Guest Editorial

Konstantinos Papapanagiotou

Open Web Application Security Project (OWASP),
Athens, 15232, Greece
E-mail: konstantinos@owasp.org

Vasileios Vlachos

Department of Computer Science and Telecommunications,
School of Technological Applications,
Technological Educational Institution (TEI) of Larissa, 41110, Greece
E-mail: vsvlachos@owasp.gr

Biographical notes: Konstantinos Papapanagiotou has more than 10 years of experience in the field of Information Security both as a corporate consultant and as a researcher. Currently he is leading the information security services practice at OTE, the largest telco in Greece. He has been involved with OWASP for several years now, leading the OWASP Greek Chapter and lately the Hackademic Challenges Project. He holds a BSc and PhD from the University of Athens and an MSc in Information Security from Royal Holloway, University of London.

Vasileios Vlachos is a Lecturer at the Department of Computer Science and Engineering of the Technological Educational Institute (TEI) of Thessaly. He holds a Diploma of Engineering in Electronic & Computer Engineering from Technical University of Crete, a MSc in Integrated Hardware and Software Systems from the Department of Computer Engineering and Informatics of the University of Patras and a PhD in Information Systems Security from the Department of Management Science and Technology of the Athens University of Economics and Business.

Every developed country has built advanced digital infrastructure that takes advantage of Information and Communication Technologies to offer digital services to its citizens. At the same time modern economies are based on the advances of technology to gain the essential competitive advantage in knowledge-based services. A possible failure of telecommunication systems or critical IT infrastructure could lead into severe consequences on a nation-wide level. These could include financial damage due to attacks to the banking system, or even human casualties if a targeted attack aimed at Supervisory Control and Data Acquisition (SCADA) systems or even electronic medical equipment and hospitals.

Most governments have identified the size and importance of the problem and have tried to respond in various ways. In most cases an immediate reaction involves the creation of military units or security teams, in charge of protecting critical infrastructure and responding to espionage-related incidents of military, political or industrial nature.

USA considers cyberspace as the fifth domain of warfare in addition to land, sea, air and space, in which they need to ensure their dominance. For this reason, they have created the United States Cyber Command (USCYBERCOM).

At the same time, NATO (The Tallinn manual – NATO Cooperative Cyber Defence Centre of Excellence), examines the legal framework related to responding to cyber-attacks, that may be initiated even by cyber-activists, by using not just legal measures but also active countermeasures. The massive amount of legal aspects and opinions involved in this process is indicative of the difficulty that is associated with handling such incidents.

Various researchers and political analysts advocate that the use of cyber-attacks as a weapon may pose consequences that can be compared with those related with the use of nuclear weapons. Such comparison may be misleading as cyber-attacks can be committed not only by organised military groups but also by other entities, such as individual hackers or hacktivists and cyber-criminals. Similarly, the motives of such attacks are quite different from those related with financial fraud or industrial espionage and critical information theft.

Owing to their organisation and infrastructure, military units can apply strict and effective security policies on their networks. Likewise, the private sector has the required human and technological resources to implement efficient defensive mechanisms that will harden its IT infrastructure.

Conversely, on a global scale, the economic crisis has lead a lot of countries to minimise costs. As a result, most public services do not have the means to respond to the most complex attacks, which puts citizens' personal information at risk. Very few countries have a holistic framework that protects public sector. Such limitations have led in delays to introduce e-government services as most citizens do not feel safe enough to use modern practices that are related to the use of Information and Telecommunication Technologies.

The main purpose of this special issue is to highlight the gaps that are identified in the field of security in e-government services and the efforts for improvement that is derived from recent scientific research, which focuses on improving the security and resilience of the services offered by a government.

The remediation of such issues cannot come about on a global scale at once. On the contrary, a step-by-step approach which gradually provides solutions to open issues based on scientific evidence produced by years of research performed by experts in the field seems more appropriate.

In the first paper of this special issue, P. Drogkaris, S. Gritzalis and C. Lambrinoudakis examine ways to lay down citizens' worries for the usage of their personal data from state agencies. In their paper 'Employing privacy policies and preferences in modern e-government environments', they present a methodology and an XML schema offering a variety of electronic services to the citizens and at the same time safeguarding their privacy.

In their paper titled 'Secure e-government services across EU' K. Rantos, Y. Katsikogiannis, A. Papadakis and A. Stasis analyse European initiatives and working frameworks that are promoted to EU members to offer unified e-services to citizens. The authors focus on the design and technical requirements that such a platform should set to enforce the basic principles of security and at the same time maintain its usability to efficiently support the required electronic services and transactions. They focus on e-signatures as a means to safely exchange electronic documents.

A.W. Akotam, M.S. Kontoh and A.K. Ansah approach this subject by using public key cryptography in the form of public key infrastructure (PKI) and the use of X.509 digital certificates. In their paper titled 'E-governance public key infrastructure (PKI) model', they present an architecture based on public key cryptography that can be used efficiently to offer electronic services to citizens. Their suggestions form a comprehensive framework of scientific advances that could be immediately put into practice to safeguard citizens' privacy and personal data.

The aforementioned are complemented by E. Wihlborg's paper titled 'Secure electronic identification (eID) in the intersection of politics and technology', where she discusses the introduction of an electronic ID system, as it was implemented in Sweden. The political implications of such a project are very important as are the technical challenges that have to be overcome for a successful implementation. In any case, the most important aspect is the participation and engagement of citizens in e-government through the use of Information and Communication Technologies. The collaboration between government and citizens in e-government processes and most importantly in e-consultation heavily depends on the security and privacy that these services offer to their users.

The effects of privacy and security are also discussed in the paper titled 'Are security and privacy equally important in influencing citizens to use e-consultation?' by L. Enggong and B. Whitworth.

The establishment of e-government and its vast adoption from the public, effectively leading to taking advantage of what Information and Communication Technologies can offer, heavily depends on safeguarding users' personal data and privacy. In this special issue, mature scientific tools and methodologies that can significantly contribute towards the transformation of existing public and state services to e-services are presented.