Is it Secure to Vote Electronically? Security Considerations in the e-Election Process

Maria Rigou[1,2], *Spiros Sirmakessis*[1,3], *Athanasios Tsakalidis*[1,2]

[1]Computer Technology Institute
Internet and Multimedia Technologies Research Unit
61 Riga Feraiou Str. GR-26110, Patras, Greece
&
[2]University of Patras, Computer Engineering and Informatics Department,
Multimedia, Graphics and GIS Laboratory, 26500 Patras, Greece
&
[3]Technological Education Institution of Messolongi, Department of Applied Informatics in Administration and Economy, 302 00, Messolongi, Greece
{rigou, syrma, tsak}@cti.gr

Abstract

The e-voting process is a complex process. In this paper, we present the characteristics of a "good" voting system. Based on these characteristics, several scientists have introduced different protocols for the implementation of a system. A description of these protocols and references to existing systems are presented.

Introduction

The right of individuals to vote for government representatives is at the heart of the democracy that we enjoy. Historically, great effort and care has been taken to ensure that elections are conducted in a fair manner such that the candidate who should win the election based on the vote count actually does. Of equal importance is that public confidence in the election process remains strong. In the past changes to the election process have proceeded deliberately and judiciously, often entailing lengthy debates over even the minutest of details. These changes are approached so sensitively because a discrepancy in the election system threatens the very principles that make our society free, which in turn, affects every aspect of the way we live.

Times are changing. We now live in the Internet era, where decisions cannot be made quickly enough, and there is a perception that anyone who does not jump on the technology bandwagon is going to be left far behind. Businesses are moving online at astonishing speed. The growth of online interaction and presence can be witnessed by the exponential increase in the number of people with home computers and Internet access.

There is a prevailing sentiment that any organization that continues in the old ways is obsolete. So, despite the natural inclination to treat our election process as the precious, delicate and fragile process that it is, the question of using the new advances in technology to improve our elections is natural.

The feasibility of remote electronic voting in public elections is currently being studied by several organisations, like the National Science Foundation by request of the President of the United States (see http://www.netvoting.org/). Remote electronic voting refers to an election process whereby people can cast their votes over the Internet, most likely through a web browser, from the comfort of their home, or possibly any other location where they can get Internet access. There are many aspects of elections besides security that bring this type of voting into question. The primary ones are:

- **Coercibility** the danger that outside of a public polling place, a voter could be coerced into voting for a particular candidate.
- **vote selling** the opportunity for voters to sell their vote.
- **vote solicitation** the danger that outside of a public polling place, it is much more difficult to control vote solicitation by political parties at the time of voting.
- **registration** the issue of whether or not to allow online registration, and if so, how to control the level of fraud.

The possibility of widely distributed locations where votes can be cast changes many aspects of our carefully controlled elections as we know them. The relevant issues are of great importance, and could very well influence whether or not such election processes are desirable. In this paper, we will focus in the internet voting process (Dictson and Ray, 2000). Internet voting (*i-vote*) has been referred to as the ultimate challenge in network security and data encryption. Currently, internet-based election systems are in the early stages of development and testing. A number of organizations (both public and private) are competing to be the first-to-market with their Internet-based voting systems. The organizations are utilizing some of the best engineers, scientists, and technologies in the world to create the extremely complex systems and infrastructures that will be required to conduct secure elections over the Internet.

Electronic voting systems

There have been several studies on using computer technologies to improve elections (California Internet Voting Task Force. 2000), (MIT, 2001), (Mercuri, 2000) *(NSF*, 2001), (Rubin, 2002). These studies caution about the risks of moving too quickly to adopt electronic voting machines because of the software engineering challenges, insider threats, network vulnerabilities, and the challenges of auditing.

As a result of the Florida 2000 presidential election, the inadequacies of widely-used punch card voting systems have become well understood by the general population. This has led to increasingly widespread adoption of “direct recording electronic” (DRE) voting systems (Figure 1). DRE systems, generally speaking, completely eliminate paper ballots from the voting process. As with traditional elections, voters go to their home precinct and prove that they are allowed to vote there, perhaps by presenting an ID card, although some states allow voters to cast votes without any identification at all. After this, the voter is typically given a PIN or a smartcard or some other token that allows them to approach a voting terminal, enter the PIN or smartcard, and then vote for their candidates of choice. When the voter’s selection is complete, DRE systems will typically present a summary of the voter’s selections, giving them a final chance to make changes. Subsequent to this, the ballot is “cast” and the voter is free to leave.

