A Critical View on Internet Voting Technology

Eleni Tsekmezoglou[1], John Iliadis[2]

[1]*Banking & Enterprise Solutions Division, INTRACOM S.A.,*
19.5 km Markopoulou Ave, Athens GR-19002, Greece
Email: eleni.tsekmezoglou@intracom.gr

[2]*Department of Information & Communication Systems Engineering, University of the Aegean,*
Research Unit, 30 Voulgaroktonou St., Athens GR-11472, Greece
Email: jiliad@aegean.gr

Abstract. We present a set of requirements for Internet voting protocols. We also present a short overview of the most prominent Internet voting protocols published so far, and we provide a comparative evaluation of those protocols, using the set of requirements we have developed. We proceed with discussing our thoughts regarding possible improvements in e-voting protocols. Internet is an application with a vision to the future. Nevertheless, a lot of work needs to be done before it can be accepted for large-scale elections.

Keywords

electronic voting protocols, threats, countermeasures, comparative evaluation

1 Introduction

An electronic voting system is a general term that includes several types of voting. Internet voting is one and probably the most promising of them and refers to the casting of ballots over the Internet. In this paper, we shall use the terms electronic voting and Internet voting interchangeably, even though they do not convey exactly the same meaning.

Electronic voting systems attempt to achieve at least the same level of security traditional voting systems offer. The identity of voters and their ballot must be kept private. Furthermore, unauthorised persons must be prevented from voting and authorised persons must be prevented from casting more than one ballot. There is a trade-off among security and privacy in electronic voting and it must be determined how best to strike a balance if the Internet is to be used for large-scale elections [Adler, 2000].

This paper covers issues related to a security conscious electronic polling system design. Furthermore, the most significant requirements that need to be satisfied by a practical electronic voting system are put forth. The paper also focuses on the potential benefits and drawbacks of this new technology. We present

the existing Internet voting schemes and we also provide a critical review and comparison of those schemes.

2 Security Considerations for Electronic Voting

In this section we present the security aspects of an electronic voting system. We outline the threats a voting system has to deal with and the security requirements it has to meet, such as privacy, integrity, verifiability, availability, eligibility, authentication, reliability and un-reusability.

2.1 Security Requirements

The touchstone in developing an Internet voting system is represented by the necessity to meet the requirements of legal principles [Will, 2002]. Even though the characteristics of a good electronic voting system depend on the purpose for which the system will be used, elections have to satisfy basic voting principles, which are formulated due to legal and constitutional requirements.

Specifically, elections have to be universal and equal. Universal elections guarantee equal suffrage for everybody, meaning equal access to voting. The so-called digital divide threatens to further alienate those who do not possess the financial or other means to vote electronically. Equal elections guarantee that all ballots have the same influence on the result and all voters are able to vote in the same formal way. Furthermore, elections have to be free and secret. The principle of free elections requires the facility for every voter to cast his ballot free of duress. Secrecy of elections demands that only the voter is aware of his voting decision, which may never be revealed to anybody else without her permission. To prevent disposal of votes, the voter must not be able to prove anybody whom he voted for. Finally, elections have to be direct in the sense that they prevent someone from voting on behalf of other eligible voters [Hutter, Volkamer, 2004].

A set of security requirements derive from a number of threats relative to the set-up and registration phase of the system prior to the election. In the registration stage the authorities determine who is eligible to vote, maintain proper lists of the registered voters and provide them with voting credentials that will enable them to participate in the tally. The risks at this stage are twofold: The authorities may register ineligible voters or may provide multiple credentials to a single voter. Additionally, corrupt authorities may attempt to provide credentials to voters that will allow tracking and revealing how they voted.

According to [Schneier, 1996] a voting protocol must meet the following requirements:

- Nobody can find out how a voter voted
- Every voter can make sure that his vote has been taken into account in the final tabulation
- The voting system must always be operative whenever it is expected to be

- Only eligible voters can vote
- Nobody can duplicate or change someone else's vote without being discovered
- The voting system itself should be accurate and reliable
- Authorised voters cannot vote more than once
- The voting procedure should be simple and the voting system easy to use by voters.

In the following sections, we present the security properties that derive from the aforementioned requirements.

2.1.1 Privacy

An election system is private if neither the 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.

The first factor has to do with the democratic right to keep the voter's ballot secret. The second privacy factor is important for the prevention of vote buying and threatening. The voters can only sell their votes if they are able to prove to the buyer that they actually voted according to the buyer's wishes.

2.1.2 Verifiability

Verifiability is defined as the property that allows an external auditing entity to verify that the votes have been counted correctly and a voter can determine if his vote was counted correctly.

The most verifiable systems allow all voters to verify their votes and correct any mistakes they might find without sacrificing privacy. Less verifiable systems might allow mistakes to be pointed out, but not corrected or might allow verification of the process by party representatives but not by individual voters.

2.1.3 Availability

System availability is the ability to carry on even when some authorities misbehave. The system must always be available for use whenever it is expected to be operative and protected against both accidental and malicious denials of service. This could be achieved by increasing hardware-fault tolerance and system security.

