Electronic Voting System: Preliminary Study

Subariah Ibrahim (subariah@fsksm.utm.my)
Mazleena Salleh (mazleena@fsksm.utm.my)
Maznah Kamat (c-mazna@utmjb.utm.my)

Department of Computer System and Engineering
Faculty of Computer Science & Information System
Universiti Teknologi Malaysia

Abstract

Election is a democratic process that allows a citizen to vote for a ruling government. This paper first reviews the evolution of a voting system and how an election process is carried out. It then focuses on the discussion of the security requirements for a reliable electronic voting system and how these requirements are implemented in several EVS. This paper also compares the implementation of electronic voting system with a traditional voting system.

Key words: security, cryptography, blind signature,

1.0 Introduction

One of the fundamental rights as a citizen of a democratic country is the right to vote for the ruling government. It is an instrument of democracy that provides an official mechanism for people to express their views to the government. Traditionally, the process of voting in local and national elections is cumbersome because the voter himself must be present in person at the polling station to cast his vote. The task of conducting the election is even more difficult when voters are geographically distributed. Additional to this, the mechanism that is needed to ensure that the security and the privacy of an election are maintained at all times during elections can be expensive and time-consuming for the election administrators. Most national elections are designed to minimize the possibility of fraud and maximize public confidence. This is done by inviting independent parties or representatives from each party to observe the election process and by assuring the anonymity of the voter's ballot. In addition, they are decentralized so that any fraud, which may occur, is unlikely to compromise the process as a whole.

However with the rapid growth of network technology and advancement in cryptography techniques, electronic voting system (EVS) can be designed to overcome the problems of traditional voting and thus becomes a viable alternative method of survey or voting in an election. EVS is viewed as a set of protocols that allow voters to cast their votes, while enabling authorities to collect and tally the votes, and announce the result to the public. EVS is expected to make our modern social life more convenient, efficient and inexpensive.

In this paper we review the evolution of voting system, the election process as well as the security issues that are related to electronic voting. We also survey several implementations of electronic voting system.

2.0 Evolution of Voting System

Voting is an exercise of stating one's opinion or decision of expressing satisfaction or dissatisfaction with government. There are various methods of voting and the oldest and most common form is a "voice vote" whereby a voter simply responds loudly with an appropriate "yes" or "no" to the issue in question. Ancient Greeks used colored stones for voting: white stones to indicate "yes" while black stone to indicate "no". Instead of stones, the ancient society of Florence and Venice, used colored balls called ballota to vote and this is where the word "ballot" comes from [1]. Clearly the voting techniques above do not consider the secrecy of voting as an important issue.

As time and situation changes secrecy has become an important issue in voting. This is necessary so as to protect the voter from undue influence, persuasion, coercion and bribery during voting. It is also to protect the voter's right to express his opinion. This leads to another method of voting known as the Australian Ballot System. The system is commonly used today during election in many parts the world. Under this system, a voter enters a booth alone and marks his selected candidate on the ballots at a centralized voting station. The ballot is usually a white uniform sized paper that contains all the names of candidates to ensure that each voter is selecting from the same list of candidates. At the end of polling, only valid ballots are tallied manually.

New methods of tallying the ballots are then introduced. These new methods of voting have common criteria: cheap to build and maintain, easy for the voter to use, fast and accurate to count the ballots. In addition the voting method can ensure the secrecy and honesty of the vote. One of these methods utilized mechanical machines that consist of a series of levers that a voter pull to cast his vote. Once the vote is registered, the levers physically increment mechanical rotary counters. Upon closing the poll, the backs of the voting machines are opened to reveal the vote tallies.

Unlike mechanical voting machines, machine-readable voting equipment or punch card system used computer-readable ballots. A voter is required to mark his vote on a paper card with a pencil or marker, or remove divots from perforated card with a stylus or mechanical hole puncher. The ballot cards are collected at the end of the poll and then scanned through by a computer for tallying. This system has been criticized for its vulnerability towards tampering and it is difficulty to use. To ease the procedure of marking the ballot, direct-recording voting machines are used whereby a voters cast his ballot on a computer terminal using keyboard, touch screen or pointer. The votes are immediately added to the tally.

In all the implementations mentioned above, voting are done at centralized voting station. This can results in a low rate voter turnout. Vote-by-mail aims to increase the rate of voter's participation especially in sparsely populated area. Beside the convenience provided by vote-by-mail method, a voter has more time to case a ballot. Thus the voter does not feel rushed to make his decisions. However, vote-by-mail is time consuming and cumbersome for the authority to manage since it requires extra work to send, collect and count manually the ballots. Televote is another method aiming to get a bigger participation of voters. However unlike vote-by-mail, it simplify the process of counting and tallying. In this mechanism information that includes voting instructions and a secret televoter number is mailed to the voter. During the election, a voter will make a telephone call to the televote computer. The voter then enters his televote number and a code corresponding to his choice of the ballot. Ballots are collected from each voter and are saved in a magnetic tape. At the end of polling period, the ballots are tallied by a computer.

