ANTREAS DIONYSIOU, PHD

Special Scientist / Research Associate
Computer Science Department – SREC Group
University of Cyprus
✉dionysiou.antreas@ucy.ac.cy
☎(+357) 99 041 655

Education

- 2020-2024: Ph.D. in Computer Science, University of Cyprus.
  Thesis: Hardening Modern Systems and Services for Protecting User Privacy.
  Advisor: Assoc. Prof. Elias Athanasopoulos.
- 2018-2019: M.Sc. in Computer Science with Specialization in Intelligent Systems, University of Cyprus.
  Graduated with first class honours. GPA: 9/10
  Dissertation: Assessing the Impact of Deep Learning on Internet Services' Security Mechanisms.
  Advisor: Assoc. Prof. Elias Athanasopoulos.
- 2014-2018: B.Sc. in Computer Science, University of Cyprus.
  Graduated with first class honours. GPA: 9.05/10
  Dissertation: Protein Secondary Structure Prediction using Convolutional Neural Networks in Combination with Gabor Filters and Support Vector Machines.
  Advisor: Prof. Chris Christodoulou.
- 2021: US Department of Defense: Identifying and Safeguarding Personally Identifiable Information (PII)
- 2010-2014: CISCO CCNA Discovery.
- 2010-2012: Cambridge GCE A Level Computing.
- 2009-2012: High School Apolytirion, Kato Polemidia Lyceum, Limassol, Cyprus.
- 2010-2011: Cambridge IGCSE English as a Second Language.
- 2008-2010: Cambridge IGCSE Information and Communication Technology.
- 2007-2010: European Computer Driving License (ECDL) Certified.

Employment

- September 2018 – now: University of Cyprus, Research Associate at Security Research in Cyprus (SREC) group.
- November 2020 – March 2022: Nearix, Data Scientist/Machine Learning Engineer (part-time).
- March 2016 – March 2018: University of Cyprus, Research Associate at Computational Intelligence and Neuroscience (CIN) group.
- June 2017 – August 2017: Deloitte Ltd, Software Engineer at Cyber Risk/Security Team (internship).
- July 2012 – July 2014: Soldier at Cypriot National Guard. Information and Communication Department.

Teaching

Teaching Assistant

- CS667: Computational Neuroscience, University of Cyprus, Spring 2021, 2022, 2023, 2024.

- DSC517: Data Security, University of Cyprus, Fall 2023.
- CS325: Parallel Processing, University of Cyprus, Spring 2023.
- CS444: Computational Intelligent Systems, University of Cyprus, Spring 2022, 2024.
- CS133: Object-Oriented Programming, University of Cyprus, Fall 2022.
- CS682: Advanced Security Topics, University of Cyprus, Fall 2021.

Scholarships

- Huawei Technologies (Cyprus) Co. Ltd., Seeds for the Future Scholarship for Academic Excellence (2024).
- "Evagoras and Praxandros" Scholarship. University of Cyprus, Covers PhD Tuition Fees (2020-2024).
- Cyprus State Scholarship Foundation, MSc and PhD Scholarship for Academic Excellence (2018-2024).
- Logicom Public Ltd., MSc and PhD Scholarship for Academic Excellence (2018-2024).
- Graduate Research Fellowship, SREC, Dr. Elias Athanasopoulos, 2019-2024.

Entrepreneurship

- June 2022 – now: Ergonact Ltd, Co-founder.
- September 2020 – March 2024: Ag Catalytic Solutions Ltd, Co-founder.
- March 2020 – October 2020: Climate-KIC Accelerator: Stage 2.
- February 2018 – September 2018: Ecofy Ltd, Co-founder & CEO.
- April 2018 – June 2018: Participating Startup (Ecofy Ltd) at IDEA Startup Incubator – Accelerator.
- June 2019 – September 2019: ClimateLaunchpad Climate-KIC Regional Innovation Scheme Accelerator Programme.

Awards

- Distinguished paper award finalist (IEEE EuroS&P 2022).
- 1st position at ClimateLaunchpad Climate-KIC National Finals.
- Awards of Academic Excellence for the Master student with the highest academic performance of the University of Cyprus, the Faculty of Pure and Applied Sciences and the Department of Computer Science.
- JCC Payment Systems Ltd, Award for Academic Excellence (BSc).
- iSignThis Ltd, Award for Academic Excellence in Artificial Intelligence and Systems Security (BSc).
- University of Cyprus, Department of Computer Science, Award for Academic Excellence (BSc).

