

# Vasilios Mavroudis

v.mavroudis@ucl.ac.uk    mavroud.is

## Position

DPhil in Information Security, Department of Computer Science, University College London, London, UK

## Research Interests

Systems Security, Privacy-preserving Machine learning, Provably Robust Neural Networks, Security & Safety Risks from AI

## Education

2016 — Present	<b>PhD in Computer Science</b> Supervisors: Prof. George Danezis & Prof. Emiliano De Cristofaro <i>Oasis Labs &amp; Binance Research Fellowships, Werner Romberg &amp; Ferguson Grants, Top 10 young researchers at HLF, CSAW 2018 Finalist</i>	University College London, UK
2014 — 2015	<b>M.Sc. in Information Security</b> (88/100 Distinction) Thesis: "Privacy-preserving Statistics for Tor" <i>UCL Dean's List Award, UCL Excellence Scholarship, 1st at the UCL code breaking competition, Ranked 1st in MSc cohort</i>	University College London, UK
2007 — 2012	<b>B.Sc. in Applied Informatics</b> (8.51/10 Distinction) Thesis: "Cassiopeia: Real-time mobile security monitoring system" <i>Excellence Award, Top 3%</i>	University of Macedonia, Greece

## Experience

Feb 2019 — April 2019	<b>AI Safety Camp</b> <i>Part-time Research</i> Research project on cooperative inverse reinforcement learning and how non-expert demonstration trajectories could address open AI safety problems (e.g., side-effects, safe exploration).	Remote & Madrid, Spain
May 2018 — Aug 2018	<b>Systems Security Group, Swiss Federal Institute of Technology - ETH, Zurich</b> <i>Visiting Researcher</i> Designed and prototyped a decentralized and provably secure system for low-latency onchain cryptocurrency payments.	Zurich, Switzerland
Sep 2015 — Feb 2016	<b>Computer Security Group, University of California, Santa Barbara</b> <i>Research Assistant</i> Conducted a comprehensive study of the security and privacy implications of ultrasound tracking in mobile Android apps.	California, USA
July 2014 — Sep 2014	<b>Computer Security Group, University of California, Santa Barbara</b> <i>Research Assistant</i> Designed and developed a prototype that analyses JavaScript malware samples and detects samples that exhibit non-deterministic behavior in order to evade detection.	California, USA
May 2013 — May 2014	<b>Centre for Research &amp; Technology Hellas</b> <i>Research Assistant</i> I studied large-scale attacks against telecommunication networks and developed early-detection techniques based on machine learning models.	Thessaloniki, Greece
Mar 2012 — Aug 2012	<b>Deutsche Bank, GT Security/Security Information Solutions dept.</b> <i>Research Internship</i> Deployed a proof-of-concept system that used Intel IPT to protect webbanking customers from malware attacks. I also developed large-scale auditing tools for the bank's Public Key infrastructure.	Frankfurt, Germany

## Technologies

*Proficient:* Python, JavaCard; *Competent:* TensorFlow, Keras, Numpy, C++; *Prior Experience:* Java, Solidity, Javascript

## Honors, Awards, Certs & Grants

**Research Fellowship** by Oasis Labs (Sep 2019-Sep 2020)

**Research Grant** by Binance Labs on market manipulation in electronic exchanges (Jun 2019-Present)

**Cert** Coursera Deep Learning Specialization (January 2019)

**Research Grant** from the Allan & Nesta Ferguson Charitable Trust (Nov 2018)

**Award Finalist** CSAW Europe 2018 Applied Research Award (Oct 2018)

**Honor** Heidelberg Laureate Forum's 10-out-of-200 young researchers list (Sep 2018)

**Project Grant** UCL Public Engagement Unit funding for the development of "Cryptogame" (Jul 2018)

**Werner Romberg Grant** by the Heidelberg Laureate Forum (Sep 2018)

**Grant** Data Transparency Lab engagement funding (Nov 2016)

**Award** Dean's List commendee at UCL for outstanding academic performance (Apr 2016);

**Honor** Distinction in Information Security M.Sc. and ranked 1st in cohort (Nov 2015)

**Award** First place at UCL code breaking competition (May 2015)

**Scholarship** UCL Excellence Scholarship for MSc candidates (Aug 2014)

**Scholarship** Arnaoutis Foundation excellence scholarship for postgraduate studies (Sep 2014)

**Honor** 'Excellent GPA', University of Macedonia (Sep 2012)

## Selected Projects

### Encrypted Traffic Classification using High-dimensional Embeddings

This project studies the resilience of encrypted-communications schemes against adversaries that try to breach the privacy of individual users. For this purpose, we used deep neural network models to map encrypted traffic traces as high-dimensional representations (see figure on the left). We show that communication patterns suffice to reconstruct the user activity with high accuracy and thus widely-deployed encrypted-communications systems offer weaker privacy guarantees than previously thought.

### Information Leakage Classification with Deep Neural Networks

This project proposes a set of techniques that allow security researchers to evaluate the leakage properties of any chip. Using deep neural network models, we are able to outperform previously proposed methods (e.g., difference of means, multivariate templates), especially in the context of single-shot classification and small memory regions. We validate the practicality of our proposed models by classifying the leakages from the SRAM of a modern ARM Cortex-M4 chip.

