Konstantinos Rantos (MSc, PhD)

Personal Information

Address: P.O. Box 1103 N.Iraklitsa, N.Peramos, Kavala, Greece, 64007
Sex: Male
Date of birth: 21 March 1973
Nationality: Greek
Marital Status: Married (2 children)
Tel: +30 6947405223
E-mail: krantos@teiemt.gr
Blogs: e-sig.blogspot.com
Profile: http://lnkd.in/NetcCb

Education

1997 – 2001 Royal Holloway, University of London Egham, Surrey

PhD in Information Security

- Thesis: "Key Recovery in a Business Environment". The work was funded by the European Commission: Marie Curie Research and Training Grant.

1996 - 1997 Royal Holloway, University of London Egham, Surrey

MSc in Information Security

- Independent research project: "An approach to a key recovery agent and its communication with the authorities".

1990 - 1996 University of Patras Patras, Greece

Diploma in Computer Engineering and Informatics

- Dissertation: "Health Systems Security. Presentation and Comparison of Security Algorithms".

Relevant Experience and Scientific Interests

- Public-key infrastructures, key management
- e-id, e-Government services security
- Embedded systems security
- Network and telecommunications security
- Electronic payments systems
- Design of security protocols, security evaluation

Work Experience

Jun '10 – Today Eastern Macedonia and Thrace Institute of Technology, Kavala, Greece

Assistant Professor at the Department of Computer and Informatics Engineering

Apr '07 – Apr '10 Hellenic Ministry of Interior and e-Government Athens, Greece

Information Security Scientific Officer

Scientific expert on e-identification, digital signatures and e-procedures security. Contribution to several e-government projects including the design, deployment, and management of a PKI for the Hellenic Public Administration and mechanisms for the protection of e-government services across EU. National representation to EU technical groups.

Feb ’08 – Jun ‘08 University of Central Greece Lamia, Greece

Adjunct Lecturer

Responsible for teaching IT Security course at the Department of Informatics with Appliances in Biomedicine

June ’06 – Feb ‘07 Encode Middle East FZ-LLC Dubai, UAE

IT Security Consultant

Responsible and contributor to IT security related projects including PKI infrastructures, security awareness programs, secure coding practices and web applications security.

Feb 06 – June 06 Democritus University of Thrace Xanthi, Greece

Adjunct Lecturer

Responsible for teaching the course IT Security at the Department of Electrical and Computer Engineering.

Sep 04 – Jun 06 TEI Kavalas Kavala, Greece

Associate Professor

Responsible for teaching the courses: Computer Networks, Network Security, Cryptography, and Information Systems Security at the Industrial Informatics, and Information Management Departments of the Technological Educational Institute of Kavala.

May 03 – Aug 03 Encode S.A. Athens, Greece

IT Security Consultant

Responsible for the design, implementation, and documentation of a public key infrastructure compliant with ETSI TS 102 042 V1.1.1 for an Internet Banking application of a leading Greek Bank. Contribution to IT security related projects including secure coding practices and web applications security.

Jan 01 – May 03 Datacard Group London

IT Security Architect

Contribution to the design, implementation, testing, and debugging of certain areas of the Aptura project, a smart card operating system compliant with Java Card 2.1.1 and GlobalPlatform 2.0.1’ specifications (also compliant with ISO/IEC7816 and EMV Level 1). Primary responsibilities also involved the design of the security architecture for a CALC (Proton World) compliant card, specification of crypto test cases for the Aptura project, as well as contributions to evolving standards. Participation in Datacard’s proposal for an asymmetric authentication and key establishment protocol to be used by GlobalPlatform compliant cards. Contribution to the preparation of the Aptura project for Common Criteria evaluation. Investigation of certificate revocation techniques to be used by smart cards. Responsible for the implementation of Mastercard’s Mchip v4.0.

