

## Jamie Hayes

---

CONTACT INFORMATION	University College London Dept. of Computer Science Gower Street, London WC1E 6BT, U.K.	<i>Voice:</i> +44 (0) 7956959859 <i>Email:</i> <a href="mailto:j.hayes@cs.ucl.ac.uk">j.hayes@cs.ucl.ac.uk</a> <i>WWW:</i> <a href="http://www0.cs.ucl.ac.uk/staff/J.Hayes">www0.cs.ucl.ac.uk/staff/J.Hayes</a>
RESEARCH INTERESTS	Machine Learning applications to Computer Security and Privacy, Adversarial Machine Learning, Network Traffic Analysis, Anonymity Systems & Censorship Resistance	
EDUCATION	<b>Dept. of Computer Science, University College London, UK</b> <b>Sep. 2014 - Present</b> - Ph.D. candidate Privacy, Security and Machine Learning Advisor: Dr. George Danezis Second Advisor: Dr. Thore Graepel  <b>Computer Laboratory, University of Cambridge, UK</b> <b>Sep. 2013 - Apr. 2014</b> - Researcher Parameterized Computational Complexity of the Graph Isomorphism Problem Advisor: Prof. Anuj Dawar  <b>Dept. of Mathematics, University of Manchester, UK</b> <b>Sep. 2007 - Jun. 2011</b> - Master of Mathematics First Class Grade (graduated 4th out of a class of 76) Advisor: Prof. Richard Sharp  <b>Xaverian College, Manchester, UK</b> <b>Sep. 2004 - Jun. 2007</b> - A Levels  <b>Trinity C of E High School, Manchester, UK</b> <b>Sep. 1999 - Jun. 2004</b> - GCSE	
HONORS AND AWARDS	NIPS 2017 Student Travel Award  Google Phd Fellowship in Machine Learning (2017-2018)  Invited to Google PhD Summit in Security (2016) and Machine Learning (2017)  Academic Center of Excellence Scholarship, 2014  Engineering and Physical Sciences Research Council (EPSRC) Doctoral Training Studentship, 2013	
EXPERIENCE	<b>Naval Research Laboratory, Washington, DC, USA</b> <i>Internship</i> <b>August, 2017 - October, 2017</b>  Research into adversarial machine learning and network traffic analysis.  <b>Government Digital Services, London, UK</b> <i>Intern for the SecOps team</i> <b>March, 2017 - July, 2017</b>  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., 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. *To appear: 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., Danezis, G. LOGAN: Learning Universal Adversarial Perturbations with Generative Models. *Under Submission*

Hayes, J., Melis, L., Danezis, G., De Cristofaro, E. LOGAN: Evaluating Privacy Leakage of Generative Models Using Generative Adversarial Networks. *Under Submission*

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

##### PRESENTATIONS

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

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 Privacy Enhancing Technologies Symposium, July, 2018, Barcelona, Spain

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 •  $\text{\LaTeX}$  • Unix/Linux • Vim • Machine Learning (Decision Forests, SK-Learn, Neural Networks, Theano, TensorFlow, Keras, SVM, Logistic Regression, 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>.

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.

**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