Antonis Michalas

Head of Cyber Security Group

✉ : amichalas@outlook.com
: +44 77245-70070
: www.amichalas.com

Education

2009 – 2013 **PhD in Network Security**, *University of Aalborg*, Aalborg, Denmark.
Main Academic Interests: Network Security, Privacy, Trust, Cryptography, e-Voting, Reputation Systems, Cloud Security, Trusted Computing, Urban Sensing, Privacy, and...anything that looks interesting.

2006 – 2007 **Masters in Information Technology and Telecommunications**, *Athens Information Technology*, Athens, Greece.
Main Academic Interests: Computer Security, e-Learning, Web Technologies, Semantic Web.

2000 – 2006 **Degree in Mathematics**, *University of Crete*, Heraklion, Crete.
Main Academic Interests: Algebra, Approximation Theory, Mathematical Programming.

PhD Thesis

Title *Trust & Privacy in Distributed Networks*

Supervisors Professor Neeli R. Prasad & Professor Nikos Komninos

External Collaboration During my PhD I participated in the following external activities:
- Summer School. "*Mobile systems and eHealth security*". University of Agder, Norway, Grimstad
- Visitor for one month at Ben Gurion University, Beersheva, Israel
- Visitor for three months at Princeton University, New Jersey, USA

Professional Experience

09/2015 – Current **Lecturer in Cyber Security**, University of Westminster, Computer Science.
As a lecturer (assistant professor) I am teaching both undergraduate and postgraduate courses related to cryptography, forensics, cyber security and network security. My role expands to student supervision and research group coordination. In parallel, I am an active member of the department's project development and research activities. In addition to that, I am leading the cyber security research group at the University of Westminster. As the head of the cyber security research group, I lead research projects focused on network security and cryptography. The group comprises PhD students, professors and researchers. We mainly focus on applied research in security and privacy of widely deployed communication networks.

01/2014 – 09/2015 **Postdoctoral Researcher**, Swedish Institute of Computer Science (SICS).
Actively involved in the current national and European research projects in the Security Lab, where I combine research with student supervision and project management. Within one year of starting at SICS, I have successfully obtained funding for three EU projects. Currently, I conduct research in the field of Security & Privacy for People-Centric Sensing, Cloud Computing, Trusted Computing, e-Voting Systems and Secure & Privacy Preserving e-Health Systems.

03/2013 – 01/2014 **Security Consultant**, Cyber Defence Department, Hellenic Army.
Responsible for implementing and managing an information encryption system for the specific needs of the Hellenic Army. My work involved designing a secure single sign on protocol which connects online services of different web applications used by the military personnel. Additionally, I was tasked with improving the security of existing systems/applications by staging attacks and providing solutions for any discovered vulnerabilities.

2011 – 2012 **Senior Web Developer**, DPG Digital Media, Athens, Greece.
I was the team manager for Web-Related Projects. More precisely, I was responsible for talking directly with the clients and the Management Department in order to understand the needs of each project. Moreover, I was distributing the work to developers based on the requirements of each project while at the same time I was responsible for evaluating each part of the deliverable as well as programming the most demanding parts of the projects.
Main working environments: php, mysql, javascript, jquery, ajax, xml, json

2009 – 2011 **Researcher**, Athens Information Technology, Athens, Greece.
Conducting research in network security. More precisely, my research focused on private and secure e-voting systems, reputation systems, privacy in decentralized environments, cloud computing and privacy preserving protocols in participatory sensing applications.

2008 – 2009 **Software Engineer**, I-Cube S.A., Athens, Greece.
Development of European Union research projects.
Main working environments: microsoft .net (c#, vb), javascript, mysql, php, jquery, ajax and web services

2007 – 2008 **Software Engineer**, Intralot S.A., Athens, Greece.
Programming and development of lottery-related games in Europe, the USA and Australia.
Main working environments: microsoft .net (c#, vb), javascript, oracle, crystal reports and web services

2001 – 2004 **Web Developer**, Webline S.A., Heraklion, Crete.
During my undergraduate studies I worked as a Web Developer at Webline S.A.
Main working environments: xhtml, php, mysql, javascript, xml

Projects

2015 – 2018 **PaaSword**, *EU H2020 Project*.
The vision is to fortify trust in cloud services and increase the adoption rate of cloud-based solutions. To this end, we design and develop mechanisms that safeguard both corporate and personal data for cloud infrastructures and storage services. Furthermore, by addressing major cloud security challenges, we provide essential knowledge to organizations that wish to securely migrate to the cloud. Six pilots together with EU industrial partners will be implemented.