### MultiBallot: A Scheme for Privacy-preserving, Verifiable Statistics

This work introduces MultiBallot, a privacy-preserving scheme that allows organizations to publish statistics derived from sensitive user data without breaching the privacy of the individual data subjects. Our scheme extends ThreeBallot (a paper-voting scheme) and provides strong data integrity guarantees and public verifiability, when combined with a high-integrity data structure (e.g., a blockchain).

### Leakage-Resilient Design for Cryptographic Devices

In this work, we relax the strict hardware correctness requirements of cryptographic devices and demonstrate how trusted, high-assurance hardware can be built from untrusted and potentially malicious components. We employ more than a hundred COTS secure cryptocoprocessors, verified to FIPS140-2 Level 4 tamper-resistance standards, and use them to realize high-confidentiality random number generation, key derivation, public key decryption and signing.

## Selected Publications

[C = Conference] [P=Preprint] [U=Under Submission]

**[U] Alexandria Nets: Large-scale Content Fingerprinting with Deep Neural Network Embeddings**

**Mavroudis V.**, Hayes J., Shehar B.

**[C] Location, location, location: Revisiting modeling and exploitation for location-based side channel leakages**

Andrikos C., Batina L., Chmielewski L., Lerman L., **Mavroudis V.**, Papagiannopoulos K., Perin G., Rassias G., Sonnino A.

25th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt) 2019

**[C] A Touch of Evil: High-Assurance Cryptographic Hardware from Untrusted Components**

**Mavroudis V.**, Cerulli A., Cvrcek D., Svenda P., Klinec D., Danezis G.

24th ACM Conference on Computer and Communications Security, Dallas, TX, November 2017

CSAW Europe 2018 Applied Research Award Finalist

**[C] On the Privacy and Security of the Ultrasound Tracking Ecosystem**

**Mavroudis V.**, Hao S., Fratantonio Y., Maggi F., Kruegel C., Vigna G.

Proceedings of the Privacy Enhancing Technologies Symposium Minneapolis, MN July 2017

**[U] Snappy: Fast Blockchain Payments.**

**Mavroudis V.**, Wuest K., Dhar A., Kostianen K., Capkun S.

Under submission & Patent Pending

**[C] Fair Order-Matching for Electronic Financial Exchanges**

**Mavroudis V.**, Melton H.

ACM conference on Advances in Financial Technologies (AFT) 2019

**[P] VAMS: Verifiable Auditing of Access to Confidential Data**

Hicks A., **Mavroudis V.**, Al-Bassam M., Meiklejohn S., and Murdoch S.

<https://arxiv.org/abs/1805.04772>, May 2018

**[C] Bounded Temporal Fairness for FIFO Financial Markets**

**Mavroudis V.**

Proceedings of the 26th International Workshop on Security Protocols, April 2019

**[C] Market Manipulation as a Security Problem: Attacks and Defenses**

**Mavroudis V.**

Proceedings of the 12th European Workshop on Systems Security (EuroSec), March 2019

**[P] Towards Low-level Cryptographic Primitives for JavaCards.**

**Mavroudis V.**, Svenda P.

<https://arxiv.org/abs/1810.01662>, Oct 2018

**[C] Eavesdropping Whilst You're Shopping: Balancing Personalisation and Privacy in Connected Retail Spaces**

**Mavroudis V.**, Veale M. (Equal Contribution)

PETRAS/IoTUK/IET Living in the IoT Conference, 2018, January 2018

## Selected Talks

**The Good, the Bad and the Ugly of the Ultrasonic Communications Ecosystem.**

[RSA Conference 2018](#), San Francisco, US, 16-20 April 2018.

**Trojan-tolerant Hardware & Supply Chain Security in Practice.**

[Defcon 25](#), Las Vegas, US, 27-30 July 2017.

**OpenCrypto: Unchaining the JavaCard Ecosystem.**

[Blackhat US](#), Las Vegas, US, 22-27 July 2017.

**On the Privacy & Security of the Ultrasound Tracking Ecosystem.**

[Mozilla International Privacy Day](#), London, UK, 28 January 2017.

**Tough Love for the ugly Ultrasound Tracking Ecosystem.**

[Chaos Communication Congress](#), Hamburg, Germany, 27-30 December 2016.

**Talking Behind Your Back: Attacks and Countermeasures of Ultrasonic Cross-device Tracking.**

[Blackhat Europe](#), London, UK, 3-4 November 2016.

## Academic Service

**Publications co-Chair: Privacy Enhancing Technologies Symposium 2019**

[August 2018 - Present](#)

**External Reviewer for the Privacy Enhancing Technologies Symposium**

[April 2017-2019](#)

**Supervised several MSc theses for the Information Security MSc program at UCL**

[August 2017 - 2019](#)

**Elected IT Officer in the Members' Council of Goodenough College, London**

[November 2016 - Present](#)

**Guest Lecturer: Masterclasses on Maths and Cryptography at the Royal Institution**

January 2018-2019

**Co-organizing the Hacking Seminars at UCL**

September 2017-May 2018

**Organizing the Information Security Seminars at UCL**

January 2017-August 2018

**Teaching Assistant *Computer Security I* module, Information Security MSc**

Winter term, 2017-2018

**Teaching Assistant for *Computer Security II* module, Information Security MSc**

Spring term, 2016-2017

**Guest Lecture on Academic Research, In2ScienceUK Organization**

August 2017

**External Reviewer: Journal of Multi-Criteria Decision Analysis, Wiley**

2014-2015

**Internal Reviewer for deliverables of the NEMESYS FP7 project**

May 2013 - Jun 2014