2.1.4 Eligibility and Authentication

Eligibility and Authentication are there to ensure that only authorised voters cast their vote. Authentication can be achieved in different ways. Preferably, it must no longer rely on passwords since they can be easily compromised but on other types of authentication schemes such as biometrics, even though they also have recognised vulnerabilities, such as the fact that system performance may be affected by current conditions of the live sample [Banerjee, 2002].

2.1.5 Integrity

Integrity must be there to ensure that the votes cannot be modified, forged, or deleted without detection. Integrity can refer to the system, data and the people running the system.

System integrity means that the computer system (hardware and software) must be tamper proof. Ideally, system changes must be prohibited throughout the active stages of the election process. That is, once certified, the code, initial parameters, and configuration information must remain static.

Data integrity can be subverted as a result of compromises of system integrity. All data involved in entering and tabulating votes must be tamper proof and votes must be recorded correctly. One-way hashing functions or even public-key encryption may be useful for providing later verification that a particular vote was actually recorded as cast.

Personnel integrity. People involved in developing, operating, and administering electronic voting systems must be of unquestioned integrity and be trustworthy.

2.1.6 Reliability

Reliability means that an election system should work robustly, without loss of any votes and therefore be trustworthy and accurate. It can be achieved by using modern software-engineering techniques, which can result in fewer bugs and greater assurance. In a reliable system the final vote tally must be perfect, either because no inaccuracies can be introduced or because all inaccuracies introduced can be detected and corrected.

2.1.7 Un-Reusability

Un-reusability or uniqueness defines the democratic need that authorised voters can vote only once.

2.1.8 Convenience

A system is *convenient* if it allows voters to cast their votes quickly, in one session, with minimal equipment and no special skills.

2.1.9 Incoercibility

A system is incoercible if the voter cannot prove his operations to a coercer, i.e. a person who would prescribe a voter to send a ballot of some very specific kind and later check that it is present in the results.

2.2 Other Properties

A successful voting system should possess some additional properties that do not relate directly to security.

- *Flexibility*. A system is flexible if it allows a variety of ballot question formats including open-ended questions, is compatible with a variety of standard platforms and technologies, is accessible to people with disabilities.
- *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 therefore enabling voters to cast their vote from any geographical location. One of the reasons that people could be interested in electronic voting systems is that they can be mobile. Besides, technology could and should serve as a means of coping with the crisis of participation and confidence that democracy is facing in our days [Mitrou et al., 2003]. Voter participation might increase if people could easily cast votes from computers in their homes, offices, schools, and libraries. The mobility property, however, is a major contributor to some of the problems associated with an 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.
- *System disclosability* requires that the system software and hardware are open for random inspection at any time (including documentation).
- *Interface usability* is essential because systems that are particularly user-friendly may be even more amenable to subversion than those that are not.

3 Review of Existing Internet Voting Schemes

In this section we present a classification of the existing Internet voting schemes and give an overview of a representative existing protocol for each category. We proceed with an evaluation, critical analysis and comparison of the described protocols. The results are illustrated in an easy-to-read table at the end of the section.

Secret-ballot voting protocols are one of the most significant applications of cryptographic protocols. Several schemes have been proposed in the last fifteen years, some of which have been implemented as well. Most voting schemes are unable to satisfy all the desired characteristics. However, each one of them has been designed to meet specific goals and cover the needs of different applications.

The most efficient secret-ballot voting protocols can be classified by their approaches into three groups [Hirt, Sako, 2000], although some can belong to more than one. The suitability of each of these three types varies with the conditions under which it is to be applied:

- Schemes based on blind signatures ([Fujioka A., Okamoto T. & Ohta K., 1992], [Sako, 1994], [Okamoto, 1997])
- Schemes based on homomorphic encryption [Benaloh, 1987], [Benaloh, Tuinstra, 1994], [Sako, Kilian, 1994], [Cramer R., Franklin M. K., Schoenmakers, B. & Yung, M., 1996], [Cramer R. Gennaro R. & Schoenmakers B., 1997]
- Schemes based on mix nets [Chaum, 1981], [Sako, Kilian, 1995], [Hirt, Sako, 2000]

We proceed with presenting three representative protocols, the Fujioka, Okamoto and Ohta [Fujioka et al., 1992], the Cramer, Gennaro and Schoenmakers [Cramer R. Gennaro R. & Schoenmakers B., 1997] and the Chaum protocol [Chaum, 1981], which belong to each of the three aforementioned categories.

3.1 Schemes Based on Blind Signatures

"Blind signatures" is a method to maintain both security and privacy and have been introduced by Chaum. They allow someone to sign a document without knowledge of its contents.

3.1.1 Fuijioka, Okamoto and Ohta protocol

Fujioka, Okamoto and Ohta [Fujioka et al., 1992] introduced a mathematical framework for a secure election based on blind signatures, leaving out –however– many details needed for a full implementation.