2015 – 2016 **Trusted Telecommuncation IaaS Platform**, *EU EIT Project*.
This project mainly focus on the design and implementation of data confidentiality and integrity protection mechanisms for IaaS clouds that will open up radical new telecommunication business opportunities. In particular this new business offering will allow transparent storage isolation between IaaS clients and their data. The main target for the activity is to extend the OpenStack open source project with particular focus on secure storage. In particular, one important task is to extend the previous results with novel principles for efficient data search over encrypted data (Symmetric Searchable Encryption).

2013 – 2014 **InfraCloud**, *Swedish National Project*.
InfraCloud is a Swedish project that targets the security of critical information in an infrastructure as a Service (IaaS) cloud. More precisely, InfraCloud utilizes and builds upon previous research on the verification of computer resources in public IaaS clouds and paves the way for applications and organizations that wishes to securely move to a public cloud. In addition to that, the absence of reliable data sharing mechanisms is addressed by providing a framework, which enables clients of IaaS clouds to securely share data and clearly define access rights granted to peers.

2010 – 2011 **Secure Single Sign On & Identity Management**, *Greek National Project*.
The concept of this project was to design and implement a secure Single-Sign-On (SSO) framework and Identity Management System for an international company. In a SSO approach users authenticate themselves only once and they are automatically logged into application servers as necessary without required any further interaction. For the needs of this project, I implemented the Kerberos architecture in order to secure the login procedure without sending the password over the channel as well as for securing each request from users. To do so, each *http* request was based on unique tickets with unique session keys. Thus providing an additional level of security.

2009 – 2010 **PERFORM**, *EU FP7 Project*.
The PERFORM project aims to tackle problems associated with the efficient remote health status monitoring, the qualitative and quantitative assessment and the treatment personalization for people suffering from neurodegenerative diseases and movement disorders, such as Parkinson's disease (PD). Aspires to research and develop an innovative, intelligent system for monitoring neurodegenerative disease evolution through the employment of a wide range of wearable micro-sensors, advanced knowledge processing and fusion algorithms.

2009 **I-WAY**, *EU FP7 Project*.
A Geographic Information System for a European Research program. The goal of I-WAY is to develop a multi-sensorial system that can ubiquitously monitor and recognize the psychological condition of driver as well as special conditions prevailing in the road environment.

Funding

2017 **Horizon H2020-IND-CE-2016-17**.
Project Title: Cloudification of Production Engineering for Predictive Digital Manufacturing (CloudiFacturing).
Duration & Grant: Research funding for 3.5 years (*8,712,521€, 33 Partners*).
Role: WP Leader & Researcher.
Status: Active.

Horizon H2020-DS-2016-2017.
Project Title: A Novel Information Driven Cyber Security Management Framework for Cloud Computing Services Powered by Linked Data and Advanced Analytics Technologies (SHIELD).
Duration & Grant: Research funding for 3 years (*4,223,940€, 12 Partners*).
Role: WP Leader & Researcher.
Status: Under Review.

2016 **Horizon H2020-ICT-06-2016**.
Project Title: Cloud Orchestration at the Level of Application (COLA).
Duration & Grant: Research funding for 3.5 years (*4,238,580€, 14 Partners*).
Role: WP Leader & Researcher.
Status: Active.

2015 **ICT-TNG Proposal**.
Project Title: Efficient Cloud-Based Privacy Preserving Mobile Sensing.
Duration & Grant: Research funding for 1 year (≈ *53,421€, Individual Funding*).
Role: Project Leader & Researcher.
Status: Completed.

