Jamie Hayes

CONTACT INFORMATION

University College London
Dept. of Computer Science
Gower Street, London WC1E 6BT, U.K.

Email: j.hayes@cs.ucl.ac.uk
WWW: www0.cs.ucl.ac.uk/staff/J.Hayes

RESEARCH INTERESTS

Machine Learning applications to Computer Security and Privacy, Adversarial Machine Learning, Network Traffic Analysis, Anonymity Systems

EDUCATION

Dept. of Computer Science, University College London, UK
Sep. 2014 - Present - Ph.D. candidate
Privacy, Security and Machine Learning
Advisor: Dr. George Danezis
Second Advisor: Dr. Thore Graepel

Computer Laboratory, University of Cambridge, UK
Sep. 2013 - Apr. 2014 - Researcher
Parameterized Computational Complexity of the Graph Isomorphism Problem
Advisor: Prof. Anuj Dawar

Dept. of Mathematics, University of Manchester, UK
Sep. 2007 - Jun. 2011 - Master of Mathematics
First Class Grade
Advisor: Prof. Richard Sharp

HONORS AND AWARDS

NIPS 2017 & 2018 Student Travel Award

Google Phd Fellowship in Machine Learning (2017-2020)

Invited to Google PhD Summit in Security (2016, 2018) and Machine Learning (2017)

Academic Center of Excellence Scholarship, 2014

Engineering and Physical Sciences Research Council (EPSRC) Doctoral Training Studentship, 2013

EXPERIENCE

Google Research, Mountain View, CA, USA
Internship **July, 2018 - September, 2018**

Research into generative and adversarial machine learning. Developed new techniques for unsupervised style transfer, and new probabilistic conditioning methods for generative models.

Microsoft Research, Cambridge, UK
Internship **February, 2018 - May, 2018**

Research into security and privacy attacks and defenses in multi-party machine learning.

Naval Research Laboratory, Washington, DC, USA
Internship **August, 2017 - October, 2017**

Research into adversarial machine learning and network traffic analysis. Proposed a project on using

machine learning techniques for performing privacy-preserving experiments into live traffic analysis attacks on Tor.

Government Digital Services, London, UK

Intern for the SecOps team **March, 2017 - July, 2017**

I developed and implemented a privacy-preserving machine learning pipeline to aid threat analysis and improve Transaction Monitoring (TxM) on the GOV.UK Verify system.

University of Manchester, Manchester, UK

Network Technician **September, 2011 - March, 2013**

Maintenance of the internal University network that provided a connection to over 10,000 students. Duties included server maintenance, switch configurations, some SDN programming.

Publications

Peer-Reviewed

Hayes, J., Melis, L., Danezis, G., De Cristofaro, E. LOGAN: Evaluating Privacy Leakage of Generative Models Using Generative Adversarial Networks. *Proceedings on Privacy Enhancing Technologies, 2019.*

Hayes, J., Ohrimenko, O. Contamination Attacks in Multi-Party Machine Learning. *NIPS 2018*

Hayes, J. On Visible Adversarial Perturbations & Digital Watermarking. *CVPR (Workshop Track), June, 2018.*

Hayes, J., Danezis, G. Learning Universal Adversarial Perturbations with Generative Models. *IEEE Security and Privacy Workshop Track (1st Deep Learning and Security Workshop), June, 2018.*

Hayes, J., Danezis, G. Generating Steganographic Images via Adversarial Training. *NIPS 2017*

Piotrowska, A., Hayes, J., Gelernter, N., Danezis, G., Herzberg, A. AnNotify: A Private Notification Service. *Proc. 16th Workshop on Privacy in the Electronic Society - WPES '17, 2017. Satellite Workshop of CCS 2017.* `https://eprint.iacr.org/2016/466`

Piotrowska. A., Hayes, J., Elahi, T., Meiser, S., Danezis, G. The Loopix Anonymity System. *USENIX Security 2017.*

Cherubin, G., Hayes, J., Juarez, M. Website Fingerprinting Defenses at the Application Layer. *Proceedings on Privacy Enhancing Technologies. Minnesota, July, 2017.*

Hayes, J., Troncoso, C., Danezis, G. TASP: Towards Anonymity Sets that Persist. *Proc. 15th Workshop on Privacy in the Electronic Society - WPES '16, 2016. Satellite Workshop of CCS 2016.*

Hayes, J., Danezis, G. k-fingerprinting: a Robust Scalable Website Fingerprinting Technique. *USENIX Security 2016.* `http://arxiv.org/abs/1509.00789`

Hayes, J. Traffic Confirmation Attacks Despite Noise. *Understanding and Enhancing Online Privacy Satellite Workshop of NDSS, February 21, 2016, San Diego, USA*

Hayes, J., Danezis, G. Guard Sets for Onion Routing. *Proceedings on Privacy Enhancing Technologies. Philadelphia, June, 2015.*

Technical Reports

Hayes, J. A note on hyperparameters in black-box adversarial examples.