Their proposed scheme is more suitable for large-scale elections, since the communication and computation overhead is fairly small even if the number of voters is large. It provides provable security, provided that the cryptographic functions that it uses are unbreakable. Furthermore, it ensures the privacy of the voter, even if both the administrator and the counter conspire, and voting fairness, i.e., no one can know even intermediate result of the voting. Finally it prohibits fraud by either the voter or the administrator.

Okamoto [Okamoto, 1996] proposed receipt-free voting schemes for this protocol. The receipt-free property means that voting system generates no receipt (evidence) of whom a voter voted; therefore it is not possible to coerce the voter.

The major problem of this scheme is that a failure of a single voter can disrupt the whole election process. Specifically, to maintain a secure election, even people who were not able to vote must verify that no vote was counted for them. Besides, the fact that the scheme requires a communication that is both secret and anonymous, it is impractical in real elections.

The participants of the scheme consist of voters, an administrator and a counter. It is assumed that:

- an anonymous communication channel exists, through which the counter and voter communicate,

- a bit commitment scheme exists, i.e. a ballot serial number on the authority-signed ballot is returned to the voter for computing ballot. In this way, the voter can then detect attacks where the voted ballot or ballot serial number have been modified. The voter can do that by verifying that his ballot number is present among the published ballots and that it contains the correct vote,
- every voter has his own ordinary digital signature scheme, the administrator has a blind signature scheme and the counter only creates a list of ballots and publishes it.

The Fuijioka et al protocol consists of three stages: *registration*, *voting* and *opening* [Dastjerdi et al, 1994]. We examine each of these stages in the following paragraphs.

Registration Stage. In order to be certified for the eligibility, each voter sends a request to the administrator for registration. Registration requires co-operation between the voter and the administrator. The voter selects his candidates and commits to this ballot by using a random key. This committed ballot is then blinded and signed by the voter. It is then sent to the administrator. The administrator verifies the right of the voter to vote, and the signature of the blinded vote. After a voter proves his identity to the administrator, the administrator will sign the committed, blinded ballot it is given. So, for every voter, the administrator checks:

- IF the voter has the right to vote, has not already applied for a signature and the signature is valid
- THEN the administrator signs the committed, blinded ballot, sends it to the eligible voter and the voter is being removed from the list of those eligible to vote
- ELSE the administrator rejects the transaction.

Voting Stage. The voter unblinds the ballot, and verifies the administrator's signature, which, because of the blinding properties, should still be valid for the committed (but no longer blinded) ballot. The committed ballots, now signed by the administrator, are then sent, through an anonymous channel, to the counter which publishes it along with an index number. The voter will use the administrator's signature as proof of eligibility with the counter.

The vote is actually sent in two parts. First the committed ballot signed by the administrator is anonymously passed to the counter. While the counter knows the vote is valid, it cannot break the commitment scheme to actually see it. Rather it must wait for the keys to uncommit the vote to be sent through a second anonymous channel.

The counter checks the signature of the ballot using the administrator's verification key. If the check succeeds then the counter enters the ballot and the administrator's signature of it into a list. The counter

does know to count the votes, because they have the administrator's signature, however, has no way of matching the ballots it receives to any voter.

Opening Stage. At the end of the protocol, after all the committed votes have been sent in, a list of all voters who have had their vote signed is published by the administrator. This list includes their name, blinded ballot, and its signature. The counter's intermediate published list has the committed (unblinded) ballot and its signature. After everyone has had a chance to confirm the entries in the counter's published list, each voter sends in the keys needed to uncommit his vote, along with the index of the committed vote. Again the communication is through an anonymous channel.

The counter opens the ballot, retrieves the vote and also the counter counts the vote and announces the result. The final published list of the counter contains the values from the intermediate list as well as the keys used to uncommit, and the uncommitted (plaintext) vote, itself.

We proceed with examining the protocol, according to the security requirements we have specified in a previous section.

Privacy. The relationship between voters and their ID's are hidden by the blind signature scheme that is used and the ballot and the key are sent through anonymous channels and cannot be traced. So, even if the administrator and the counter conspire, no relation can be found between a voter and his vote.

Verifiability. If we assume that no voter abstains from voting and no one forges the ordinary digital scheme, then even if the administrator and the counter conspire, they cannot change the result of the voting. However, the assumption that no voter abstains from voting is not realistic. There is always the possibility that a voter registers but does not vote, therefore if the administrator and the counter conspire, they can add false vote to the list and even worse the whole election will be disrupted.

Availability. The protocol is unsuccessful in terms of availability.

Eligibility. The voter must be on the list of the eligible voters. If we assume that the ordinary signature scheme is secure then a dishonest person cannot vote.

Integrity. Counting is done after the voting is completed, so it does not effect the voting.

Reliability. If every participant is honest, the result of the voting is trustworthy.

Unreusability. If the blind signature is secure this property is fulfilled.

Convenience. The scheme requires each voter to be active in three rounds (registration stage, voting stage and opening stage) making it fail to be user-friendly. An election of this nature might require 3 days to run, one for each step, an unappealing prospect to many potential users of the system.

