Editorial

Alexander B. Sideridis

Informatics Laboratory,
Agricultural University of Athens,
Athens 118 55, Greece
E-mail: as@aua.gr

Elias Pimenidis

School of Computing, IT and Engineering,
University of East London, University Way,
London, E16 2RD, UK
E-mail: e.pimenidis@uel.ac.uk

Biographical notes: A.B. Sideridis is Professor in Computer Science and Head of the Informatics Laboratory of the Agricultural University of Athens. He earned his first degree at the University of Athens and his MSc and PhD from Brunel University. He has been the project leader of more than 30 successful national and international projects and has published more than 180 scientific papers in management and decision support systems, computer networking related to local and central administration activities, advanced computational numerical modelling, informatics and impact of computers in society and agricultural informatics.

Elias Pimenidis is a Senior Lecturer at the University of East London in the UK. The core of his research work focuses on e-business and e-government development projects. His interest in security issues is on online transactions and e-services and in particular, on the effect, these could have on e-government implementations. Other research interests include the evaluation of web services, knowledge management systems and the use of computer games for educational purposes. He is also a Visiting Lecturer at the Informatics laboratory of the Agricultural University of Athens, Greece.

Mobile devices in the forms of phones and PDAs have become part of everyday life even in the remotest ends of the planet. In fact in some remote areas mobile devices are the only way of communicating with the world beyond the local vicinity. Services built to exploit the enhanced capabilities of such devices offer their users the opportunity to store and share information (often personal and sensitive) through a variety of formats (text, picture, video, HTML, etc.). Such use raises concerns for the safety of the contents of mobile devices and the security of transactions performed using mobile devices. These concerns are becoming more critical as services accessed through such devices include those of e-government and the capabilities. With the above in mind the Hellenic Scientific Council for the Information Society had organised an one day conference on "Mobile Devices: Technological and Legal Issues", on the 28th of March 2008.

A number of high profile academics and professionals took the podium in presenting their views and research findings and the conference had ended with a very informative and mind challenging round table discussion. The highlights of that conference focusing on security and trust issues have been updated with more recent developments and findings and are presented in this special issue of the *International Journal of Electronic Security and Digital Forensics*. The issue comprises seven papers which cover a wide range of topics from trust in the use of mobile devices to secure networks for mobile services and the more societal considerations of the use of mobile devices as a means of bridging the digital divide. More specifically:

Karantjias and Polemi, present a secure, interoperable e/m-government framework in which a synchronous prototype platform operates, enabling Governmental Organisations to make the next step on digital society. The proposed e/m framework addresses core e/m-government requirements of security, interoperability, transparency, scalability and high administration in the communications with their citizens, businesses and other similar organisations.

Anagnostou and Lamprou, debate the issue and the challenges posed by the need to balance ambient intelligence, alias pervasive computing vs. privacy. Ambient intelligence is based on large-scale information exchange to provide a convenient environment to humans, while privacy is usually based on restricting information.

The authors query whether there is a convenient equilibrium point, which will satisfy both needs for ambient intelligence services and privacy?

Patrikakis, Kyriazanos, Voulodimos and Nikolakopoulos, write about the inherent risk of user interaction and communication in a peer to peer fashion and the need for protection against security threats and the corresponding need for trust establishment schemes. They discuss concept of Personal Network Federation concluding to the need for privacy protection as this appears as the counterforce for complete release of personal information in order to support true personalised service provision.

Zorkadis and Karras, discuss how the evolution of web 2.0 leads to an exponential increase of Mobile Services creation and Distribution Management Systems (MSDMS) and the challenges in collecting and processing personal data this leads to. They offer privacy-related requirements to support designing privacy-friendly mobile services distribution management schemes, especially in the case of collaborative mobile services. They also propose a privacy-enhancing MSDMS model, integrating anonymous transactions and other privacy-friendly operation-related components.

Jahankhani, presents a technical overview and in-depth analysis of the capabilities of state-of-the-art digital forensics tools. These tools are used to extract valuable evidence from smart phones and other mobile devices in the ongoing battle of law enforcement agencies against organised crime.

Ntaliani, Costopoulou, Manouselis and Karetsos, propose a framework that serves public agencies in identifying potential mG2B services; as well as a set of technical solutions for the secure provision of them. In addition they discuss the design of a web-based observatory that can help rural SMEs in finding accurate and updated information for the provided m-government services in a secure and trusted environment.

Pimenidis, Sideridis and Antonopoulou, present and discuss the use of mobile devices in applications in areas strongly affected by the digital divide. They assess the potential of mobile devices and the even growing of types of services that evolve around their use in effectively tackling the digital divide, while maintaining a secure and trusted

environment that casual and often poorly educated users and be drawn into and feel secure in.

The guest editors would like to take the opportunity to thank Dr. Hamid Jahankhani, Editor in Chief of the journal for offering them the opportunity to compile and edit this special issue that also promotes the work of the HSCIS.

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.