SEAS: A Secure E-Voting Applet System*

Fabrizio Baiardi1, Alessandro Falleni2, Riccardo Granchi2, Fabio Martinelli2, Marinella Petrocchi2, and Anna Vaccarelli2

1 Dipartimento di Informatica, Università di Pisa, Italy
baiardi@di.unipi.it
2 Istituto di Informatica e Telematica - CNR - Pisa, Italy
{alessandro.falleni, fabio.martinelli, marinella.petrocchi, anna.vaccarelli}@iit.cnr.it

Abstract. This paper presents SEAS, the Secure E-voting Applet System, a protocol for implementing a secure and private system for polling over computer networks, usable in distributed organizations whose members may range up to dozens of thousands. We consider an architecture requiring the minimum number of servers involved in the validation and voting phases. Sensus, [7], a well known e-voting protocol, requires only two servers, namely a validator and a tallyer. Even if satisfying most of the security requirements of an e-voting system, Sensus suffers of a vulnerability that allows one of the entities involved in the election process to cast his own votes in place of those that abstain from the vote. SEAS is a portable and flexible system that preserves the lightness of Sensus, but it avoids the mentioned weakness. We propose a prototype implementation of SEAS based on Java applet and XML technology.

1 Introduction

The growing interest on e-voting systems in the last two decades is due to the appealing benefits that could be achieved from such a technology. One of the main factors of interest is that these systems enable the users to easily express their preferences from whatever location. This hopefully may help to increase the number of voters in public elections. Other advantages are the exact interpretation of ballots and the virtually immediate publication of the results.

Although there have been several attempts to apply e-voting systems to public elections, there are still several doubts on their application to real elections, [16]. We may briefly recall two kinds of problems. On the one hand, the voter is not in a controlled precinct and this may increase the possibility of coercion; on the other hand, there are the usual computer security threats, e.g., the user’s PC may be unreliable due to the presence of virus, Trojan horses, etc. These problems represent serious obstacles to the application of e-voting systems to large scale public elections, given the unquestionable nature that these elections must have. Thus, an e-voting system for public elections

* Work partially supported by MIUR Project: “Strumenti, Ambienti e Applicazioni Innovative per la Società dell’Informazione”, sottoprogetto SP1: Reti INTERNET: “efficienza, integrazione e sicurezza”.

** This author is currently working at TradeSoft Technologies, Pisa, Italy.

© Springer-Verlag Berlin Heidelberg 2004
should be not only secure, but also perceived as secure by its users. Because of these considerations, several researchers still consider the application of e-voting systems to large scale elections premature.

Nevertheless, we believe that e-voting solutions may be successfully applied for specific scenarios, e.g., for e-polling systems. A successful outcome in these specific areas could increase the user confidence in such technologies. In this paper, we thus consider elections/polling in distributed organizations, whose members may range up to dozens of thousands and we suppose them to have digital certificates, following the directives of the proposed standard [10]. We investigate the adoption of the Sensus protocol [7], because it exploits a very limited number of distinct servers (basically two entities, namely the validator and the tallier). This makes the protocol more manageable w.r.t. other solutions adopting many servers, like the one proposed in [11].

Sensus suffers from a vulnerability that allows one of the entities involved in the election process to cast votes of eligible users that, although registered in the election process, abstain to vote. These illegitimate votes would fall into the final tally.

The main contribution of this paper is the design of SEAS, the Secure E-voting Applet System. SEAS has been defined by modifying the Sensus protocol, to avoid its well-known vulnerability, while preserving its other security properties. Further, we propose a prototype implementation of SEAS based on Java applet technology and XML, in order to define a flexible e-voting package.

Structure of the paper. Section 2 recalls the main goals of the e-voting protocols. Section 3 introduces notation and assumptions on which we rely throughout the paper. Section 4 describes the Sensus protocol and Section 5 introduces the SEAS protocol, our proposed variant of Sensus. Section 6 briefly sketches our prototype implementation. In Section 7 we discuss related work in the secure e-voting area. Finally, Section 8 offers some conclusions.

2 E-Voting Protocol: Goals

A comprehensive survey of the goals of an e-voting protocol has been proposed in [9]. Here, we recall some of the main properties only. Roughly speaking, any e-voting system should assure voter privacy while avoiding opportunities for fraud. Again, to be useful and acceptable by the voters community, it should be, at least, as secure as a traditional system. In particular, a set of criteria may be addressed as prudent guidelines for implementing a generic system.

Soundness, Unreusability, Completeness. These three properties are strictly related. Soundness requires that no elector can invalidate the election (or the survey). This implies that either the final tally is correct or that any error in the final tally can be detected and consequently corrected. Unreusability and Completeness can be seen as sub-properties of soundness. The former requires that nobody can vote twice. As far as the latter is concerned, a system is complete if it is not possible to i) forge a vote; ii) remove a valid vote from the final tally; iii) add an invalid vote to the final tally. In practice, the property of completeness requires that all and only the valid votes get counted.