Incoercibility. Incoercibility is not satisfied because the voter can prove whom he voted for.

3.2 Schemes Based on Homomorphic Encryption

In order to conduct an indisputable electronic election that also preserves the secrecy of each voter's choices, one can rely on three very powerful data constructions: digital signatures – which make the election indisputable, homomorphic encryption and zero knowledge proof – which keep all voter choices secret.

Homomorphic Encryption is a special kind of encryption that supports the property that the sum of two encrypted numbers is always equal to the encryption of their sum. This means that anyone can compute and verify the "encrypted sum" of a collection of encrypted values. Because the data is encrypted, this same person will not know what numbers are actually encrypted, either in the original values, or the final sum, but he will know that whatever the unencrypted values are, they maintain the sum/total relationship. The homomorphic property can be simply stated

$$f(E(m_1, m_2)) = g(E(m_1, E(m_2))),$$

where *f* and *g* are functions depending on the cryptosystem used.

The main idea of the schemes based on homomorphic encryption is that the ballot is viewed as a number. The ballot is shared and encrypted (using either secret sharing or threshold cryptosystem) between M authorities. The objective of a threshold cryptosystem is to share a public key B among M members of a group such that $E_B(x)$ can be decrypted only when a substantial subset t cooperate. Now, using homomorphism properties, ballots are first summed up and only then the sum is decrypted and reconstructed.

Protocols based on homomorphic encryption have been presented in [Benaloh, 1987], [Benaloh, Tuinstra, 1994], [Sako, Kilian, 1994], [Cramer et al., 1996], [Cramer et al., 1997]. We shall see how the above are implemented in the Cramer et al. protocol.

3.2.1 Cramer et. al. Protocol

Ronald Cramer, Rosario Gennaro and Berry Schoenmakers proposed an election scheme in [Cramer et al., 1997]. Four primitive ideas are used in this scheme:

- Threshold cryptosystem
- Public key encryption
- Bulletin board as a repository for voters' ballots
- Zero-knowledge proofs

There are M authorities $A_1,...A_m$ and a bulletin board. According to threshold cryptosystem, the authorities share a common ElGamal public key

$B = (p, g, \gamma)$, where $\gamma = g^{\alpha}$

According to Shamir threshold secret sharing scheme, each authority owns his secret share s_i of private key $C = \alpha$. The authorities are committed to their shares by public values $h^i=g^{S_i}$. This implies, that there is threshold trust with threshold *t* on the authorities. Also, each voter has his own public key pair.

As far as the general case is concerned, there are several ways of encoding *N* votes, such that the sum of several votes yields the sum of each type of vote. If, for example, $N = 2$ then one could set $V \in \{1,-1\}$ and could well derive the number of cast votes and how many 1-votes and how many (-1)-votes were cast. In the case that $N > 2$, one can still use a similar approach. For example, if voters are allowed to cast "yes", "no", or "empty", and we are only interested in whether there are more "yes" or more "no" votes (disregarding the number of "empty" votes), one can use the encoding 1 for "yes", -1 for "no" and 0 for "empty". However, if it must be possible to derive the exact number of cast votes for each choice, then more involved approaches are necessary.

In the case we are dealing with here, voter V can select between two different options. So, the ballot can be seen as one of numbers {1, -1}. The result of the election is calculated as the sum of these numbers. If the sum is positive or negative, then one option was selected more than the other. If it is zero, however, both options have been selected the same number of times.

When a voter wants to cast his ballot, he firstly has to compute g^v, where $v \in \{1,-1\}$ is his ballot. After that, he encrypts g^v: $(y_1, y_2) = (g^r, \gamma^r g^v)$ and constructs non interactive proof that the ballot was constructed correctly. This can be accomplished with a zero-knowledge proof of knowledge.

The encrypted ballot (y_1, y_2) and non interactive proof of correctness are sent to the bulletin board. This is signed using the voter's private key.

After all the voters have cast their votes and the election is over, the submitted ballots are verified by the authorities. If a ballot is incorrect it is removed and not counted in the result of the election. The eligibility of the election is ensured by checking the signatures of the ballots. In order to ensure un-reusability, at most one ballot of each voter must be counted. This can be succeeded by, for example, using the latest ballot sent by the particular voter.

At this point, the homomorphism property of ElGamal encryption is used on the encrypted ballots. As we know, the original ElGamal scheme is homomorphic with respect to multiplication.

$(g^{r_1}, \gamma^{r_1} g^{v_1})$

…

$(g^{r_N}, \gamma^{r_N} g^{v_N})$

which produces

$(g^{\sum r_i}, \gamma^{\sum r_i} g^{S})$

where $S = \sum v_i$ is the result of the election.

Afterwards, g^S is decrypted according to the threshold cryptosystem. This can be accomplished by any *t* authorities. Now, it is needed to extract *S* from g^S. Generally, computing discrete logarithm is considered infeasible, but in this case $S \in \{-N...N\}$. A solution could be to (pre)compute $g^{-N}, g^{-N+1}, ..., g^{-1}, g^0, g^1, ...g^{N-1}, g^N$ and compare these values with g^S.

