Introduction

Sokratis Katsikas

Systems Security Laboratory,
Department of Digital Systems,
School of Information & Communication Technologies,
University of Piraeus,
150 Androutsou St. Piraeus 18532, Greece
Email: ska@unipi.gr

and

Center for Cyber and Information Security,
Norwegian University of Science and Technology,
P.O. Box 191, Gjøvik N-2802, Norway
Email: sokratis.katsikas@ntnu.no

Vasilios Zorkadis

Hellenic Data Protection Authority,
Kifissias 1-3, Athens 11523, Greece
Email: zorkadis@dpa.gr

Biographical notes: Sokratis Katsikas is a Professor with the Center for Cyber and Information Security, Norwegian University of Science and Technology, Norway, and Professor of the Department of Digital Systems of the University of Piraeus, Greece. His research interests lie in the areas of information and communication systems security and of estimation theory and its applications. He has authored or co-authored more than 260 journal publications, book chapters and conference proceedings publications and he has participated in more than 60 funded national and international R&D projects in these areas. He is serving on the editorial board of several scientific journals, he has authored/edited 33 books and has served on/chaired the technical programme committee of more than 500 international scientific conferences.

Vasilios Zorkadis has been working as the Secretariat's Director of the Hellenic Data Protection Authority since 2004. He received a Diploma in Electrical Engineering from Aristotle University of Thessaloniki, Greece and holds a PhD on Computer Network Security from University of Karlsruhe, Germany. He is author of books on 'Cryptography', and 'Information Theory' and author or co-author of more than 60 journal and conference papers on security and privacy protection. He taught for almost 20 years in Greek universities courses on information theory, information security, cryptography, computer networks and digital communications. He is a founding member and the current president of the "Hellenic Council for the Information Society".

Information and communication technologies move fast; faster than society, faster than governments, faster than the law. Connectivity is already impressive, but the near future brings about the interconnection of everything, via the Internet of Things. It also brings fundamental changes to our computing paradigm, with cloud computing gaining momentum and being expected to become the prevalent computing paradigm in the years to come. Increasingly more data are being collected, about almost everything one can imagine; and they remain there, in cyberspace, forever, sometimes even resisting efforts to delete them. These data are so attractive that a new science, going by the name ‘big data’ has already emerged. All these developments constitute in most cases an improvement in our everyday lives, but sometimes infringe our rights as citizens. The challenge, therefore, is to safeguard citizen rights in the face of a new era, landmarked by new computing paradigms.

This special issue contains extended and expanded versions of selected papers that were presented in the 6th occasion of the *International Conference on e-Democracy* that was held in Athens, the cradle of democracy, on 10–11 December, 2015.

The first paper of the special issue, entitled ‘Democracy in the digital age: digital agora or dystopia’, by Parycek et al., addresses the effects of increased digitalisation with a particular view to the effects of ICTs (information and communication technologies) on democracy and the rule of law. Drawing on a legal review, case studies and quantitative survey data about citizens’ view on transparency and participation opportunities in the German-speaking region, the paper summarises the relevant discourses of democratisation via ICTs, and the dominant criticism for the selected areas. The paper concludes with an outlook on contemporary questions of digital democracy between protecting citizens’ rights and citizen control.

The next five papers of the special issue address e-government services and tools. The first among those, entitled ‘Investigating the mobile side of e-participation’, by Ntaliani et al. addresses electronic participation through mobile services. Acknowledging the fact that local governments have not reached a clear strategy on how to design successful mobile services for participation, this study proposes a way for exploiting mobile participation in municipal governments. It presents e-participation and m-participation progress in 325 Greek municipal governments and proposes a framework for introducing efficient and effective mobile participation applications so as to make local societies more inclusive.

In the same cluster, the paper entitled ‘E-voting vs. e-trust: a test bed for e-democracy in a world in crisis?’, by Shat and Pimenidis addresses the question whether the maturity of e-voting technologies and their rigorous testing suffice to inspire people to trust e-voting systems and to participate in e-voting; particularly in areas where the political climate might be volatile and trust is a rare commodity. The authors present the outcome of a survey among the Palestinian diaspora to gauge their trust and willingness to use e-voting systems in the Palestinian Authority’s elections.

Sideridis et al., inspired by the major crisis created due to the mass movement of hundreds of thousands of Syrian and Iraqi refugees across Europe, in their paper entitled ‘Smart cross-border e-Gov systems: an application to refugee mobility’, present an implementation of a Smart Cross-Border e-Government System for supporting the management of individuals and their movement in order to address this crisis.

The paper entitled 'TRILLION project approach on scenarios definition for citizen security services', by Patrikakis et al. proposes a methodology towards a comprehensive definition of use cases, accounting for all aspects, such as technical, social, organisational and regulatory, related to the design and development of a platform being developed within the TRILLION project to foster effective collaboration of citizens and law enforcement officers. A particular use case from the project is used in order to demonstrate the application of the proposed methodology.

The last paper in this cluster, entitled 'Advanced process simulation tool for improving the quality of decision-making in local government of the Czech Republic', by Molhanec and Merunka, addresses the problem of low participation of residents of small settlements in the territorial planning processes. Low participation causes dissatisfaction with democracy in local government and decreases the quality of life. The paper presents a solution, which consists of the use of computer simulation tools to increase the level of knowledge of the persons concerned, which results in greater participation. This hypothesis was confirmed experimentally by the authors' project in settlements of Central Bohemia.

E-government services need to be evaluated with respect to their effectiveness and efficiency in achieving their intended objectives. The paper entitled 'An evaluation scheme for local e-government and local e-democracy: the case of Greek municipalities', by Lappas et al. presents a citizen-centric framework for the evaluation of local e-government projects and its validation in the context of Greek municipalities. The proposed model incorporates the different aspects of e-government as well as e-democracy. To develop and validate the model two studies were conducted: one survey that captured citizens' opinions about the important e-government features and a website analysis to check the level of e-government sophistication of Greek local government websites.

Next, two papers addressing privacy issues in online social networking follow. In the first, entitled 'Privacy protection of tagged multimedia content in online social networks', by Michota and Katsikas, the authors investigate the privacy implications of unauthorised audience discrepancies in tagged multimedia content that are due to the different privacy restrictions that users apply to their personal identifiable information (PII). By examining all the possible visibility combinations in a two-level social relationship scale for different anonymised real user profiles, according to the offered choices that are provided by the privacy mechanisms in OSNs, the cases where there exist audience discrepancies that can cause privacy breaches have been identified. Their findings indicate that the current privacy mechanisms of OSN users' tagged multimedia content are insufficient, as they cannot fully match the users' privacy intentions.

The second paper in the cluster, entitled 'Sharing secrets, revealing thoughts and feelings: perceptions about disclosure practices and anonymity in a FB university students' community', by Sideri et al., identifies students' perceptions about personal information disclosure and anonymity in a specific Facebook University Community, by means of an online survey. The explicit goal of this Community is the sharing of secrets and the revelation of students' deepest thoughts and feelings on high sensitive issues like their erotic or sexual life, leading to information disclosures in various ways. Anonymity as expected is valued positively while privacy violations seem to bother.

The last paper of the special issue, entitled 'Security policy rules and required procedures for two crucial cloud computing threats' by Georgiou and Lambrinoudakis, turns our attention to security issues associated with the new cloud computing paradigm. In this paper two crucial security threats of cloud computing systems are presented and are classified in four categories – gates of a proposed Security Policy. Moreover, security metrics that providers could use to evaluate the security of their services are proposed. Finally, the necessary policy rules and required procedures are described.