2014 **Horizon H2020-ICT-2014-1 Proposal**.

Project Title: A Holistic Data Privacy and Security by Design Platform-as-a-Service Framework Introducing Distributed Encrypted Persistence in Cloud-based Applications (PaaSword).
Duration & Grant: Research funding for 3 years (*3,984,575€, 10 Partners*).
Role: Scientific Coordinator & Researcher.
Status: Active.

European Institute of Innovation & Technology (EIT) Proposal.

Project Title: Trusted Telecommunication IaaS Platform.
Duration & Grant: Research funding for 1 year (*320,000€, 3 Partners*).
Role: Project Leader & Researcher.
Status: Completed.

Teaching - Supervising

2015 – Current **University of Westminster**.

Since September 2016 I am the course leader for the Cyber Security and Forensics MSc at the University of Westminster. In addition to that, as a lecturer I have been involved in the following undergraduate and postgraduate courses:

A. Postgraduate

- Internet Security (Module Leader)
- Computer Security & Applications (Module Leader)

B. Undergraduate

- Security & Forensics (Assistant)
- Information Technology Security (Module Leader)
- Algorithms and Complexity (Assistant)

2009 – 2011 **Athens Information Technology**.

As a researcher I have been regularly involved in the provision (by giving a number of lectures and organizing lab exercises/seminars) of the following undergraduate level courses: Web Technologies and Programming, Cryptography, Network Security, Linear Algebra, Calculus, Mathematical Analysis.

Supervising PhD Students.

- **Ali Haidar:** PhD Thesis "Attribute-Based Encryption Techniques for Platform-as-a-Service Clouds"
  University of Westminster, London, UK. Degree expected end of 2019.
- **Nicolae Paladi:** PhD Thesis "Storage Security in Infrastructure as a Service Clouds"
  In collaboration with Lund University, Sweden. Degree expected end of 2017.

Supervising MSc Students.

- **Felipe Solferini:** The Race of Cryptocurrency.
  University of Westminster, London, UK.
- **Kashif Ghafoor:** Are Your Pictures Truly Yours?
  University of Westminster, London, UK.
- **Joolokeni Haimbala:** Secure Cloud Storage with a focus on Searchable Encryption.
  University of Westminster, London, UK.
- **Rohan Murray:** MemTri: A Memory Forensics Triage Tool using Bayesian Network and Volatility.
  University of Westminster, London, UK.

Publications

Journals

2017.

- Rafael Dowsley, **Antonis Michalas**, Matthias Nagel and Nicolae Paladi. "*A Survey on Design and Implementation of Protected Searchable Data in the Cloud*". Journal of Computer Science Review, Elsevier, 2017.
- Y. Verginadis, **Antonis Michalas**, P. Gouvas, G. Schiefer, G. Hubsch and I. Paraskakis. "*PaaS-word: A Holistic Data Privacy and Security by Design Framework for Cloud Services*". Journal of Grid Computing, a special issue on "Cloud Computing and Services Science". Springer, 2017.
- Kassaye Yitbarek Yigzaw, **Antonis Michalas** and Johan Gustav Bellika. "*Secure and Scalable Deduplication of Horizontally Partitioned Health Data for Privacy-Preserving Distributed Statistical Computation*". Journal of Medical Informatics and Decision Making (BMC), 2017.

2016.

- Nicolae Paladi, Christian Gehrmann and **Antonis Michalas**. "*Providing End-User Security Guarantees in Public Infrastructure Clouds*". IEEE Transactions on Cloud Computing, a special issue on "Cloud Security Engineering", IEEE, 2016.
- Kassaye Yitbarek Yigzaw, **Antonis Michalas** and Johan Gustav Bellika. "*Secure and scalable statistical computation of questionnaire data in R*". IEEE Access Journal, a special issue of Big Data Analytics for Smart and Connected Health, IEEE, 2016.

2014.

- Tassos Dimitriou and **Antonis Michalas**. "*Multi-Party Trust Computation in Decentralized Environments in the Presence of Malicious Adversaries*". Ad Hoc Networks Journal, a special issue on "Smart Solutions for Mobility Supported Distributed and Embedded Systems", Elsevier, 2014.