The advent of computer and networking has enabled a step further in voting mechanism whereby voting is done digitally, hence it is known as EVS. In EVS, voting is done at a personal computer and ballots are transferred to a central system through a communication channel. The ballots are processed automatically at the receiving end without human intervention. With the employment of cryptographic techniques in EVS, secrecy and other properties, example verifiability and authenticity, which are not generally obtainable in traditional voting system can be implemented.

EVS may become a viable alternative for many elections and surveys. With the widespread use of Internet, EVS can be convenient for the voters who has easy access to the network, even if the voters are geographically distributed. In addition, it can reduce the workload in managing the election.

3.0 Election Process

The basic procedure for conducting a democratic election is generally the same for any voting system. Normally, this procedure involves four main tasks, that is, registering of eligible voters, validating voters' credentials, collecting voted ballots and tallying the ballots. In addition to the tasks above, there are several other tasks that need to be carried out prior to the election day by the election authority. This includes the determination of the boundary of each precinct, duration for voters' registration, election date for voting and duration for nomination of candidates.

In order for an individual to be eligible to vote on the election date, he must register himself to the election authority. During the registration, eligibility criteria set by the authority, for example age and citizenship, will be verified for each voter before his name can be recorded in the registration list. The list of registered voters will then be produced for public viewing so that any discrepancy can be challenged.

On an election day, a voter will be verified before he is allowed to cast his vote. During this task, the credentials of the voter will be validated by using the voters' registration list. At the same time the task will also keep track of who has voted to prevent multiple casting of votes by a single voter. After the credentials has been validated then the voter can cast his vote. The election authority will then collect the votes and then tallied. Once the election result is certified, the election result will be announced to the public.

The most important issue in any election is the security of the election process, starting from the task of the voter's registration to the tallying of the cast ballots. To gain public's confidence in election results, people must believe that every process in the election procedure is conducted with high security measures. Without these measures, numerous opportunities for a widespread fraud and corruption may exist. There are several ways on how the election process can be manipulated. For example, phantom voters may exist in the registration list by registering under the name of a deceased person. Election result can be compromised when a particular party colludes with election authorities in order to win the election. In some fraud cases, a person can impersonate as a registered voter at the polls to increase the number of votes for his chosen candidate. Therefore security is vital in an election process in order to prevent such fraud. To overcome these problems, an election should have the following requirements: the confidentiality of the cast ballot, authenticity of the voter, the integrity of the result and verifiability of a voter's ballot.

So, how does EVS differ from traditional voting? Generally the process is the same for both electronic and traditional voting. However the security implementation in EVS is different from the one implemented in traditional voting. The whole process of EVS, which includes registration, verification, voting and tallying of ballots are done digitally. In EVS, there is no physical ballot. As the ballot is transferred through the computer network, it is open for manipulation, thus harming the integrity of the election as well as the confidentiality of the ballot. In contrast conventional voting uses physical measures to counter security problems. For examples, paper ballots are used as an audit trail for verifying the results and independent observers are invited to observe the whole election process to minimize the possibility of fraud and conspiracy.

4.0 Security Issues of EVS

EVS is more vulnerable than traditional voting due to the nature of digital processing of election data which can be easily manipulated, hence may result in widespread fraud. Therefore, specific security measures must be included in designing EVS in order to achieve the same level of security as the conventional election.

In electronic voting literature [2][3], an extensive list of properties and requirements is discussed. Here we summarized the core requirements that are desirable in any election system and it can be categorized into four aspects:

(i) Confidentiality
(ii) Integrity
(iii) Authentication
(iv) Verifiability

The voter's ballot should be kept confidential. No one, including the election authority should know for whom a voter votes and a voting protocol must not allow any voter to prove that he or she voted in a particular way. This is important to avoid opportunity of vote buying and extortion.

In electronic voting, there is no physical ballot. The digital ballot can be tampered with ease, given the insecure nature of current computer networks. Hence, with digital ballot system, the integrity of receipt by the computer of the voter's choice is a great issue. The published results should measure how the eligible voters actually vote. To achieve the integrity of the EVS, the protocol must ensure only valid votes are counted in the final tally and no one can change anyone else's vote without being discovered.

If every process in the voting procedure were to be implemented electronically, a person will need to register himself by using a computer. If this is implemented through a network, then there must be some form of verification in order to validate that a person is someone he claims to be. During voting, EVS must provide an authentication mechanism that ensures that a voter who is allowed to vote must be an eligible voter and he is a person he claims to be. Therefore during registration, some form of credential or ticket must be given to a voter so that it can be used to authenticate him during voting.

Another issue that must be considered and preserved in any democratic election is the notion of one-person one vote. EVS must provide a mechanism to check this notion. The authentication mechanism that is employed in EVS must ensure that a voter who is

allowed to vote is an eligible voter. In addition, the mechanism must also check that a voter has not already cast a vote in order to prevent double voting.

Verifiability can be categorized into two: individual and universal verifiability. Individual verifiability means a voter can check that his vote was properly received and has been taken into account in the final tally. While a universal verifiability means anyone can verify at a later time that the election was properly performed [4]. Universal verifiability allows auditing by the public and therefore anyone can verify that all votes have been counted correctly. In manual voting, paper ballots allow universal verifiability of election results.

4.1 Implementation of EVS Requirements

Cryptographic techniques such as encryption and decryption can be used to secure electronic data in order to provide integrity and confidentiality of data as well as authenticity of the sender. Many of the proposed electronic voting system employ some cryptographic techniques to achieve EVS requirements. In this paper we review the implementations of discussed requirements in (4.0) in eight different EVS and compare them with traditional systems.

Election authority is an important entity in providing the security needed in election process. In traditional system, the authority determines and implements the election protocol in orders to achieve a certain level of security required in the system and therefore must be trusted completely. In EVS, several approaches, from a single authority to multiauthority, has been designed to mimic the election authority. One Agency Protocol uses a single authority while Two Agency Protocol, Fujioka, Sensus [2] and Davenport, et. al. [5] entrust two authorities, namely, a validator and a tallier, whereby each authority plays a different role. Evox implementation employs several authorities which comprises of a commissioner, a manager, an anonymizer, a counter (same role as tallier) and *n* administrators (same role as validator). A commissioner does not play much role except for receiving any complaints that violate the voting protocol. A manager's function is to distribute the ballot to voters and sign it after the voter cast the ballot and concatenate it with administraors signature. The manager's signature is used to detect if a voter double. Unlike other protocols, Cramer et. al. presented a different approach whereby it uses n-authority with the same role [2].

Multi-authority is a better choice than a single authority because a dishonest administrator in a single authority may exploit his power and thus publish election results in his favor. A dishonest single administrator may create phantom voters, cast a vote for abstaining voters, allow some registered voters to cast more than once or even miscount the ballots. The two-authority protocol is better than a single authority. However, a collusion problem may arise as in Two Agency Protocol since the validator knows whom the identification tags belong to while the tallier knows the ballot and the corresponding identification tags. With multi-authority scheme, a protocol can be designed in such a way so that each authority will not get all information about the ballot, thus no authority can trace whom the ballot belongs to. The bigger the number of authorities, the more secure the election protocol will be.

Authentication procedure is essential in any voting system so that only registered voters are allowed to cast a vote. In traditional voting, a voter has to come in person and present an ID in order to vote and the election authority manually verifies him and uses (matches the ID with) the voters' registration list to check his eligibility before giving him

a blank ballot. The authority must also note that he voted in order to prevent double voting. In EVS, this procedure has to be done digitally over the network and therefore the security is more crucial. Two Agency Protocol issued identification tag that is given to the user when he registered to vote. This tag is then used to verify him during voting [2]. Most other protocols used some form of identification as well as public-key cryptosystem for authentication. However, public-key cryptosystem is not only used to verify the voter, but also to verify the authority. In this case, the voter can ensure that there is no bogus authority and in the case of multi-authority protocol, the 'counter' can validate that the ballot is signed by the right validator.

In traditional voting, the privacy and integrity of voter's ballot is protected as a voter cast his vote at a polling booth and drops his ballot into the ballot box himself. Many electronic voting systems employ cryptographic techniques to provide confidentiality of the voter's ballot. The most popular technique is a blind signature which [2][4][5][6] was first proposed in 1982 by Chaum. Fujioka used the technique in his EVS to solve the collusion problem that exist in Two Agency Protocol [2]. Since then, most protocols employ a blind signature in their EVS implementations. A blind signature is used to authenticate the voter without disclosing the content of a ballot. Hence the authority whose function is to verify the eligibility of a voter will not know whom a voter votes for.

In traditional system, paper ballots are used as an audit trail and therefore recounting of ballots is easy and hence the election results can be verified. In electronic voting, to achieve verifiability, the results and the collected ballots are published for public viewing. Sensus provides both individual and universal verifiability by publishing a list of encrypted ballots, decryption keys and decrypted ballots after the election. With this published list a voter can verify that his vote was properly received. Two Agency Protocol developed by Nurmi also provides both individual and universal verifiability. However, