Editorial

Elias Pimenidis*

School of Architecture, Computing and Engineering,
University of East London,
4-6 University Way, E16 2RD, London, UK
E-mail: E.Pimenidis@uel.ac.uk
*Corresponding author

Christos K. Georgiadis

Department of Applied Informatics,
University of Macedonia,
156 Egnatia Str., GR 54006, Thessaloniki, Greece
E-mail: geor@uom.gr

Biographical notes: Elias Pimenidis has worked in manufacturing for more than ten years before moving to academia and completing a PhD at the University of Abertay Dundee in the UK. He is a CITP member of the British Computer Society and a Senior Lecturer at the University of East London. His research focuses on risk in developing web-based applications in the area of e-business and e-government, while his most recent endeavours concern the security of web services and its impact on their interoperability. Other work in the area of security includes digital identification and its interoperability across Europe.

Christos K. Georgiadis received his BSc in Mathematics and his PhD in Information Systems Security – 'Access control for web data bases' from the Aristotle University of Thessaloniki, Greece. His research interests include the areas of e-commerce and m-commerce technologies, e-security, and web services supporting technologies. He is a professional member of ACM, and the SIGEcom. He is Assistant Professor at the Department of Applied Informatics of the University of Macedonia in Greece.

The volume of data, information and knowledge that is processed and traded across computer networks throughout the world is continuously increasing in unprecedented rates. At the same time the demands for quality of services offered on the basis of such transactions are becoming increasingly high. Secure transactions, supported by safe (physically and digitally) systems and sustainable services, are therefore the expected norm in the information services world. As a result over the past decade there has been considerable emphasis on research addressing issues related to the above key requirements in information service provision and the work presented in this issue reflects this trend. Despite the valiant efforts of a large number of researchers and the excellent outputs produced, security breaches continue to occur at alarming levels, risk levels are still running high and there are considerable percentages of information systems users that appear confused and insecure in exchanging information online.

The papers comprising this special issue of the *International Journal of Electronic Security and Digital Forensics* are extended versions of papers that were originally presented at the 7th International Conference in Global Security, Safety and Sustainability, that was held at Thessaloniki, Greece, in August 2011. The original papers have been revised, extended and enhanced to reflect current developments in the area of information systems security, to reflect more recent results of the authors work and to consider new challenges as they emerge in the very agile and volatile world of information systems security. The variety of topics and the currency of the research will make this a very interesting and challenging issue for the journal's readership.

More specifically, Gonzalez Granadillo, Ben Mustapha, Hachem and Debar discuss the management of security events. Considering the heterogeneous nature of network systems and networked devices, they propose an ontology-driven approach at managing risks that might affect the administrative tasks of security event due to different characteristics and functionalities of systems.

Ntouskas, Papanikas and Polemi address the concerns over information security risks in small, medium and micro enterprises (SMEs, mEs) in the European digital economy. Such companies, despite being the backbone of their industries, have been identified as one of the weakest links in information security. The authors use a parameterised open source collaborative environment called 'STORM' to address security weaknesses and needs, resulting in implementing trusted services for SMEs/mEs and allowing them to self-manage the security of their information and telecommunication (IT) systems.

Mavridou, Zhou, Dawkins and Papa discuss security, access control and risk mitigation in the smart-grid and their importance to critical infrastructure. The focus of their work is on addressing concerns relating to the security risks posed by dated SCADA protocols used for communications and the systems that implement those protocols supporting the electric power grid communications. They propose a comprehensive framework that provides situational awareness (SA) for SCADA devices and their operations in a smart-grid environment. Situational awareness is achieved by processing information collected by monitoring sensors and understanding threats that may affect operations. The proposed framework employs a threat modelling methodology to support this mission.

Karayianni, Katos and Georgiadis delve into the word of computer forensics and challenge the widely accepted approach where a first responder does not capture the RAM of a computer system if found to be powered off at a crime scene. Their work explores the presence of confidential data in RAM such as user passwords. They conclude that if a computer is switched off but not yet removed from the mains, the data are preserved and therefore capturing the memory could be as critical on a switched off system as on a running one. They proceed by proposing a framework for password recovery from volatile memory.

Tsiakis, Katsaros and Gritzalis address the ever evolving and increasing nuisance of spam over internet telephony (SPIT) that has over the past few years developed into a serious threat with adverse impact and costs for the economy. They introduce an audio completely automated public Turing test to tell computers and human apart (CAPTCHA) as a means of distinguishing automated software agents (bots) from humans. They lay the principles for an adequate understanding of the SPAM-related economic models, as well as their analogies to the SPIT phenomenon, so as to weigh the benefits of audio CAPTCHA protection against the incurred costs. Their approach is based on the

economic assessment of externalities, i.e., the economic impact associated with the SPIT side effects on everyday life.

Addressing a different type of authentication problem, Tait tests the ability of a computing system, robot, or any man made system to recognise human commands and understand their instructions. This work considers a novel approach of improving the current voice recognition and authentication efforts of existing software systems. It does not replace or make any current efforts obsolete. Instead research by Fletcher-Munson on equal loudness is integrated into a new algorithm which is used as a 'plug in', and implemented as a middle tier software algorithm. The author has found that the application of this algorithm reduced the false acceptance rate and false rejection rate of tested voice authentication systems.

Sá, Borges, Magalhães and Dinis Santos, focus more on the social impacts of security systems and explore the issues surrounding the use of biometric technologies in security systems as perceived by the Portuguese society. This is a key topic that could affect the way security is applied across the globe, pending its acceptance by different societies, based on notion of safety it instils versus any drawbacks that the exposure to technology might raise.

Damasceno, Teixiera and Campos explore the use of computer-based technology in support of physical safety to people. Their proposed model uses data mining to predict criminal levels in geographic areas. The model specifically addresses socio-economic crimes and the authors expect to validate a unified process for building systems which can help decision managers to fight and prevent crimes of this nature.

The guest editors would like to take the opportunity to thank Professor Hamid Jahankhani, Editor-in-Chief of the journal for offering them the opportunity to compile and edit this special issue.

We hope that the readership of this journal will find the contents of this issue interesting, challenging and of real added value to their work, studies and research activities.