Academic Personnel Short Profile / Short CV

University:	Frederick University
Surname:	Dionysiou
Name:	Antreas
Rank/Position:	Lecturer
Faculty:	School of Engineering
Department:	Electrical Engineering, Computer Engineering and Informatics
Scientific Domain: *	Computer Security

Academic qualifications

Qualification	Year	Awarding Institution	Department	Thesis title (Optional Entry)
PhD in Computer Science	2024	University of Cyprus	Computer Science Department	Hardening Modern Systems and Services for Protecting User Privacy
MSc in Computer Science with Specialization in Intelligent Systems (First Class Honours)	2019	University of Cyprus	Computer Science Department	Assessing the Impact of Deep Learning on Internet Services' Security Mechanisms
BSc in Computer Science (First Class Honours)	2018	University of Cyprus	Computer Science Department	Protein Secondary Structure Prediction using Convolutional Neural Networks in Combination with Gabor Filters and Support Vector Machines

Employment history in Academic Institutions/Research Centers				
Period of employment		Employer	Location	Position
From	To			
September 2024	NOW	Dept. of Electrical Engineering, Computer Engineering and Informatics, Frederick University	Limassol, Cyprus	Lecturer
September 2018	August 2024	Security Research in Cyprus (SREC) group, University of Cyprus	Nicosia, Cyprus	Research Associate
September 2016	June 2020	Computational Intelligence and Neuroscience (CIN) group, University of Cyprus	Nicosia, Cyprus	Research Associate

Key ***refereed*** journal papers, monographs, books, conference publications etc.						
Ref. Number	**Year**	**Title**	**Other authors**	**Journal and Publisher / Conference**	**Vol.**	**Pages**
1	2024	Validating Memory Safety in Rust Binaries	Antonis Louka, **Antreas Dionysiou**, and Elias Athanasopoulos	In Proceedings of the 17th European Workshop on Systems Security (EuroSec)	DOI	8-14
2	2023	SoK: Membership Inference is Harder than Previously Thought	**Antreas Dionysiou** and Elias Athanasopoulos	In Proceedings of the 23rd Privacy Enhancing Technologies Symposium (PETS)	DOI	286-306
3	2023	Exploring Model Inversion Attacks in the Black-box Setting	**Antreas Dionysiou**, Vassilis Vassiliades, and Elias Athanasopoulos	In Proceedings of the 23rd Privacy Enhancing Technologies Symposium (PETS)	DOI	190-206
4	2022	Lethe: Practical Data Breach Detection with Zero Persistent Secret State	**Antreas Dionysiou** and Elias Athanasopoulos	In Proceedings of the 7th IEEE European Symposium on Security and Privacy (EuroS&P), *Distinguished paper award finalist*	DOI	223-235
5	2021	Unicode Evil: Evading NLP Systems Using Visual Similarities of Text Characters	**Antreas Dionysiou** and Elias Athanasopoulos	In Proceedings of the 14th ACM Workshop on Artificial Intelligence and Security (AISEC)	DOI	1-12

6	2021	HoneyGen: Generating Honeywords Using Representation Learning	**Antreas Dionysiou**, Vassilis Vassiliades, and Elias Athanasopoulos	In Proceedings of the 16th ACM Asia Conference on Computer and Communications Security (AsiaCCS)	DOI	265-279
7	2020	SoK: Machine vs. Machine - A Systematic Classification of Automated Machine Learning-based CAPTCHA Solvers	**Antreas Dionysiou** and Elias Athanasopoulos	In Proceedings of the Elsevier Computers & Security	DOI	101947
8	2018	Convolutional Neural Networks in Combination with Support Vector Machines for Complex Sequential Data Classification	**Antreas Dionysiou**, Michalis Agathocleous, Chris Christodoulou and Vasilis Promponas	In Proceedings of the 27th International Conference on Artificial Neural Networks (ICANN)	DOI	444-455