We proceed with evaluating the Cramer et. al. protocol against the requirements that an electronic voting protocol should meet.

Privacy is ensured as long as at most *t-1* authorities misbehave according to the threshold trust on them.

Integrity and *verifiability* are satisfied because both voters and authorities must prove correctness of their actions. The authorities prove correctness of their actions implicitly when performing verifiable decryption in the setting of threshold cryptosystem.

Reliability and *availability* are also satisfied. Actually, result can be calculated as long as t authorities are available.

The *eligibility* of the election is ensured since the signatures of the ballots are checked, thus only authorised users can vote.

Unreusability is also satisfied given the fact that at most one ballot of each voter must be counted. This is succeeded by using the latest ballot sent by the particular voter.

Regarding *convenience*, the number of rounds for voter is 1.

Incoercibility is not satisfied because the voter can decrypt his ballot and present certificate for encryption (randomness used) to the coercer.

3.3 Schemes Based on Mix Nets

The main idea of this approach is to use different types of "mixes". Mixes take as an input a sequence of "scrambled" messages and produces as an output a sequence of "unscrambled" messages that correspond to some permutation of original sequence. Mixes can be used to permute different entities: ballots of

different voters or, for instance, all possible ballots for one voter, amongst which he can select the one he prefers.

The purposes of the mix are:

- To hide the correspondence between the items in its input and those in its output.
- To ensure that no item is processed more than once by attaching something like a time-stamp, that is only valid for a particular batch.

There are several schemes based on mix nets [Chaum, 1981], [Sako, Kilian, 1995], [Hirt, Sako, 2000]. We present a brief overview of the protocol proposed by David Chaum in [Chaum, 1981].

3.3.1 Chaum Protocol

The original secret voting protocol [Chaum, 1981] is based on a very simple idea. Each voter is allowed to submit one scrambled ballot to the input of a mix net. These submissions could be held on a bulletin board. After elections are over, the mix net unscrambles all submitted ballots. Now, the connection between voters and unscrambled ballots is broken. There is no restriction on the form of ballots. This allows having many questions of any kind. Each ballot in the output of mix net must be verified to satisfy prescribed format and then election results can be calculated.

So the protocol makes use of a trusted "mix" to scramble pair of votes and of digital pseudonyms in order to protect voter's privacy. But what are digital pseudonyms?

A *digital pseudonym* is a public key used to verify the signatures made by the anonymous holder of the corresponding private key. A list of pseudonyms is created by an authority that decides which applications for pseudonyms to accept. The authority, however, is unable to trace the pseudonyms in the completed list. The applications may be sent to the authority anonymously.

A prerequisite of the protocol is the existence of an *anonymous or untraceable communication channel.* For voter *V* to send message *M* to the administrator *B* anonymously, voter *V* has to seal first message *M* with his public key:

$$K, Y = E_K(R_0, M),$$

where R_0 is a big random number in order to eliminate the possibility of checking *Y* = *M* (to increase security).

Afterwards, voter *V* concatenates the address of *B* to the encrypted message and then encrypts with public key of mix K_1 and then sends via mix to *B*:

$$E'_{K_1}(R_1, E_K(R_0, M), A),$$

where R_1 is a random string number to increase security by eliminating the possibility of checking equality of plaintext and ciphertext, and *A* is address of *B*.

The Chaum voting scheme uses an anonymous communication channel and provides unconditional security against tracing the votes but the failure of a single voter can disrupt the election. This approach is not practical for large-scale elections because of the fact that the election must be restarted when a failure is traced.

Privacy is ensured since the correspondence between a voter and his vote cannot be found, while the scheme's *verifiability* and *reliability* depend on the respective properties of the mix net used. Regarding *availability*, the protocol is unsuccessful as failure of only one mix server halts the whole system. Similar mix net schemes with better availability and reliability would be more suitable.

Eligibility and *unreusability* can be ensured by requiring voters to sign their scrambled ballots before they are sent to the bulletin board. Later, before sending them to the mix net, signatures can be verified and multiple ballots from one voter can be dropped.

Integrity can be ensured in a straightforward manner.

Regarding *convenience*, the number of rounds for voter is 1.

Regarding *incoercibility,* scrambling is performed by encryption. Therefore the voter can prove to the coercer the value of his ballot by presenting certificates for encryption.

Regarding freedom of choice, as scrambling is performed by (possibly multiple) encryption; the voter can prove to the coercer the value of his ballot by presenting certificates for encryption. This excludes incoercibility. Also, vote duplication becomes quite important. The reason is that all ballots are decrypted and can be analysed separately. This problem can be tackled by requiring voters to prove that they possess encryption certificates.

In 1988, at EUROCRYPT'88, Chaum [Chaum, 1988] proposed a new protocol, which unconditionally conceals the identity of voters so that they are made untraceable. However, elections conducted with this protocol can still be disrupted by a single voter. Although Chaum's protocol can detect such disruptions, it cannot recover from them without restarting the entire election.