2012.

- **Antonis Michalas**, Tassos Dimitriou, Thanassis Gianetsos, Nikos Komninos and Neeli R. Prasad. "*Vulnerabilities of Decentralized Additive Reputation Systems Regarding the Privacy of Individual Votes*". Springer Wireless Personal Communication, Springer, 2012.

2011.

- **Antonis Michalas**, Nikos Komninos and Neeli R. Prasad. "*Mitigate DoS and DDoS attack in Ad Hoc Networks*". International Journal of Digital Crime and Forensics, IGI Global, 2011.

Conferences

2017.

- **Antonis Michalas** and Rohan Murray. "*MemTri: A Memory Forensics Triage Tool using Bayesian Network and Volatility*". Proceedings of the 9th ACM CCS International Workshop on Managing Insider Security Threats (MIST'17) in Conjunction with ACM CCS 2017, Dallas, USA, October 30 – November 03, 2017.
- **Antonis Michalas** and Ryan Murray. "*Keep Pies Away from Kids: A Raspberry Pi Attacking Tool*". Proceedings of the 1st ACM CCS International Workshop on Internet of Things Security and Privacy (IoT S&P'17) in Conjunction with ACM CCS 2017, Dallas, USA, October 30 – November 03, 2017 (Accepted as a Poster/Short Paper).
- Jose Costa and **Antonis Michalas**. "*Middle Man: An Efficient Two-Factor Authentication Framework*". Proceedings of the 3rd IEEE International Conference On Computing, Communication, Control And Automation, Pune, India, August 17-18, 2017. (Invited).
- **Antonis Michalas** and Noam Weingarten. "*HealthShare: Using Attribute-Based Encryption for Secure Data Sharing Between Multiple Clouds*". Proceedings of the 30th IEEE International Symposium on Computer-Based Medical Systems (CBMS'17), Thessaloniki, Greece, 2017.

2016.

- **Antonis Michalas** and Kassaye Yitbarek Yigzaw. "*LocLess: Do You Really Care Your Cloud Files Are?*". Cloud Security and Data Privacy by Design (CloudSPD'16), Workshop co-located with the 9th IEEE/ACM International Conference on Utility and Cloud Computing, Luxembourg, December 12-15, 2016.
- **Antonis Michalas**. "*Sharing in the Rain: Secure and Efficient Data Sharing for the Cloud*". Proceedings of the 11th IEEE International Conference for Internet Technology and Secured Transactions (ICITST'16), Barcelona, Spain, December 5-7, 2016.
- **Antonis Michalas** and Thanassis Giannetsos. "*The Data of Things: Strategies, Patterns and Practice of Cloud-based Participatory Sensing*". International Conference on Innovations in Info-business and Technology (ICIIT), Sri Lanka, March 4-5, 2016. (Position Paper)

2015.

- **Antonis Michalas** and Rafael Dowsley. "*Towards Trusted eHealth Services in the Cloud*". Cloud Security and Data Privacy by Design (CloudSPD'15), Workshop co-located with the 8th IEEE/ACM International Conference on Utility and Cloud Computing, Limassol, Cyprus, December 7-10, 2015.
- Y. Verginadis, **Antonis Michalas**, P. Gouvas, G. Schiefer, G. Hubsch and I. Paraskakis. "*PaaS-word: A Holistic Data Privacy and Security by Design Framework for Cloud Services*". In the 5th International Conference on Cloud Computing and Services Science (CLOSER'15), 20-22 May, 2015, Lisbon, Portugal. (Position Paper)

2014.