Research Projects

Ref. Number	Date	Title	Funded by	Project Role*
1	2023-2025	SecOPERA: Secure Open-Source Software and Hardware Adaptable Framework	Horizon Europe	WP Leader / Research Associate
2	2022-2025	CyberSecPro: Collaborative, Multi-modal and Agile Professional Cybersecurity Training Program for a Skilled Workforce In the European Digital Single Market and Industries	Horizon Europe	Research Associate
3	2019-2022	CyberSec4Europe: Establishing and Operating a Pilot for a Cybersecurity Competence Network to Develop and Implement a Common Cybersecurity Research and Innovation Roadmap	Horizon 2020	Research Associate
4	2018-2020	PERSONAS: Situational Awareness, Control and Security Policies Enforcement on Multiple Virtualization Personas of Personal Devices	RIF	WP Leader / Research Associate
5	2020-2023	LightSense: Intelligent Light Sensing for Next Generation Smart Grids	RIF	Data Scientist / Machine Learning Engineer

**Project Role: i.e. Scientific/Project Coordinator, Research Team Member, Researcher, Assistant Researcher, other*

Academic Consulting Services and/or Participation in Councils / Boards/ Editorial Committees				
Ref. Number	**Period**	**Organization**	**Title of Position or Service**	**Key Activities**
1	2024	International Conference on Network and System Security (NSS)	Program Committee	Paper Reviewer
2	2024	International Conference on Security and Cryptography (SECRYPT)	Program Committee	Paper Reviewer
3	2024	Information Security Conference (ISC)	Program Committee	Paper Reviewer
4	2024	EAI International Conference on Security and Privacy in Communication Networks (SecureComm)	Program Committee	Paper Reviewer
5	2024	International Conference on Advanced Information Networking and Applications (AINA)	Program Committee	Paper Reviewer
6	2023, 2024	International Conference on Distributed Computing Systems (ICDCS),	Program Committee	Paper Reviewer
7	2024-NOW	Springer Nature Scientific Reports (Journal)	Program Committee	Paper Reviewer
8	2024-NOW	IEEE Transactions on Services Computing (Journal)	Program Committee	Paper Reviewer
9	2020-NOW	Elsevier Computers & Security (Journal)	Program Committee	Paper Reviewer
10	2022-NOW	Springer Neural Computing & Applications (Journal)	Program Committee	Paper Reviewer
11	2023-NOW	Elsevier Computer Methods and Programs in Biomedicine (Journal)	Program Committee	Paper Reviewer
12	2020, 2024	USENIX Security Symposium	Artifact Evaluation Committee	Artifact Reviewer
13	2022	International Smart Cities Conference (ISC2)	Program Committee	Paper Reviewer
14	2023	International European Conference on Parallel and Distributed Computing (EuroPar)	Artifact Evaluation Committee	Artifact Reviewer
15	2019	International Conference on Artificial Intelligence Applications & Innovations (AIAI)	Program Committee	Paper Reviewer
16	2019	International Conference on Engineering Applications of Neural Networks (EANN)	Program Committee	Paper Reviewer
17	2018	International Conference on Artificial Neural Networks (ICANN)	Program Committee	Paper Reviewer

Awards / International Recognition			
Ref. Number	**Date**	**Title**	**Awarded by:**
1	2019-2024	Graduate Research Fellowship	Security Research in Cyprus (SREC) group, University of Cyprus
2	2024	Seeds for the Future Scholarship for Academic Excellence	Huawei Technologies (Cyprus) Co. Ltd
3	2020-2024	“Evagoras and Praxandros” Scholarship (Covers PhD Tuition Fees)	University of Cyprus
4	2020-2024	PhD Scholarship for Academic Excellence	Cyprus State Scholarship Foundation
5	2018-2019	MSc Scholarship for Academic Excellence	Cyprus State Scholarship Foundation
6	2020-2024	PhD Scholarship for Academic Excellence	Logicom Public Ltd
7	2018-2019	MSc Scholarship for Academic Excellence	Logicom Public Ltd
8	2020	1st position at ClimateLaunchpad Climate-KIC National Finals	EIT Climate-KIC
9	2019	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	University of Cyprus
10	2018	Award for Academic Excellence (BSc)	JCC Payment Systems Ltd
11	2018	Award for Academic Excellence in Artificial Intelligence and Systems Security (BSc)	iSignThis Ltd
12	2018	Award for Academic Excellence (BSc)	University of Cyprus