Sep 98 – Jan 01 Royal Holloway, University of London Egham, Surrey, UK

Research Assistant

The work was part of the project "Minimum interoperability specification for key escrow mechanisms" funded by the European Commission (TMR programme) aiming to define a minimum set of requirements for key recovery mechanisms to enable interoperability between dissimilar schemes.

Sep 97 – Jan 99 Royal Holloway, University of London Egham, Surrey, UK

Research Assistant

Contribution to ACTS project ASPeCT, an international collaborative project on security of third generation mobile communications. Among the objectives of ASPeCT were the migration of security features from existing mobile systems to UMTS and the investigation of the role of Trusted Third Parties (TTPs) for end-to-end security services in UMTS. Contributions included the design of the authentication and initialisation of payment protocol (between a user and a value-added service provider), the design of the TTP infrastructure, and the implementation of the system for demonstration purposes.

Publications

- K. Fysarakis, K. Rantos, Oth. Sultatos, Ch. Manifavas, I. Papaefstathiou. Policy-based Access Control for DPWS-enabled Ubiquitous Devices. In proceedings of: 19th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2014), Barcelona, Spain, September 2014.
- A. Papanikolaou, K. Rantos and I. Androulidakis. Proxied IBE-based Key Establishment for LLNs. In Proceedings of: The 10Th International Conference on Digital Technologies 2014, Zilina, Slovak Republic, July 2014.
- Ch. Manifavas, K. Fysarakis, K. Rantos, K. Kagiambakis, I. Papaefstathiou. Policy-based Access Control for Body Sensor Networks. In proceedings of: 8th Workshop in Information Security Theory & Practice (WISTP 2014), Heraklion, Crete, Greece, June 2014.
- Ch. Manifavas, K. Fysarakis, K. Rantos, G. Hatzivasilis. DSAPE – Dynamic Security Awareness Program Evaluation. Human Aspects of Information Security, Privacy and Trust (HCI International 2014), Heraklion, Crete, Greece, 2014.
- K. Fysarakis, G. Hatzivasilis, K. Rantos, A. Papanikolaou, and C. Manifavas. Embedded Systems Security Challenges. In Proceedings of "Measurable security for Embedded Computing and Communication Systems (MeSeCCS 2014)", within the International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS 2014), Lisbon, Portugal, 2014.
- Ch. Manifavas, G. Hatzivasilis, K. Fysarakis, K., and K. Rantos. Lightweight cryptography for embedded systems – A comparative analysis. In 6th International Workshop on Autonomous and Spontaneous Security (SETOP 2013), Egham, U.K, Springer-Verlag LNCS (8247), pp. 371–382.
- K. Rantos, Y. Katsikogiannis, A. Papadakis and A. Stasis. "Secure e-government services across EU", Int. J. Electronic Governance 6 (2), 117-132, 2013.
- K. Rantos and K. Markantonakis. "Analysis of Potential Vulnerabilities in Payment Terminals". In K. Markantonakis and K. Mayes (eds): Secure Smart Embedded Devices, Platforms and Applications, Springer New York, pp. 311-333.
- K. Rantos, A. Papanikolaou, C. Manifavas, and I. Papaefstathiou. IPv6 security for low

power and lossy networks. In Wireless Days 2013 (WD 2013), IFIP, vol., no., pp.1,8, 13-15 Nov. 2013, Valencia, Spain.