- **Antonis Michalas**, Nicolae Paladi and Christian Gehrmann. "*Security Aspects of e-Health Systems Migration to the Cloud*". Proceedings of the 16th IEEE International Conference on E-health Networking, Application & Services (Healthcom), October 15 - 18, 2014, Natal, Brazil.
- Nicolae Paladi, **Antonis Michalas** and Christian Gehrmann. "*Domain Based Storage Protection with Secure Access Control for the Cloud*". The 2014 International Workshop on Security in Cloud Computing, held in conjunction with the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS), June 3, 2014, Kyoto, Japan.
- **Antonis Michalas** and Nikos Komninos. "*The Lord of the Sense: A Privacy Preserving Reputation System for Participatory Sensing Applications*". Proceedings of the 19th IEEE International Conference on Communications (ISCC'14), Madeira, Portugal, 2014.
- Nicolae Paladi and **Antonis Michalas**. "*One of Our Hosts in Another Country: Challenges of Data Geolocation in Cloud Storage*". Proceedings of the 6th IEEE Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), May 11 - 14, 2014, Aalborg, Denmark. (Invited)

2012.

- **Antonis Michalas** and Menelaos Bakopoulos. "*SecGOD - Google Docs: Now I Feel Safer!*". Proceedings of the 7th IEEE International Conference for Internet Technology and Secured Transactions (ICITST'12), London, UK, 2012.
- **Antonis Michalas**, Menelaos Bakopoulos, Nikos Komninos and Neeli R. Prasad. "*Secure & Trusted Communication in Emergency Situations*". Proceedings of the 35th IEEE Sarnoff Symposium, Newark, New Jersey, USA, 2012.
- Tassos Dimitriou and **Antonis Michalas**. "*Multi-Party Trust Computation in Decentralized Environments*". Proceedings of the 5th IFIP International Conference on New Technologies, Mobility & Security (NTMS'12), Istanbul, Turkey, 2012.

2011.

- **Antonis Michalas**, Tassos Dimitriou, Thanassis Gianetsos, Nikos Komninos and Neeli R. Prasad. "*Vulnerabilities of Decentralized Additive Reputation Systems Regarding the Privacy of Individual Votes*". Proceedings of the 3rd International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (MobiSec'11), Aalborg, Denmark, 2011.**(Best Paper Award)**
- **Antonis Michalas**, Vladimir A. Oleshchuk, Nikos Komninos and Neeli R. Prasad. "*Privacy-preserving Trust Establishment scheme for Mobile Ad Hoc Networks*". Proceedings of the 16th IEEE International Conference on Communications (ISCC'11), Corfu, Greece, 2011.
- **Antonis Michalas**, Nikos Komninos and Neeli R. Prasad. "*Multiplayer Game for DDoS Attacks Resilience in Ad hoc Networks*". Proceedings of the 2nd IEEE International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless Vitae 2011), Chennai, India, 2011.

2010.

- **Antonis Michalas**, N. Komninos, Neeli R. Prasad and Vladimir A. Oleshchuk. "*New Client Puzzle Approach for DoS Resistance in Ad hoc Networks*". Proceedings of the IEEE International Conference on Information Theory and Information Security (ICITIS'10), Beijing, China, 2010.

Book Chapters

2011.

- **Antonis Michalas**, Nikos Komninos and Neeli R. Prasad. "*Cryptographic Puzzles and Game Theory against DoS and DDoS attacks in Networks*". Encryption: Methods, Software and Security", Nova Science Publishers, 2011.

Invited Talks

07/09/2017 **RISE SICS Security Day**, *RISE, Stockholm, Sweden*.
Title: Trust in Public Clouds and...Keep Pies Away from Kids!.

22/02/2017 **Panel Discussion**, *The European Information Security Summit (TEISS'17), London, UK*.
Title: Segregating third party access in the cloud.

17/02/2017 **Keynote Speaker**, *IEEE International Conference on Internet of Things, Next Generation Networks and Cloud Computing (ICINC'17), Pune, India*.
Title: Sharing in the Rain: Security, Privacy and Trust in Cloud Computing and Internet of Things.

02/03/2016 **Guest Lecture**, *IIT University, Colombo, Sri Lanka*.
Title: Introduction to Cyber Security.

10/03/2015 **Advances in Cryptography & Coding**, *Chalmers University, Gothenburg, Sweden*.
Title: No More Dark Clouds: Towards Trusted Cloud Environments.

05/02/2014 **Swedish Institute of Computer Science**, *Stockholm, Sweden*.
Title: Trust & Privacy in Distributed Networks.