Service

Program Committee

- Information Security Conference (ISC), 2024.
- EAI International Conference on Security and Privacy in Communication Networks (SecureComm), 2024.
- International Conference on Advanced Information Networking and Applications (AINA), 2024.
- International Conference on Distributed Computing Systems (ICDCS), 2023, 2024.
- International Smart Cities Conference (ISC2), 2022.
- International Conference on Artificial Intelligence Applications & Innovations (AIAI), 2019.
- International Conference on Engineering Applications of Neural Networks (EANN), 2019.
- International Conference on Artificial Neural Networks (ICANN), 2018.

Reviewing for Journals

- Elsevier Computers & Security.
- Springer Neural Computing & Applications.
- Elsevier Computer Methods and Programs in Biomedicine.

Artifact Evaluation Committee

- USENIX Security Symposium, 2024.
- International European Conference on Parallel and Distributed Computing (EuroPar), 2023.
- USENIX Security Symposium, 2020.

European Funded Projects

Research Associate

- SecOPERA: Secure Open-source softwarE and hardwaRe Adaptable framework (HORIZON-CL3-2021-CS-01). Duration 2023-2025.
- CyberSecPro: Collaborative, Multi-modal and Agile Professional Cybersecurity Training Program for a Skilled Workforce In the European Digital Single Market and Industries (Horizon Digital Europe). Duration 2022-2025.
- CyberSec4Europe: Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research and Innovation Roadmap. Funded by The European Commission (H2020/SU-ICT-03-2018). Duration 2019-2022.
- PERSONAS: Situational Awareness, Control and Security Policies Enforcement on Multiple Virtualization Personas of Personal Devices. Funded by Research Promotion Foundation (RESTART/ENTERPRISES). Duration 2018-2020.

Selected Publications

1. Antonis Louka, Antreas Dionysiou, and Elias Athanasopoulos. Validating Memory Safety in Rust Binaries. *In Proceedings of the 17th European Workshop on Systems Security (EuroSec)*, April, 2024. Athens, Greece.
2. Antreas Dionysiou and Elias Athanasopoulos. SoK: Membership Inference is Harder than Previously Thought. *In Proceedings of the 23rd Privacy Enhancing Technologies Symposium (PETS)*, June, 2023. Lausanne, Switzerland.
3. Antreas Dionysiou, Vassilis Vassiliades, and Elias Athanasopoulos. Exploring Model Inversion Attacks in the Black-box Setting. *In Proceedings of the 23rd Privacy Enhancing Technologies Symposium (PETS)*, June, 2023. Lausanne, Switzerland.
4. Antreas Dionysiou and Elias Athanasopoulos. Lethe: Practical Data Breach Detection with Zero Persistent Secret State. *In Proceedings of the 7th IEEE European Symposium on Security and Privacy (EuroS&P)*, June, 2022. Genoa, Italy. ***Distinguished paper award finalist.***
5. Antreas Dionysiou and Elias Athanasopoulos. Unicode Evil: Evading NLP Systems Using Visual Similarities of Text Characters. *In Proceedings of the 14th ACM Workshop on Artificial Intelligence and Security (AISEC)*, November, 2021. Virtual.
6. Antreas Dionysiou, Vassilis Vassiliades, and Elias Athanasopoulos. HoneyGen: Generating Honeywords Using Representation Learning. *In Proceedings of the 16th ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, June, 2021. Hong Kong, China (virtual).
7. Antreas Dionysiou and Elias Athanasopoulos. SoK: Machine vs. Machine - A Systematic Classification of Automated Machine Learning-based CAPTCHA Solvers. *In Proceedings of the Computers & Security*, 97, 101947, July, 2020.
8. Antreas Dionysiou, Michalis Agathocleous, Chris Christodoulou and Vasilis Promponas. Convolutional Neural Networks in Combination with Support Vector Machines for Complex Sequential Data Classification. *In Proceedings of the 27th International Conference on Artificial Neural Networks (ICANN)*, October, 2018. Rhodes, Greece.

Contributed Book Chapters

- Blue Book – A set of cybersecurity roadmaps and challenges for researchers and policymakers. Ch. Machine Learning, 2022. https://the-blue-book.eu/