Chapter XI

A Protocol for Anonymous and Accurate E-Polling

Danilo Bruschi, Università degli Studi di Milano, Italy
Andrea Lanzi, Università degli Studi di Milano, Italy
Igor Na Fovino, Joint Research Centre, Italy

ABSTRACT
E-polling systems are a fundamental component of any e-democracy system as they represent the most appropriate tool for fostering citizens’ participation to public debates. Contrarily to e-voting protocols, they are characterized by less stringent security requirements and they can also tolerate errors affecting a small percentage of votes, without compromising of the final result. Thus, their realization can be effectively pursued supporting the diffusion of e-democracy. In this chapter, we propose a simple protocol for an accurate and anonymous e-polling system. Such a protocol satisfies, among the others, the following properties: a vote cannot be altered, duplicated, or removed without being detected and votes remain anonymous. Moreover, voters will be able to measure the level of trust of the process by verifying that their own votes have been correctly counted.
INTRODUCTION

The milestone of any democracy is participation. Obviously, such a postulate holds even in the case of e-democracy. In such a context, the model of direct democracy, which is hindered by nowadays population sizes and state organizations, would become possible through the adoption and diffusion of electronic polling systems. Whereby electronic polling systems we mean a set of hardware and software devices, which enable people to express their opinion on specific issues, provide a mean for gathering, and concentrate opinions from many participants. The main objective of e-polling systems is to capture general trends and people orientation on some specific issue. Generally speaking, polling systems, are one of the most appropriate tool for fostering citizens participation to public debates, and their online version enables more people to voice their views with less effort, because electronic polling can be performed from distributed locations at different times. Even if polling systems resemble voting systems, they are strongly differentiated by their final scopes. In fact, votes impose decisions while opinions expressed in a poll can only influence decisions. Such a difference has a huge impact on the security requirements, which characterize the two systems. In particular, the most critical security requirements, which so far compromised the realization of complete e-voting protocols only have a minor relevance in the construction of a polling system. For example, while a perfectly correct output has to characterize a voting process, an almost correct output can be tolerated by a polling process. Again, coercion and vote buying is a huge problem for voting systems but it has no relevance for polling systems. Thus even if we still do not have a complete solution to e-voting in either theoretical nor practical domains, we strongly believe that the current state of knowledge enables the construction of reliable and efficient polling systems, which in the short term could become a very important component of any e-democracy system, and significantly contribute to the diffusion of this new form of democracy. Starting from this consideration we devised a polling system which is: anonymous, sufficiently reliable (i.e., reproduce the opinions expressed by voters only with a marginal error), individually verifiable, and it is quite efficient and cost-effective. We believe that the adoption of our protocol and of similar ones, will greatly improve the state of the art on e-democracy, and contribute to its diffusion. This chapter is organized as follows: in “Related Works,” we will provide a brief overview on e-voting protocols, which can be adopted as well for building e-polling system; in “Voting vs. Polling,” we formally define an e-polling system underlying the differences with traditional e-voting systems. In “Preliminaries,” we describe the notation adopted throughout the chapter and we provide the definitions of peculiar concepts used for designing our protocol. In “The E-Polling Protocol,” a detailed description of the credential system and of our e-polling protocol is provided. The section “Correctness Analysis” contains a correctness analysis of our protocol, followed of our final considerations.
Exploring Importance of Environmental Factors for Adoption of Knowledge Management Systems in Saudi Arabian Public Sector Organisations
