supervised more then 10 projects, each of which was graded with a distinction and some of which were published.

Laboratory Demonstrator — University of St Andrews
Sep 2015 - May 2016 — St Andrews, UK

Helping 1^{st} and 2^{nd} year Computer Scientists with concepts, related to Computer Networks, Object-Oriented Programming, Functional Languages, Scripting languages.

WORK EXPERIENCE

Visiting Research Scholar — *Vector Institute, University of Toronto*
Jun 2020 - Sept 2020 — Toronto, Canada

Adversarial Machine Learning research under the supervision of Dr Nicolas Papernot.

Research Intern — *School of Computer Science and Engineering, New York University*
Jul 2019 - Sept 2019 — New York, USA

Cybercrime research under the supervision of Dr Damon McCoy.

Visiting Research Scholar — *ICSI, University of California Berkeley*
Jul 2018 - Sept 2018 — San Francisco, USA

Cybercrime research under the supervision of Dr Sadia Afroz.

Research Intern — *University of Cambridge*
Jul 2017 - Sep 2017 — Cambridge, UK

Systems research under the supervision of Dr Robert Watson.

Research Assistant — *University of St Andrews*
May 2016 - Sep 2016 — St Andrews, UK

Computer Vision research under the supervision of Dr Ognjen Arandelovic.

Research Assistant *University of St Andrews*
May 2016 - Sep 2016 St Andrews, UK

Experiment reproducibility research under the supervision of Prof Ian Gent and Dr Chris Jefferson.

Bright Mind Intern *Microsoft Research*
Jun 2015 - Sep 2015 Cambridge, UK

Worked in Systems and Networks Research group under supervision of Dr Christos Gkantsidis on Software Defined Network optimisation and software testing.

Application Developer Intern *JPMorgan and Chase*
Jun 2014 - Sep 2014 Glasgow, UK

Software development along with the introduction to the financial sector and business analysis.

Research Intern *University of St Andrews*
Jun 2013 - Aug 2013 St Andrews, UK

Development of software using Java with Hibernate, Spring. Usage of different types of databases, including MySQL, pl/pgSQL, neo4j, MariaDB. Analysis, adaptation, and optimisation of different algorithms. Practical experience of operating Jenkins, Logging, Unit Testing, Mock Testing, Test Driven Development, Bash-scripting, working in a team, presenting work in a readable format, meeting tight deadlines.

OTHER EXPERIENCE

Program Committee member *University of St Andrews*
Jun 2013 - Aug 2013 St Andrews, UK

Help with organisation of FIPR 20th anniversary conference University of Cambridge
Sep 2017 - Sep 2018 Cambridge, UK

Helped with conference organisation.

Security group representative University of Cambridge
Sep 2017 - Present Cambridge, UK

Security group representative to the Graduate forum at the Department of Computer Science and Technology, University of Cambridge.

Student Mentor University of St Andrews
Sep 2015 - May 2016 St Andrews, UK

Mentoring one 1^{st} year and one 2^{nd} year Computer Science students. Helping with concepts, related to Computer Networks, Object-Oriented Programming, Functional Languages, Scripting languages.

JPMorgan Spring Week JPMorgan and Chase
May 2013 - May 2013 London, UK

An insight into investment banking and technologies used in the financial sector. Introduction to business analysis techniques and technology stack utilised by the bank.

JPMorgan Code for Good JPMorgan and Chase
Nov 2013 - Nov 2013 London, UK

Development of a system to access the Internet for the places in Africa where there is only GSM signal available. The software written included Android application and sms-based system. Technologies used: Java (Android part), Python Django (Server-side for the application), Bootstrap (UI), sms-server. Team took the *first place*.

Hackathon organisation University of St Andrews
Nov 2013 - Nov 2013 St Andrews, UK

Organisational work associated with running a hackathon.

Cyber-security Hackathon University of Edinburgh
Oct 2013 - Oct 2013 Edinburgh, UK

Development of two-step level biometrics-based authentication system, that can be inserted into any system. That involved usage of OpenCV, Ruby On Rails, Python Flask. St Andrews team took the *second place*.