Ilia Shumailov

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

PROFILE

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

EDUCATION

Postgraduate Fellowship in Security of Machine Learning — *Vector Institute, University of Toronto*
Sept 2021 - Sept 2022 — Toronto, Canada

Supervisor(s): Prof Nicolas Papernot and Prof Kassem Fawaz
Funding: DARPA and CIFAR.

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

Supervisor(s): Prof Ross Anderson
Thesis: Computer Security Engineering in era of Machine Learning
Funding: Department of Computer Science and Technology, University of Cambridge; Full scholarship from 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*
Oct 2016 - Jun 2017 — Cambridge, UK

Supervisor(s): Prof Ross Anderson and Dr Laurent Simon
Thesis: Inferring smartphone PINs and text through acoustic side-channels (89%, top 2)

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)

PAPERS

ExtremeBB: Enabling Large-Scale Research into Extremism, the Manosphere and Their Correlation by Online Forum Data
Anh V. Vu, Lydia Wilson, Yi Ting Chua, Ilia Shumailov, Ross Anderson.
Currently under review.

Bounding Membership Inference
Anvith Thudi, Ilia Shumailov, Franziska Boenisch, Nicolas Papernot.
Currently under review.

On the Necessity of Auditable Algorithmic Definitions for Machine Unlearning
Anvith Thudi, Hengrui Jia, Ilia Shumailov and Nicolas Papernot.
31st USENIX Security Symposium 2022.

Rethinking Image-Scaling Attacks: The Interplay Between Vulnerabilities in Machine Learning Systems
Yue Gao, Ilia Shumailov and Kassem Fawaz.
Currently under review.

Rapid Model Architecture Adaption for Meta-Learning
Yiren Zhao, Xitong Gao, Ilia Shumailov, Nicolo Fusi and Robert Mullins.
Currently under review.

***Bad Characters: Imperceptible NLP Attacks**
Nicholas Boucher, Ilia Shumailov, Nicolas Papernot and Ross Anderson.
IEEE Symposium on Security and Privacy 2022 (acceptance rate ∼15%).

***Markpainting: Adversarial Machine Learning meets Inpainting**
David Khachaturov, Ilia Shumailov, Yiren Zhao, Nicolas Papernot and Ross Anderson.
38th International Conference on Machine Learning 2021 (acceptance rate ∼21.5%)

***Manipulating SGD with Data Ordering Attacks**
Ilia Shumailov, Zakhar Shumaylov, Dmitry Kazhdan, Yiren Zhao, Nicolas Papernot, Murat A. Erdogdu, Ross Anderson.
35th Conference on Neural Information Processing Systems 2021 (acceptance rate ∼26%).

***Towards Robust Keyword Spotting**
Shimaa Ahmed, Ilia Shumailov, Nicolas Papernot, Kassem Fawaz.
31st USENIX Security Symposium 2022.

***Turning Up the Dial: the Evolution of a Cybercrime Market Through Set-up, Stable, and Covid-19 Eras**
Anh Viet Vu, Jack Hughes, Ildiko Pete, Ben Collier, Yi Ting Chua, Ilia Shumailov and Alice Hutchings.
ACM Internet Measurement Conference 2020 (IMC 2020).

***Towards certifiable adversarial sample detection**
Ilia Shumailov, Yiren Zhao, Robert Mullins and Ross Anderson.
13th ACM Workshop on Artificial Intelligence and Security (AISec 2020).

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

***Sponge Examples: Energy-Latency Attacks on Neural Networks**
Ilia Shumailov, Yiren Zhao, Daniel Bates, Nicolas Papernot, Robert Mullins and Ross Anderson.
6th IEEE European Symposium on Security and Privacy (EuroS&P 2021).

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

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

***Blackbox Attacks on Reinforcement Learning Agents Using Approximated Temporal Information**
Yiren Zhao, Ilia Shumailov, Han Cui, Xitong Gao, Robert Mullins and Ross Anderson.
Dependable and Secure Machine Learning 2020 (DSML20).

Towards Automatic Discovery of Cybercrime Supply Chains
Rasika Bhalerao, Maxwell Aliapoulios, Ilia Shumailov, Sadia Afroz and Damon McCoy.
eCrime 2019 (Acceptance rate ∼44%). Received Honorable Mention.

***To compress or not to compress: Understanding the Interactions between Adversarial Attacks and Neural Network Compression**
Ilia Shumailov, Yiren Zhao, Robert Mullins and Ross Anderson.
Second Conference on Machine Learning and Systems (MLSys 19) (Acceptance rate ∼16%).

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

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

Making Bitcoin Legal
Ross Anderson, Ilia Shumailov and Mansoor Ahmed.
International Workshop on Security Protocols 2018 (SPW18).

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

***Computational Analysis of Valence and Arousal in Virtual Reality Gaming using Lower Arm Electromyogram**
Ilia Shumailov, Hatice Gunes.
Affective Computing and Intelligent Interaction 2017 Conference (ACII 17).

Comparing Relational and Graph Databases for Pedigree Datasets
Graham Kirby, Conrad de Kerckhove, Ilia Shumailov, Jamie Carson, Alan Dearly, Christopher Dibben, Lee Williamson.
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

Experiment reproducibility research under the supervision of Prof Ian Gent and Dr Chris Jefferson. Computer Vision research under the supervision of Dr Ognjen Arandelovic.

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.