Figure 1. Direct recording electronic" (DRE) voting systems

The most fundamental problem with such a voting system is that the entire election hinges on the correctness, robustness, and security of the software within the voting terminal. Should that code have security relevant flaws, they might be exploitable either by unscrupulous voters or by malevolent insiders. Such insiders include election officials, the developers of the voting system, and the developers of the embedded operating system on which the voting system runs. If any party introduces flaws into the voting system software or takes advantage of pre-existing flaws, then the results of the election cannot be assured to accurately reflect the votes legally cast by the voters.

The Characteristics of a "Good" Electronic Voting System

The characteristics of a good electronic voting system depend on the purpose for which the system will be used. However, there are similarities between most polls that it is possible to develop a set of general characteristics that are likely to be desirable in most situations. When designing an electronic polling system, it is essential to consider ways in which the polling tasks can be performed electronically without sacrificing voter privacy or introducing opportunities for fraud. The following is one set of desirable characteristics for electronic polling systems which incorporates the characteristics of most systems described in the electronic voting literature (Cranor and Cytron, 1996):

- **Accuracy.** A system is accurate if it is not possible for
  - a vote to be altered,
  - a validated vote to be eliminated from the final tally, and
  - an invalid vote to be counted in the final tally.

- **Democracy.** A system is democratic if it
  - permits only eligible voters to vote and
  - ensures that each eligible voter can vote only once.

- **Privacy.** A system is private if
  - neither election authorities nor anyone else can link any ballot to the voter who cast it and
  - no voter can prove that he or she voted in a particular way.

- **Verifiability.** A system is verifiable if anyone can independently verify that all votes have been counted correctly.

- **Convenience.** A system is convenient if it allows voters to cast their votes quickly and with minimal equipment or special skills.
- **Flexibility.** A system is flexible if it allows a variety of ballot question formats.
- **Mobility.** A system is mobile if there are no restrictions (other than logistical ones) on the location from which a voter can cast a vote.

The mobility property itself is a major contributor to some of the problems associated with designing a secure and private electronic voting system. By allowing voters to cast their votes from virtually anywhere, we dramatically expand the universe of ineligible people who may attempt to vote. We also limit our abilities to prevent voters from proving how they voted, as there are no longer private voting booths that can prevent vote buyers from observing vote sellers as they cast their votes. Based on these characteristics we can define several voting protocols (Cranor, 1996) described in the following section.

Cryptographic Voting Protocols

Any voting protocol should be able to follow the characteristics of a "good" voting system. Some of the protocols already defined in the international literature follow. Each protocol involves a voter (an individual registered and authorized to participate in the voting process), a validator (a specific, predefined person, responsible for the accuracy of the process) and a tallier (a person/machine that counts the votes). In each country and vote, these three persons may have different names or responsibilities.

The Simple Protocol follows the common voting process, without employing any cryptographic techniques. Such a protocol, illustrated in Figure 2, requires the voter to submit to an electronic *validator* an electronic ballot with the voter identification number attached. The validator uses the identification number to check the voter off on a list of registered voters. Then the validator stripes off the identification number and sends the ballot to an electronic *tallier*. The tallier records the votes and adds them to the election tally.

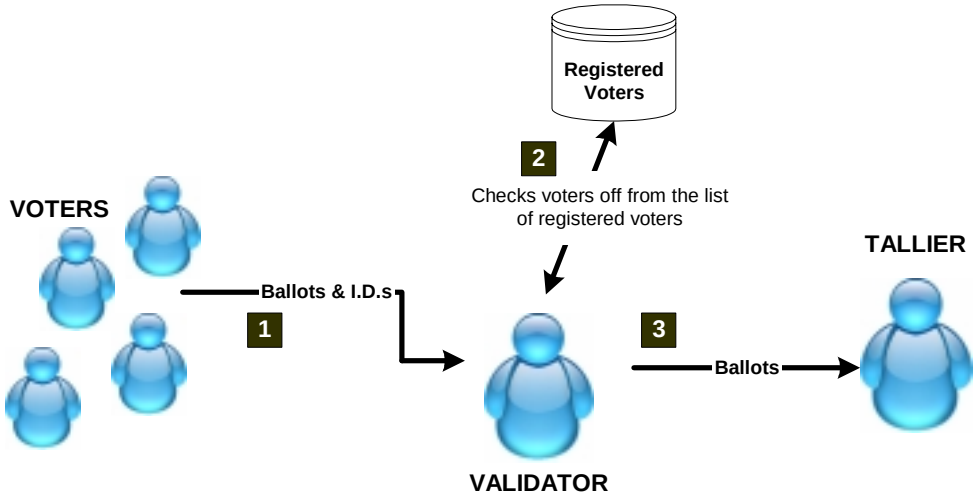

Figure 2. The Simple Protocol.