4 Comparison of Voting Schemes

Each of the presented protocols [Fujioka et. al., 1992], [Cramer et al., 1997], and [Chaum, 1981] has both advantages and disadvantages and can be used to meet different requirements.

Fujioka, Okamoto, and Ohta developed a practical voting scheme that uses blind signatures to solve the collusion problem without significantly increasing the overall complexity of the protocol. A number of

other, less satisfactory blind signature protocols have also been proposed. Sako [Sako, Kilian, 1994], for example, proposed a protocol that is simpler but does not completely prevent election administrators from linking ballots with the voters who cast them. The Fujioka et. al. protocol is considered to be one of the most suitable and promising for large-scale elections, since the communication and computation overhead is fairly small even if the number of voters is large. Moreover, this type of scheme naturally can allow multiple value voting, and is also very compatible with the framework of existing physical voting systems.

In the Fujioka, Okamoto, and Ohta protocol the tallier responds by placing the encrypted ballot on a list that is published after all voters vote. Thus, a voter cannot submit his or her decryption key until after the voting phase of the election is over. As a result, votes cannot be cast in a single session.

In addition, a major advantage of the Fujioka et. al. protocol is the fact that it is based on a framework that is widely acceptable and easily verifiable. In the opening stage, everyone has the chance to raise a claim if he is suspicious about the contents of the list. In that case, anyone could clearly determine whether the claim is valid or not, by checking the validity of the administrator's signature included in the claim.

The protocol proposed by Chaum in 1981 is the first published cryptographic voting protocol. The original protocol does not guarantee the untraceability of voters' identity. Furthermore, elections conducted with this protocol can be disrupted by a single voter. Even though it can detect such disruptions, the protocol cannot recover from them without restarting the entire election making the system rather impractical for large-scale elections.

When evaluating and comparing schemes we need to examine some core properties related to the system. We examine eight core security properties that have been analysed in a previous section. We have attempted to evaluate all three systems [Fujioka et. al., Cramer et. al. and Chaum] in relation to these properties and the results are given on the table that follows.

	Fujioka et. al.	Cramer et. al.	Chaum
Privacy	√	√	√
Verifiability	X	√	Depends on mix net
Availability	X	√	X
Eligibility	√	√	√
Integrity	√	√	√
Reliability	√	√	Depends on mix net
Un-reusability	√	√	√
Convenience	X	√	√
Incoercibility	X	X	X

Table I. Comparison of Voting Schemes

Privacy, integrity, eligibility and un-reusability are satisfied by all three schemes. However, in the case of Cramer et. al. protocol privacy is ensured as long as at most *t-1* authorities misbehave according to the threshold trust on them. Also, the eligibility requirement is satisfied in all three schemes under the assumption that the ordinary signature scheme is secure so the dishonest person cannot vote. The un-reusability of the Fujioka et. al. protocol is fulfilled if the blind signature is secure. It is also fulfilled in the Cramer et. al. given the fact that at most one ballot of each voter must be counted by using the latest ballot sent by the particular voter. Finally, the Chaum protocol ensures un-reusability by verifying signatures before sending them to the mix net so multiple ballots from one voter can be dropped.

The Fujioka et. al. protocol is not generally verifiable as there is always the possibility that a voter registers but does not vote and therefore if the administrator and the counter conspire, they can add false vote to the list and even worse the whole election will be disrupted. Chaum's scheme verifiability depends on the properties of the mix net used. Incoercibility is not covered in any protocol as the voter can prove to the coercer the value of his ballot by presenting encryption certificates. However, incoercibility is satisfied for the Fujioka et. al. protocol, according to the additions to the original protocol proposed by Okamoto [Okamoto, 1997].

Concerning the availability of Cramer et. al. we need to mention that the result can be calculated as long as t authorities are available. The Fujioka et. al. scheme is robust if every participant is honest. On the other hand, reliability of Chaum's depends again on the properties of the mix net used. Convenience is quite satisfactory for Cramer et. al and Chaum as the number of rounds for voter is 1 and they are both revisable. However, Fujioka et. al. is not so convenient and user friendly as the scheme requires each voter to be active in three rounds.

Finally, evaluation of all three protocols in terms of their feasibility, is a fairly controversial issue. Internet voting protocols examined in this paper can be feasible with a few –more or less– changes. Besides, there have already been mentioned a number of actual implementations based on these protocols that meet some requirements and are practical for large-scale elections. Nevertheless, some of the prerequisites defined in the theoretical analysis of these protocols can be unrealistic to achieve in practice.

Besides, when comparing the efficiency of voting schemes, one needs to refer to some "reasonable" parameter values. The most important parameters are the number of voters N and the number of options of multiple option question L. Other parameters are the number of authorities M and the trust threshold t. So the suitability and usability of each protocol varies and depends a lot on these actual numbers.

