Dimitris Karakostas

https://dimkarakostas.com
Edinburgh, Scotland, UK

Email: dimit.karakostas@gmail.com
Github: https://github.com/dimkarakostas
LinkedIn: linkedin.com/in/dimitris-karakostas/

Education

- **University of Edinburgh** — Edinburgh, Scotland, UK
  PhD in Computer Science — *2017 – 2020 (expected)*
  Researching cryptocurrency wallets, decentralised account management and applications of the Settlement Layer of Proof-of-Stake blockchains. Research Topics: *account management, stake delegation, hardware wallets.*

- **National Technical University of Athens** — Athens, Greece
  Dipl.-Ing of Electrical and Computer Engineering — *2010 – 2016*
  Degree equivalence: *B.Eng in Electrical & Computer Engineering* and *M.Eng in Computer Science* (5 years minimum)
  Thesis: Probabilistic attacks against compressed encrypted protocols

Experience

- **IOHK** — Remote
  Researcher — *Jan 2018 - present*
  Conducted research on the settlement layer of Proof-of-Stake blockchains. Designed the stake delegation mechanism of the decentralised release of Cardano.

- **SignedBlock** — Athens, Greece
  Blockchain Advisor — *Sep 2017 - present*
  Start-up blockchains consulting and development company.

- **Cryptography and Security Lab, University of Athens** — Athens, Greece
  Research Assistant — *Feb 2016 - Mar 2017*
  Investigated compression-based side-channel attacks both from a theoretical and engineering perspective. Developed the Rupture and CTX frameworks.

- **Nokia** — Athens, Greece
  Software Engineer Intern — *Apr 2015 - Feb 2016*
  Improved code health by building test automation tools used by product teams, including a Continuous Integration system and a fault predictability tool.

Technical Skills

- **Expert**: Cryptography, Blockchains, Compression/Side-channel attacks, BREACH/CRIME, MitM/Sniffing/Injection attacks, SSL/TLS, Python, Django/Flask, REST, Git
- **Advanced**: Ethereum/Solidity, Javascript, Node/React, Network/Web/Operations security, Databases, MySQL, HTML5/CSS3, Linux, Test automation/Jenkins, TCP/IP, Vim
- **Intermediate**: : C/C++, UI/UX design, Java, PHP, Subversion, LaTeX, ARM Assembly

Invited Conference Talks

- **Security BSides Athens 2017**: Attacking IPv6 - A MitM IPv6 patch for Bettercap
- **Black Hat Europe 2016**: CTX: Eliminating BREACH with Context Hiding
- **Black Hat Asia 2016**: Practical New Developments in the BREACH Attack
- **Real World Crypto 2016**: New developments in BREACH
- **Security BSides Athens 2016**: Rupture: Automating cryptanalysis of HTTPS for AES ciphers
- **FOSSCOMM Greece 2016**: Rupture - A framework to break HTTPS

Teaching

- **Blockchains & Distributed Ledgers Course 2018-2019**: Teaching Assistant, University of Edinburgh. Prepared and marked semester project and written exams, including setting up a private Ethereum testnet.
- **Cryptography Course 2015-2016**: Teaching Assistant, National Technical University of Athens. Prepared and delivered 2 2-hour lectures on web security and blockchains.
- **Security Class 2014**: Authored exercises for a series of 5 2-hour lectures on product and information security for 200 students.