Although this simple protocol is flexible, mobile, and convenient, it has several major problems. Voters could stuff the ballot box by using other voters' identification numbers. Although the validator program is not supposed to read or record the contents of the ballot, voters cannot really be sure that the validator program does not violate their privacy in this way. Also, there is no way to ensure that the validator does not alter ballots before sending them to the tallier or manufacture ballots that were never actually submitted by voters. At last, there is no way to ensure that the tallier accurately records the votes.

The problem of voters stuffing the ballot box can be solved by requiring voters to sign their ballots with digital signatures (using PGP). Thus, unless a voter's secret key has been compromised, we can be assured that voters are not using others' identification numbers. Furthermore, we can prevent the validator from violating voters' privacy by having voters encrypt their ballots with the tallier's public key. Thus the validator will not be able to read or alter the ballots. However, if the validator and tallier team up and the validator obtains the tallier's secret key, privacy can be compromised. Thus we need a more sophisticated approach to incorporating cryptography into our electronic voting system.

The one and two agency protocols. Nurmi, Salomaa, and Santean (1991) proposed an approach that solves many of the problems mentioned above. In this "Two Agency Protocol," shown in Figure 3, the electronic validator distributes a secret identification tag to each voter prior to the election. The validator then sends the tallier a list of all identification tags, with no record of the corresponding voters. Each voter sends the tallier his or her identification tag and an encrypted file containing a copy of the tag and the voted ballot. At this point the tallier can make sure the identification tag is valid, but the program has no way of examining the contents of the ballot. The tallier publishes the encrypted file (so that the voter has proof that the file was submitted on time), and the voter responds by sending the tallier the key necessary to decrypt it. When the election is over, the tallier publishes a list of all voted ballots and the corresponding encrypted files. At this point the voters can confirm that their votes were counted properly. Any voter who finds an error can protest by submitting the encrypted file and decryption key again. Because the encrypted file was published earlier, the tallier cannot deny having received it.

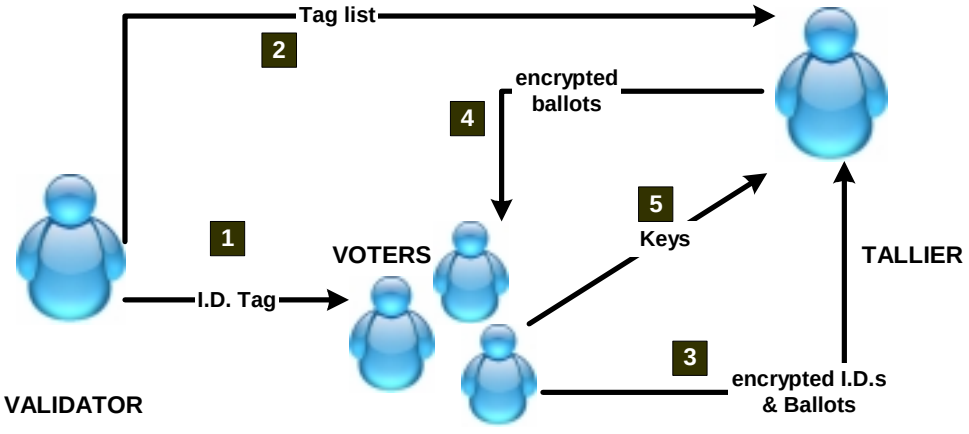

Figure 3. Two Agency Protocol

The Two Agency Protocol is verifiable by individual voters however, it still has several problems; it does not protect voters' privacy if the tallier and validator collude. Thus, the authors state that if the two agencies are going to work together, there might as well be just one agency.

The One Agency Protocol (Salomaa, 1991) is identical to the Two Agency Protocol, except for the tag distribution procedure. In the One Agency Protocol, tags are distributed by the tallier (there is no validator) using an ANDOS (http://www.julienstern.org/files/andos/node10.html)-all or nothing disclosure of secrets protocol for secret selling of secrets. This solves the collusion problem; however, the ANDOS protocol is quite computationally complex and does not scale well.

Both of the Nurmi, Salomaa, and Santean protocols fail to satisfy the second part of the privacy property and part of the accuracy property. The mechanism that allows voters to verify that their votes were counted correctly also allows them to prove that they voted in a particular way. The accuracy property is not completely satisfied because the tallier may cast votes for all the voters who have been assigned tags but do not exercise their right to vote. These voters may discover this violation and report it, but they cannot prove that they did not actually vote.

Blind signature protocols. When David Chaum first introduced the concept of blind signatures in 1982, he suggested that blind signatures could be used for secret ballot elections. Ten years later, Fujioka, Okamoto, and Ohta (1992) developed a practical voting scheme that uses blind signatures to solve the collusion problem inherent in protocols like the Two Agency Protocol without significantly increasing the overall complexity of the protocol. Blind signatures are a class of digital signatures that allow a document to be signed without revealing its contents. The effect is similar to placing a document and a sheet of carbon paper inside an envelope. If somebody signs the outside of the envelope, they also sign the document on the inside of the envelope. The signature remains attached to the document, even when it is removed from the envelope.

In the Fujioka, Okamoto, and Ohta protocol, shown in Figure 4, the voter prepares a voted ballot, encrypts it with a secret key, and blinds it. The voter then signs the ballot and sends it to the validator. The validator verifies that the signature belongs to a registered voter who has not yet voted. If the ballot is valid, the validator signs the ballot and returns it to the voter. The voter removes the blinding encryption layer, revealing an encrypted ballot signed by the validator. The voter then sends the resultant signed encrypted ballot to the tallier. The tallier checks the signature on the encrypted ballot. If the ballot is valid, the tallier places it on a list that is published after all voters vote. After the list has been published, voters verify that their ballots are on the list and send the tallier the decryption keys necessary to open their ballots. The tallier uses these keys to decrypt the ballots and add the votes to the election tally. After the election the tallier publishes the decryption keys along with the encrypted ballots so that voters may independently verify the election results.

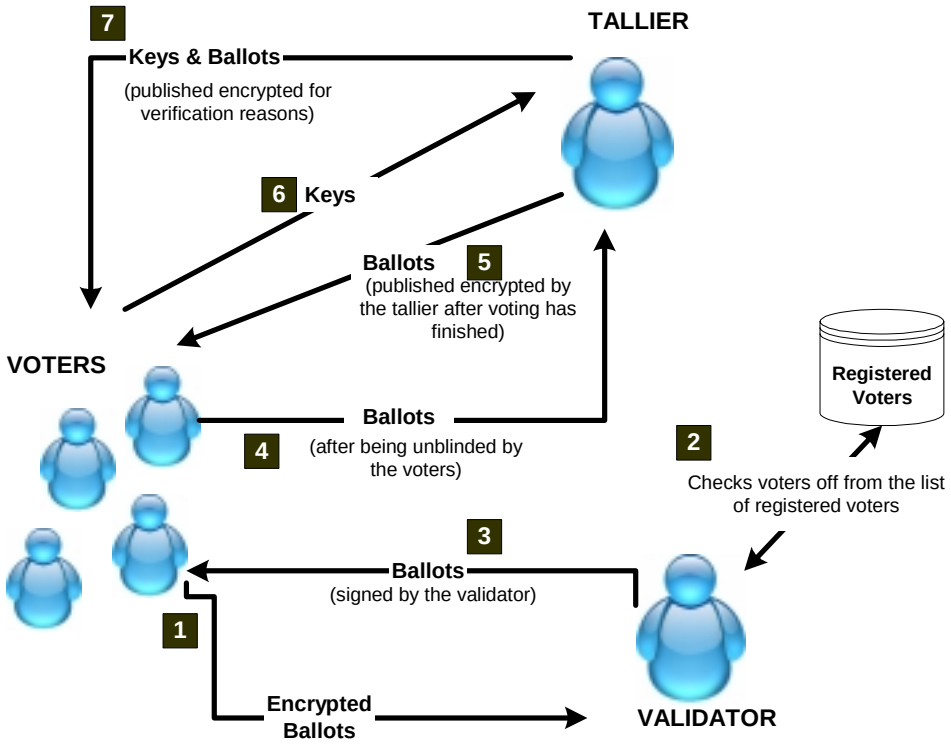

Figure 4: Blind Signature Protocol.