5 Discussion

Internet voting is definitely a big step ahead to a technologically advanced world. Its adoption and use for small or large-scale elections has both advantages and disadvantages. For the moment, we believe no one should seriously claim that Internet voting could replace the traditional voting system. It should be regarded and treated, however, as an optional alternative that is easy, fast, cheap and practical, and would make it easier for some people to vote (handicapped, people living abroad, frequent travellers) without inconveniencing anyone else.

There is a large gap between making a theoretical approach to Internet voting and putting these considerations into implementation. A number of practical issues (technical, socio-political etc) have to be resolved before Internet-based elections can become a reality, otherwise the integrity of the voting process would be put under risk. A wise move would be to experiment by making trial elections in order to gain valuable experience prior to large-scale implementation. Only when an adequate security-conscious hardware and software infrastructure is available and the social science issues are addressed should Internet voting be deployed. However, despite these practical concerns if scientists and experts keep researching the issue, it is possible that advances in technology may enable Internet voting quite soon in the future.

5.1 Technical Problems

One category of problems related to Internet voting concerns the technical problems. All existing Internet voting protocols are based on the existing framework of Internet, computer hardware, computer software and cryptography. Therefore, all the weaknesses and vulnerabilities of those are transferred to the voting protocol as well, like the insecurity of the Internet (trojan horses, trapdoors), hardware limitations and others. An e-voting protocol can ensure vote secrecy only within its own (execution) boundaries. Computer security flaws (e.g. keyloggers, phishing scams against the Internet voters etc) could reveal the votes of specific voters, no matter what voting protocol they use. Furthermore, the result of an electronic election could easily be manipulated by disrupting the access of selected geographical or other groups of voters (which are likely to vote for party X) to the Internet or the Internet voting system, e.g. through power outages or communication lines outages. Internet voting protocols do assume that the workstations of the voters are available and secure, and that there is guaranteed Internet access to the electronic voting system.

Another technical issue we need to comment on are the standards. The introduction of Internet voting would ask for the establishment of new relevant standards concerning the voting platform, security and benchmarks.

5.2 Public Acceptance

Public acceptance relates a lot to the fact that people do not understand the technology of the Internet and how computer systems work. It is reasonable, therefore, that Internet Voting is mostly acceptable by those members of the public who have the greatest access to and familiarity with the Internet. Undoubtedly, the public acceptance of electronic voting is an important issue that must be addressed in order to make it a viable solution in the future.

5.3 Socio-Political Issues

Before implementing an electronic voting scheme and putting it into practice, it should be decided whether it would be useful at all. Certain issues would need to be resolved, for example, new sections of law would have to be created to punish illegal e-voting behaviour. Without an established legal framework for electronic election procedures we could end up harming democracy and staining the voting process.

5.4 Cost

An important factor in determining whether to implement Internet voting systems is the benefits that derive from it, with respect to the cost for their implementation. This cost includes the expenditure associated with system acquisition, implementation, technical support and upgrades for the life cycle of the systems. This cost is not really known at the moment but it is believed to be very high as electronic voting devices, digital signatures or other cryptographic components and technical support cost a lot.

5.5 Balancing Security and Other Interests

While a major consideration when talking about Internet voting is security and privacy, on the other hand there is a need for additional requirements to be fulfilled. There is often a trade-off between the goals for an efficient voting scheme. For example, for the sake of privacy we can sacrifice convenience, which is one of the basic advantages of the electronic technology. Modern means to enhance security can be used (e.g. smart cards, biometrics) that make the unfamiliar users feel inconvenient using them.

6 Conclusions

A voting protocol needs to satisfy a number of security requirements and meet some characteristics in order to be acceptable. This is, however, very complex and maybe even impossible. While elections may meet many of these criteria, they often do not need to meet all of them.

We presented some of the security requirements of an electronic voting system but this set is by no means complete. There are other attributes electronic voting systems need to satisfy also. For example, voting systems must conform with whatever election laws may be applicable, must not be shared with other applications running concurrently, pre- and post-election testing must take place.

One of the biggest arguments in favour of electronic voting is the increase in the access to the democratic process that it would offer [E-Vote, 2003]. Although nowadays none of the barriers which were erected between citizens and their right to vote in the past exist anymore, there are still barriers to voting communities such as the fact that people with limited knowledge of technology or handicapped voters must have equal access, to mention but a few.

A voting system must be realisable and feasible. The above considerations have a substantial interaction and many trade-offs among them. For example, efforts to improve security generally increase costs, reduce convenience and flexibility, and complicate implementation. We need to examine all these aspects before we can start using electronic voting more widely.

Electronic voting is definitely an application with a vision to the future. Its popularity is likely to rise over time as public access to the Internet approaches the levels of home telephony and television usage. Besides, the World Wide Web has already become integrated in our daily lives. At the same time, electronic voting is said to be probably the most promising application of cryptography. Nevertheless, a lot of work needs to be done before an electronic voting scheme can be accepted for a large-scale election. This work can be generally divided into three parts: scientific, technical, and socio-political.

Acknowledgments

We wish to thank the reviewers for their valuable comments.