- K. Rantos, A. Papanikolaou, and C. Manifavas, “IPsec over IEEE 802.15.4 for low power and lossy networks,” in 11th ACM International Symposium on Mobility Management and Wireless Access (MobiWac), Barcelona, Spain, 3–8 November 2013, pp. 59–64.
- K. Rantos, K. Fysarakis and Charalampos Manifavas. How Effective Is Your Security Awareness Program? An Evaluation Methodology, Information Security Journal: A Global Perspective, 21:6, 328-345, 2012.
- K. Rantos, A. Papanikolaou, K. Fysarakis and Ch. Manifavas. Secure Policy-Based Management Solutions in Heterogeneous Embedded Systems Networks. Proceedings of IEEE International Conference on Telecommunications & Multimedia, TEMU 2012, Heraklion, Crete, 2012.
- K. Rantos. Digital Signatures: How close is Europe to truly interoperable solutions?, in B. De Decker, J. Lapon, V. Naessens, and A. Uhl (eds.): Proceedings of the *12th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security - CMS 2011, Ghent, Belgium, 2011*, Springer-Verlag (LNCS 7025), pp.155-162.
- K. Fysarakis, C. Manifavas, K. Rantos. Embedded Systems Security, Presented in the *10th International Symposium on Ambient Intelligence and Embedded Systems, AMIES 2011*, *Chania, Greece, 2011*, http://www.fh-kiel.de/amies-2011.
- A. Papadakis, K. Rantos, A. Stasis, "Promoting e-Gov Services: e-Document Interoperability across EU": Proceedings of the 15th Panhellenic Conference on Informatics, Kastoria, Greece, 2011, pp.304-308.
- A. Papadakis, K. Rantos, A. Stasis. The Realization of the Greek E-GIF, *Official Proceedings of the Second European Summit on Interoperability in the iGovernment, Rome 2008*, www.esiig2.it.
- K. Rantos. Limitations Regarding Certificate Handling on Smart Cards, in: P. Bozanis and E. Houstis (eds.): Proceedings of *the 10th Panhellenic Conference in Informatics (PCI 2005)*, Volos, Greece, November 2005, pp. 77-87.
- K. Rantos and C.J. Mitchell. Matching key recovery mechanisms to business requirements. *Computers & Security* (2005) 24 (3), 232-245.
- K. Rantos and K. Markantonakis. An asymmetric cryptography secure channel protocol for smart cards, in: Yves Deswarte, Frédéric Cuppens, Sushil Jajodia, Lingyu Wang (eds.): Security and Protection in Information Processing Systems, IFIP 18th WorldComputer Congress, TC11 19th International Information Security Conference, August 2004, Toulouse, France. Kluwer 2004, pp. 351–366.
- K.Rantos and C.J. Mitchell. Key recovery scheme interoperability - a protocol for mechanism negotiation, in: B. Honary (ed.), Cryptography and Coding - Proceedings of the 8th IMA International Conference, Cirencester, UK, December 2001, Springer-Verlag (LNCS 2260), Berlin (2001), pp.268-276.
- K.Rantos and C.J.Mitchell. Key recovery for archived data using smart cards. In *Proceedings of the 5th Nordic Workshop on Secure IT Systems* (*NORDSEC 2000*), Reykjavik, Iceland, October 2000.
- C.J. Mitchell and K. Rantos. A fair certification protocol. *ACM Computer Communication Review*, 29 no. 3 (July 1999) 47-49.
- K. Rantos and C.J. Mitchell. Remarks on KRA's key recovery block format. *Electronics*

Letters, 35 (1999) 632-634.

- C. Markantonakis and K. Rantos. On the life cycle of the certification authority key pair in EMV 96. In *Proceedings of Euromedia '99*, Munich, Germany, April 1999.
- K.Rantos and C.J. Mitchell. Key Recovery in ASPeCT Authentication and Initialisation of Payment Protocol. In *Proceedings of the 4th ACTS Mobile Communications Summit*, Sorrento, Italy, June 1999.
- B. Preneel, K.M. Martin, G. Horn, P. Howard, C.J. Mitchell, and K. Rantos. Trialling secure billing with Trusted Third Party support for UMTS applications. In *Proceedings of the Third ACTS Mobile Communications Summit*, Rhodes, Greece, June 1998.

