

A Framework for Protecting Voters' Privacy In Electronic Voting Procedures

C. Manolopoulos, Computer Technology Institute and Press "DIOPHANTUS", University of Patras, Patras, Greece

D. Sofotassios, Computer Technology Institute and Press "DIOPHANTUS", University of Patras, Patras, Greece

P. Spirakis, Computer Technology Institute and Press "DIOPHANTUS", Computer Engineering and Informatics Department, University of Patras, Patras, Greece

Y.C. Stamatiou, Computer Technology Institute and Press "DIOPHANTUS", Business Administration Department, University of Patras, Patras, Greece

EXECUTIVE SUMMARY

eVoting is considered to be one of the most challenging domains of modern eGovernment and one of the main vehicles for increasing eParticipation among citizens. One of the main obstacles for its wide adoption is the reluctance of citizens to participate in electronic voting procedures. This reluctance can be partially attributed to the low penetration of technology among citizens. However, the main reason behind this reluctance is the lack of trust which stems from the belief of citizens that systems implementing an eVoting process will violate their privacy. The departure point of this approach is that the emergence of such a belief can be considerably facilitated by designing and building systems in a way that evidence about the system's properties is produced during the design process. In this way, the designers can demonstrate the respect in privacy using this evidence that can be understood and checked by the specialist and the informed layman. These tools and models should provide sufficient evidence that the target system handles privacy concerns and requirements that can remove enough of the fears towards eVoting. This paper presents the efforts of the authors' organization, the Computer Technology Institute and Press "Diophantus" (CTI), towards the design and implementation of an eVoting system, called PNYKA, with demonstrable security properties. This system was based on a trust-centered engineering approach for building general security critical systems. The authors' approach is pragmatic rather than theoretical in that it sidesteps the controversy that besets the nature of trust in information systems and starts with a working definition of trust as people's positive attitude towards a system that transparently and demonstrably performs its operations, respecting their privacy. The authors also discuss the social side of eVoting, i.e. how one can help boost its acceptance by large social groups targeting the whole population of the country. The authors view eVoting as an innovation that must be diffused to a population and then employ a theoretical model that studies diffusion of innovation in social network, delineating structural properties of the network that help diffuse the innovation fast. Furthermore, the authors explain how CTI's current situation empowers CTI to realize its vision to implement a privacy preserving, discussion and public consultation forum in Greece. This forum will link, together, all Greek educational institutes in order to provide a privacy preserving discussion and opinion gathering tool useful in decision making within the Greek educational system.

Keywords: Cryptographic Protocol, eVoting, Privacy, Risk Assessment, Security Architecture, Trust

DOI: 10.4018/jcit.2013040101

1. ORGANIZATION BACKGROUND

The Computer Technology Institute and Press “Diophantus” is a research and technology organization focusing on research and development in Information and Communication Technologies (ICT). Particular emphasis is placed on education, by developing and deploying conventional and digital media in education and lifelong learning; publishing printed and electronic educational materials; administrating and managing the Greek School Network; and supporting the organization and operation of the electronic infrastructure of the Greek Ministry of Education, Lifelong Learning and Religious Affairs and all educational units. Since its establishment in 1985, and in the past decades of rapid technological development, CTI has actively contributed to many of the advances that today are taken for granted.

The *Information Society Sectors* are the organization’s conveying mechanisms of know-how, in turn supporting the Hellenic State’s devolvement into the Information Society. The Sectors, which are currently the following, are coordinated by the Board of Executives:

- Educational Technology Sector;
- Networking Technologies Sector;
- E-Government Sector;
- Center of Telematics & Applications for regional development;
- Further Education & Training Sector;
- Strategic & Development Policy Sector;
- Computing & Networking Systems Security Sector.

The work that resulted in the PNYKA system was done in collaboration between CTI and *EXPERTNET Advanced Applications S.A.* The work was partially supported by the General Secretariat of Research and Technology of Greece, under the project PNYKA (project code DEL_2, decision 8948/04.05.06, project

site <http://pnyka.cti.gr/>), Operational Program of Western Greece, 3rd Community Support Framework.

With respect to the acceptance of the projects’ results, on June 13th 2008, CTI submitted the PNYKA system at the “eVoting Competition 2008” organized by the Competence Center for Electronic Voting and Participation sponsored by Internet Foundation Austria (IFA). The Competition targeted non-commercial, internet eVoting systems fully developed using open source tools and takes place for the first time in Europe. The PNYKA system was awarded the first prize from among numerous submissions from all over Europe.

2. SETTING THE STAGE

During the last decades, we have witnessed a rapid growth of Information and Communication Technologies (ICTs) as well as the diffusion of Internet in people’s lives. These facts, in conjunction with the need for more efficient and economical government services have led to an increase of eGovernment services in many countries. In this context, democratic societies face the challenge to improve public participation in political debate and policy formation processes, realizing the concept of *eParticipation*. One of the most important and critical facets of eParticipation is *Electronic Voting* or eVoting. eVoting has attracted lately the attention of many governments as an alternative to conventional voting with the hope to increase citizens’ participation and reduce the costs.

While eParticipation initiatives have been deployed across the EU with mixed results so far, some encouraging signs come from few but important eVoting initiatives (see, also, Susa & Grönlund, 2012, for an interesting recent effort to systematize the study of the eParticipation domain as well as Sæbø et al. (2008), who attempt to provide a formal model for defining and studying eParticipation). In Switzerland, eVoting and especially Internet voting, was

31 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/framework-protecting-voters-privacy-electronic/88124

Related Content

Discovering an Effective Measure in Data Mining

Takao Ito (2009). *Encyclopedia of Data Warehousing and Mining, Second Edition* (pp. 654-662).

www.irma-international.org/chapter/discovering-effective-measure-data-mining/10890

Online Analytical Processing Systems

Rebecca Boon-Noi Tan (2009). *Encyclopedia of Data Warehousing and Mining, Second Edition* (pp. 1447-1455).

www.irma-international.org/chapter/online-analytical-processing-systems/11011

Evaluation of Decision Rules by Qualities for Decision-Making Systems

Ivan Bruha (2009). *Encyclopedia of Data Warehousing and Mining, Second Edition* (pp. 795-801).

www.irma-international.org/chapter/evaluation-decision-rules-qualities-decision/10911

Storage Systems for Data Warehousing

Alexander Thomasian (2009). *Encyclopedia of Data Warehousing and Mining, Second Edition* (pp. 1859-1864).

www.irma-international.org/chapter/storage-systems-data-warehousing/11072

Meta-Learning

Christophe Giraud-Carrier, Pavel Brazdil, Carlos Soares and Ricardo Vilalta (2009). *Encyclopedia of Data Warehousing and Mining, Second Edition* (pp. 1207-1215).

www.irma-international.org/chapter/meta-learning/10976