Hayes, J. An Introduction to the Dynamics of Real and Complex Quadratic Polynomials. *University of Manchester, 2011.*

Presentations

On Visible Adversarial Perturbations & Digital Watermarking, *CVPR Workshop Track, June, 2018*

Learning Universal Adversarial Perturbations with Generative Models, *IEEE Security and Privacy Workshop Track (1st Deep Learning and Security Workshop), June, 2018*

Invited talk on Adversarial Machine Learning, *Microsoft Research, Cambridge, June, 2018*

Invited talk on Adversarial Machine Learning, *Facebook, London, June, 2018*

Invited talk on Adversarial Machine Learning, *IBM, IBM Thomas J. Watson Research Center, October, 2017*

Invited talk on Adversarial Machine Learning, *University College London Information Security Seminar. London, January, 2018*

Invited talk on Network Traffic Analysis, *UK Gov, July, 2017*

TASP: Towards Anonymity Sets that Persist. *WPES 2016, Satellite Workshop of CCS 2016, October, 2016, Vienna, Austria*

k-fingerprinting: a Robust Scalable Website Fingerprinting Technique. *USENIX Security 2016, August, 2016, Austin, USA*

Traffic Confirmation Attacks Despite Noise. *Understanding and Enhancing Online Privacy Satellite Workshop of NDSS, February 21, 2016, San Diego, USA*

Guard Sets for Onion Routing. *Proceedings on Privacy Enhancing Technologies. Philadelphia, June, 2015*

Guard Sets for Onion Routing. *University College London Information Security Seminar. London, May, 2015*

Secure Sets in Graphs. *Programming, Logic, and Semantics Reading Group, Computer Lab, University of Cambridge, Cambridge, December, 2013*

Services

Peer-reviewer for NIPS 2018 Workshop on Security in Machine Learning

Peer-reviewer for Transactions on Information Forensics & Security

Peer-reviewer for Transactions on Pattern Analysis and Machine Intelligence

Peer-reviewer for Privacy Enhancing Technologies Symposium 2018, 2019

Co-advisor (along with George Danezis) for Axel Goetz's MSc Thesis, 'Evaluating the use of Deep Learning for Website Fingerprinting', 2017

External Peer-reviewer for CCS, October, 2017, Dallas, USA

Peer-reviewer for Privacy Enhancing Technologies Symposium, July, 2017, Minneapolis, USA

External Peer-reviewer for NDSS, February, 2016, San Diego, USA

External Peer-reviewer for IEEE Symposium on Security and Privacy, May, 2016, San Diego, USA

Skills

Knowledge of:
Python • Shell • LaTeX• Unix/Linux • Vim • Machine Learning (SK-Learn, TensorFlow, PyTorch) • Cloud Computing (Amazon AWS, Fabric)

Exposure to:
Go • JavaScript • C • SQL • HTML • CSS • Git

Code and Side Projects

Public code available at `https://github.com/jhayes14`, code for private projects available on request from `https://bitbucket.org/jhayes14`.

A note on hyperparameters in black-box adversarial examples - `https://github.com/jhayes14/black-box-attacks`

Learning Universal Adversarial Perturbations with Generative Models - `https://github.com/jhayes14/UAN`

k-fingerprinting: a Robust Scalable Website Fingerprinting Technique - `https://github.com/jhayes14/k-FP`

Generative Adversarial Network - `https://github.com/jhayes14/GAN`

Numerai competition code - `https://github.com/jhayes14/Num`

Tutorial on dangers of unencrypted web traffic - `https://github.com/jhayes14/web-uncover`

Tabber extension - `https://github.com/jhayes14/tabber`

Other

In my spare time I like to participate in Numerai (usually placing within the top 5-10%) and Kaggle competitions.

References

Please inform me if references are to be contacted.

George Danezis
Reader in Security and Privacy Engineering (Professor)
Email: g.danezis[at]ucl.ac.uk
University College London,
Dept. of Computer Science,
Gower Street, London WC1E 6BT, U.K.

Emiliano De Cristofaro
Reader in Security and Privacy Engineering (Professor)
Email: E.DeCristofaro[at]ucl.ac.uk
University College London,
Dept. of Computer Science,
Gower Street, London WC1E 6BT, U.K.

Louise Walker
Reader in Mathematics
Email: Louise.Walker[at]manchester.ac.uk
Room 2.243, Alan Turing Building
School of Mathematics,
University of Manchester
Oxford Road, Manchester M13 9PL, UK