Biographies

John Iliadis holds a Bsc in Information Systems Engineering from the Department of Informatics, Technological Educational Institute of Athens Greece, and an Msc in Information Security from the Royal Holloway College, University of London, UK. Mr Iliadis is currently a Network Security Administrator with TEIRESIAS Banking Information Systems, Greece and he is also pursuing a PhD in PKI with the Department of Information and Communication Systems Enginering, University of the Aegean. His interests include Information and Communication Systems Security, Computer Security and Distributed Systems Security. His published scientific work includes more than fifteen (15) journal and international conference papers.

Eleni Tsekmezoglou holds a Bsc in Computer Science from the Department of Informatics, University of Piraeus, Greece. She also holds an Msc in Information Security from the Royal Holloway College, University of London, UK. Mrs Tsekmezoglou is currently an Information Security Consultant with the Banking & Enterprise Solutions Division, Intracom S.A., in Athens, Greece. Her interests include information security strategy, information risk assessment and risk management, development of information security management systems.

References

Adler J., 2000, “Internet Voting Security”, VoteHere.net, January

Banerjee U., 2002, Enforcing security with Biometrics, pp. 12-13

Benaloh J., 1987, Verifiable Secret-Ballot Elections, Ph.D. Thesis, Yale University, Department of Computer Science, New Haven, CT, September

Benaloh J. & Tuinstra D., 1994, “Receipt-Free Secret-Ballot Elections”, Proc. 26th ACM Symposium on the Theory of Computing (STOC), ACM, pp. 544-553.

Cramer R., Franklin M. K., Schoenmakers, B. & Yung, M., 1996, “Multi-Authority Secret-Ballot Elections with Linear Work”, Advances in Cryptology, EUROCRYPT ’96, Springer-Verlag, May, pp. 72-83.

Cramer R. Gennaro R. & Schoenmakers B., 1997 “A Secure and Optimally Efficient Multi-Authority Election Scheme”, European Transactions of Telecommunications, pp. 103-118.

Chaum D., 1981, “Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms”, Communications of the ACM, 1981, pp. 84-88.

Chaum D., 1988, “Elections with Unconditionally Secret Ballots and Disruption Equivalent to Breaking RSA”, Advances in Cryptology EUROCRYPT ‘88, .G. Gunther (Ed.), Springer-Verlag, pp. 177-182.

E-Vote, 2003, “Secure Electronic Voting”, Dimitris Gritzalis (Ed.), Kluwer Academic Publishers

Dastjerdi, A., Pieprzyk, J., Naini, S., A Review Study on Electronic Election, The Centre for Computer Security Research, Department of Computer Science, University of Wollongong, Australia, June 2, 1994.

Fujioka A., Okamoto T. & Ohta K., 1992, “A Practical Secret Voting Scheme for Large-Scale Elections”, Advances in Cryptology, AUSCRYPT ’92, Springer-Verlag, pp. 244-260.

Hirt M. & Sako K., 2000, “Efficient Receipt-Free Voting based on Homomorphic Encryption”, Eurocrypt, pp. 1-2.

Mitrou, L., Critzalis, D., Katsikas, S., Quirchmayr, G., 2003, “Electronic Voting: Constitutional and Legal requirements, and their technical implications”, in Secure Electronic Voting, Gritzalis, D., Ed., Kluwer Academic Publishers.

Okamoto T., 1996, “An Electronic Voting Scheme”, Proc. IFIP ’96, Advanced IT Tools, Chapman & Hall, pp. 21-30.

Okamoto T., 1997, “Receipt-Free Electronic Voting Schemes for Large-Scale Elections”, In Proc. Of Workshop on Security Protocols ’97, vol. 1361 of LNCS, Springer-Verlag, pp. 25-35.

Sako K., 1994, “Electronic Voting Schemes allowing Open Objection to the Tally”, Transactions of the Institute of Electronic, Information and Communication Engineers.

Schneier B., 1996, Applied Cryptography, John Wiley & Sons, New York.

Sako K. & Kilian J., 1994, “Secure Voting using Partially Compatible Homomorphisms”, Advances in Cryptology, CTYPRO ’94, Springer-Verlag, pp. 411-424.

Sako K. & Kilian J., 1995,, “Receipt-Free Mix-Type Voting Scheme – A Practical Solution to the Implementation of a Voting Booth”, Advances in Cryptology, EUROCRYPT ’95, Vol. 921 LNCS, Springer-Verlag, pp. 393-403.

Hutter, D., Volkamer, M.: From Legal Principles to an Internet Voting System (July. 8th, 2004), in Electronic Voting in Europe - Technology, Law, Politics and Socierty (Workshop of the ESF TED Programme together with GI and OCG; July 7th-9th, 2004 in Schloss Hofen/Bregenz, Lake of Constance, Austria)

Will M., 2002, Internetwahlen - Verfassungsrechtliche Möglichkeiten und Grenzen, Institut für Öffentliches Recht Philipps, Universität Marburg, Richard Boorberger Verlag GmbH & Co, Recht und neue Medien Band 2.