Projects contribution

- Member of the Advisory Board for the project ADVISE (Advanced Video Surveillance archives search engine for security applications), 2014.
- "PIN Processing Options" for the UK Cards Association, 2014.
- "Open courses" for the Eastern Macedonia and Thrace Institute of Technology, 2014.
- "nshield: new embedded Systems arcHItecturE for multi-Layer Dependable solutions", ARTEMIS Joint undertaking, 2011.
- Design, deployment and management of Hellenic Public Administration's PKI, 2009.
- Greek eGovernment Interoperability Framework, http://www.e-gif.gov.gr, 2009.
- Large scale pilot projects SPOCS (Simple Procedures Online for Cross-border Services - www.eu-spocs.eu), 2009.
- eGovernment Forum project: Transparency, Accountability, Inclusiveness, http://www.e-governmentforum.gr, 2008.
- Responsible for the design of a PKI for the Hellenic Bank Association, 2008.
- Preparation and development of eGovernment Services and Information Security related training material for the Hellenic National Centre for Public Administration & Local Government, 2008.
- "Deployment of a PKI and an e-id scheme for the needs of the Hellenic Public Services Portal, ermis.gov.gr", 2008.
- "Design of a PKI for a security IT infrastructure", for a leading bank in the Middle East, 2006.
- "Design and delivery of a security awareness program", for Saudi Aramco, 2007.
- "Delivering a security awareness program", for Saudi Telecomms, 2006.
- "Best Practices for Key Management on Smart Cards", for Codes&Ciphers, UK, 2006.
- "PKI Design & Implementation", for Eurobank-Greece, 2003.
- "Best practices for developing secure applications", for a major foreign bank, 2003.
- "Guidelines for compiling a Service Level Agreement", for a major foreign bank, 2003.
- EU ACTS project ASPeCT: Advanced Security for Personal Communications Technologies, 1998.

Other Professional activities

- National representative to EU technical group for digital signatures and e-procedures.
- Consultant on e-identification and digital signatures for the Greek Ministry of Interior and Administrative Reconstruction.
- Teaching in training courses organized by the Hellenic National Centre for Public Administration & Local Government.

- Participation in management, evaluation and implementation of EU co-funded IT related projects: Digital Acropolis museum (2014), Greek government portal ERMIS (2010), ICT infrastructures Assessment Laboratory (2008), Greek e-government interoperability framework (2007).
- Member of Conferences Program Committee:
  - IADIS International Conference: Information Systems 2014, Spain 2014.
  - 4th International Conference on Pervasive and Embedded Computing and Communication Systems, PECCS 2014, Portugal.
  - IADIS International Conference: Information Systems 2013, Portugal 2013.
  - Workshop in Information Security Theory and Practices 2010: *Security and Privacy of Pervasive Systems and Smart Devices*, Passau, Germany, 2010.
  - Workshop in Information Security Theory and Practices 2009: *Smart Devices, Pervasive Systems, Ubiquitous Networks*, Brussels, Belgium, 2009.
  - Workshop in Information Security Theory and Practices 2008: *Smart Devices, Convergence and Next Generation Networks*, Sevilla, Spain, 2008.
  - Workshop in Information Security Theory and Practices 2007: *Smart Cards, Mobile and Ubiquitous Computing Systems*, Heraklion, Crete, May 2007.
- Reviewer of Journals:
  - Computers & Security (Elsevier)
  - Journal of Systems and Software (Elsevier)
  - Computer Networks (Elsevier)
  - Information Sciences (Elsevier)
  - Journal of Computer Science and Technology (Springer)
  - Security and Communication Networks (Wiley)
  - SpringerPlus
- Invited Speaker
  - Polis, Infosystem 2009, Thessaloniki
  - 4th Regional Electronic Security Forum, Telecommunications Networks & Systems Security November 2008,Thessaloniki
  - Information Security Matrix Forum 2007, Athens, Greece
  - Information Security Matrix Forum 2005, Athens, Greece

Other Personal Skills

Languages: Greek (Mother Tongue)

English (Proficient user)

Communication Skills: Good communication skills gained through my experience at various positions.

Driving License: Clean Category B