04/02/2013 **Athens Information Technology**, *Athens, Greece*.
Title: Multi-Party Trust Computation in Decentralized Environments in the Presence of Malicious Adversaries.

In the Media

28/06/2017 **Interview/Panel Discussion on Al Jazeera**.
Title: How can cyberattacks be stopped?
Link: `http://tinyurl.com/y7xk8p8r`

18/05/2017 **Article at the online magazine "Huffington Post"**.
Title: Three Things We Have Learnt From The WannaCry Cyber Attack
Link: `http://tinyurl.com/yd37orqr`

28/03/2017 **Article at the online magazine "The Conversation"**.
Title: How WhatsApp encryption works – and why there shouldn't be a backdoor
Link: `http://tinyurl.com/lt3mzsm`

26/03/2017 **Live Interview on Al Jazeera**.
Topic: On the 26th of March I gave a live interview at the "Newshour" show at Al Jazeera regarding the fact that UK government and secret services are asking encrypted messaging services such as WhatsApp to allow them access to users' data.
Link: `http://www.amichalas.com/blog/al-jazeera-interview-regarding-whatsapp-encryption/`

25/03/2017 **Interview on the Italian National Broadcasting company (RAI)**.
Topic: In the wake of the March (2017) attack at Westminster, I talked about terrorism and the importance of cyber security.
Link: `http://tinyurl.com/kyeg6tp`

Awards

2017 **Staff Appreciation Award**. Students voted me as one of the best staff members in the University for the academic year 2016/17.
Where: University of Westminster, Department of Computer Science

2014 **ERCIM Scholarship** for conducting postdoctoral research for 1 year.
Total grant: *33,600€*.

2011 **Best Paper Award** for the paper entitled "*Vulnerabilities of Decentralized Additive Reputation Systems Regarding the Privacy of Individual Votes*". In Mobisec, Aalborg, Denmark: 17 – 19 May 2011.

Technical Program Committee Membership

IEEE Transactions on Cloud Computing, IEEE Transactions on Knowledge and Data Engineering, Elsevier Ad Hoc Networks Journal, Elsevier Computers & Security Journal, Elsevier Journal of Computer and System Sciences, Springer Journal of Trust Management, Springer Journal of Wireless Networks, The Computer Journal – Oxford Journals, IEEE Conference on Communications & Electronics (ICCE), IEEE Conference on Advanced Technologies for Communications (ATC), IEEE Global Wireless Summit (GWS).

Miscellaneous

2015 – Current **Head of Cyber Security Group**, University of Westminster.
I am leading the Cyber Security (CSec) research group at the University of Westminster. The primary objective of the group is to bring together expertise in education, research and practice in the field of information security and cryptography. Group members conduct research in areas spanning from the theoretical foundations of cryptography to the design and implementation of leading edge efficient and secure communication protocols. As the head of CSec, I lead research projects focused on network security and cryptography. Within a year of establishing CSec, we have successfully obtained funding for two research projects (1 EU and 1 UK) that brought to the University approximately 1,000,000€.

2016 – Current **Course Leader**, University of Westminster.
Since September 2016 I am the course leader for the Cyber Security and Forensics MSc offered by the University of Westminster, Department of Computer Science.

2017 **BCS Accreditation**, University of Westminster.
I have successfully participated in the BCS accreditation for the Cyber Security and Forensics MSc offered by the University of Westminster, Department of Computer Science.

Programming skills

Advanced xhtml - html5, css, javascript, jquery, php, .net, c#, vb, java, mysql, sql server, cvs/subversion

Intermediate c, android development, oracle, XNA Framework

Languages

Greek **Mothertongue**

English **Cambridge FCE, TOEFL**

Spanish **Elementary**

Interests

- Traveling
- Literature
- Cinema
- Theater
- Music
- Photography
- Programming
- Technology
- Sports
- Cooking
- An active member of ARCHELON (Sea Turtle Protection Society of Greece). Worked as a volunteer in the European Union funded programme Life based in Lakonikos Bay – South Peloponnese