Cranor and Cytron's Sensus system (Cranor, and Cytron, 1996) is based closely on the Fujioka, Okamoto, and Ohta scheme. The main difference between these schemes emerges after the voter has submitted the encrypted ballot to the tallier. In the Sensus protocol, the tallier responds by sending a receipt to the voter. The Sensus protocol is one of the few electronic voting protocols that have actually been implemented. Another variation of the Fujioka, Okamoto, and Ohta protocol was implemented by Davenport, Newberger, and Woodard (Davenport et al., 1995) and used to conduct a student government election.

Conclusion

In the previous section, we presented several protocols that can be used to implement an e-voting process. Despite any complexity issues, any software or hardware that supports the voting should ensure that elections are conducted in a fair manner such that the candidate who won the election based on the vote count actually does. Of equal importance is that public confidence in the election process remains strong.

The protocols, presented in this paper, demonstrate that an e-voting system can be accurate, democratic, verifiable, convenient, flexible, mobile and ensures privacy. The technology that would be chosen to support the protocol should focus in achieving the characteristics of an efficient e-voting system. The importance of security in elections cannot be overstated. The future of any country rests on public confidence that the people have the power to elect their own government. Any process that has the potential to threaten the integrity of the system, or

even the perceived integrity of the system, should be treated with the utmost caution and suspicion.

The design of a "good" voting system, whether electronic or using traditional paper ballots or mechanical devices must be robust against a wide variety of potentially fraudulent behavior. The anonymity of a voter's ballot must be preserved, both to guarantee the voter's safety when voting against a malevolent candidate, and to guarantee that voters have no evidence that proves which candidates received their votes. The existence of such evidence would allow votes to be purchased by a candidate. The voting system must also be tamper-resistant to thwart a wide range of attacks, including ballot stuffing by voters and incorrect tallying by insiders. Another important consideration, as shown by the so-called "butterfly ballots" in the Florida 2000 presidential election, is the importance of human factors. A voting system must be comprehensible to and usable by the entire voting population, regardless of age, infirmity, or disability. Providing accessibility to such a diverse population is an important engineering problem and one where, if other security is done well, electronic voting could be a great improvement over current paper systems. Flaws in any of these aspects of a voting system, however, can lead to indecisive or incorrect election results. Research in the area of security, cryptography and anonymity can improve the existing e-voting systems.

References

California Internet Voting Task Force. (2000) *A report on the feasibility of Internet voting*, http://www.ss.ca.gov/executive/ivote/.

Chaum, D. (1982) Blind signatures for untraceable payments. In Proceedings of Crypto 82, Plenum Press, New York., pp. 199-203.

Cranor, L.F. and Cytron, R.K. (1996) Design and Implementation of a Security-Conscious Electronic Polling System. Washington University Computer Science Technical Report WUCS-96-02.

Cranor, L. F. (1996) Electronic Voting, ACM Crossroads, available at http://www.acm.org/crossroads/xrds2-4/voting.html

Davenport, B., Newberger, A., and Woodard, J. (1995) Creating a secure digital voting protocol for campus elections. Unpublished paper. Available online from http://www.princeton.edu/~bpd/voting/

Dictson, Derek and Ray, Dan, (2000) The Modern Democratic Revolution: An Objective Survey of Internet-Based Elections, White Paper, available through SecurePoll http://www.securepoll.com/Papers.htm.

MIT Voting Technology Project, (2001) Voting: What Is; What Could be, http://www.vote.caltech.edu/Reports/.

Fujioka, A, Okamoto, T., and Ohta, K. (1992) A practical secret voting scheme for large scale elections. In Advances in Cryptology - AUSCRYPT '92, Springer-Verlag, Berlin, pp. 244-251.

Mercuri. R. (2000) *Electronic Vote Tabulation Checks and Balances*. PhD thesis, University of Pennsylvania, Philadelphia, PA.

National Science Foundation. (2001) *Report on the National Workshop on Internet Voting: Issues and Research Agenda*, http://news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf.

Nurmi, H., Salomaa, A., and Santean, (1991) L. Secret ballot elections in computer networks. Computers and Security, 36, 10, pp. 553-560.

Rubin A. D. (2002) Security considerations for remote electronic voting. *Communications of the ACM*, 45(12):39–44, http://avirubin.com/e-voting.security.html.

Salomaa, A. (1991) Verifying and recasting secret ballots in computer networks. In New Results and New Trends in Computer Science, Springer-Verlag, Berlin., pp. 283-289.