Vasilios Mavroudis

v.mavroudis@ucl.ac.uk ⌂ mavroud.is

Research Interests

Secure System Design, Distributed Systems, Machine Learning Robustness, Privacy-preserving computations, & Market Manipulation

Education

2016 — Present **PhD in Computer Science** University College London, UK
Supervisors: Prof. George Danezis & Prof. Emiliano De Cristofaro
Werner Romberg Grant, Top 10 young researchers at HLF,
Allan & Nesta Ferguson Grant, CSAW 2018 Finalist

2014 — 2015 **M.Sc. in Information Security** (88/100 Distinction) University College London, UK
UCL Dean's List Award, UCL Excellence Scholarship,
1st at the UCL code breaking competition, Ranked 1st in MSc cohort
Thesis: "Privacy-preserving Statistics for Tor"

2007 — 2012 **B.Sc. in Applied Informatics** (8.51/10 Distinction) University of Macedonia, Greece
Excellence Award, Top 3%
Thesis: "Cassiopeia: Real-time mobile security monitoring system"

Experience

May 2018 — Aug 2018 **Systems Security Group, Swiss Federal Institute of Technology - ETH, Zurich** Zurich, Switzerland
Visiting Researcher
Designed and prototyped a decentralized and provably secure system for low-latency onchain cryptocurrency payments.

Sep 2015 — Feb 2016 **Computer Security Group, University of California, Santa Barbara** California, USA
Research Assistant
Comprehensive study of the security and privacy implications of ultrasound tracking. This work has been published at Privacy-enhancing Technologies Symposium 2017 and received wide-spread attention. It is considered the seminal work on the security of that ecosystem.

July 2014 — Sep 2014 **Computer Security Group, University of California, Santa Barbara** California, USA
Research Assistant
Designed and developed a prototype that analyses JavaScript malware samples and detects samples that exhibit non-deterministic behavior in order to evade detection.

May 2013 — May 2014 **Centre for Research & Technology Hellas** Thessaloniki, Greece
Research Assistant
Research on security technologies for seamless service provisioning in smart mobile ecosystems. I studied large-scale attacks against telecommunication networks and developed detection algorithms and attack mitigation countermeasures.

Mar 2012 — Aug 2012 **Deutsche Bank, GT Security/Security Information Solutions dept.** Frankfurt, Germany
Research Internship
Deployed a proof-of-concept system that prevented malware from altering the contents of the Deutsche Bank's webbanking webpage by rendering sensitive parts of the page in a secure compartment of the CPU (Intel IPT). Additionally, I developed auditing tools for the bank's Public Key infrastructure.

Technologies

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

Honors, Awards, Certs & Grants

Cert Coursera Deep Learning Specialization (January 2019); **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); **Travel Grant** RISE School 2018, BlackHat US 2017, Google Summit 2016; **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); **Scholarship** Erasmus European program for internships (Mar 2012); **Scholarship** Security in IT Course, Danmarks Tekniske Universitet (Aug 2011);

Selected Publications

[C = Conference] [T=Technical Report] [P=Preprint] [U=Under Submission]

[C] Market Manipulation as a Security Problem: The case of decentralized exchanges.
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

[U] Snappy: Fast Blockchain Payments.
Mavroudis V., Wuest K., Dhar A., Kostiainen K., Capkun S.
Under Submission, Feb 2019

[U] Location, location, location: Revisiting modeling and exploitation for location-based side channel leakages.
Papagiannopoulos K., Andrikos C., Rassias G., **Mavroudis V.**, Sonnino A., Lerman L., Chmielewski L., Batina L.
Under Submission, Feb 2019

[P] Towards Low-level Cryptographic Primitives for JavaCards.
Mavroudis V., Svenda P.
`https://arxiv.org/abs/1810.01662`, Oct 2018

[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] 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

[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

[T] Anomaly detection within femtocell architectures
Liebergeld St., Lange M., Borgaonkar R., Drosou An., **Mavroudis V.**
Enhanced Network Security for Seamless Service Provisioning in the Smart Mobile Ecosystem, EU FP7, November 2104

[C] Visual Analytics for enhancing supervised attack attribution in mobile networks
Papadopoulos S., **Mavroudis V.**, Drosou A.., Tzovaras D.
29th International Symposium on Computer and Information Sciences (ISCIS), Krakow, Poland, October 2014

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

Mentoring: Supervised several MSc theses for the Information Security MSc program at UCL
August 2017 - Present

External Reviewer for the Privacy Enhancing Technologies Symposium
April 2017-Present

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-Present

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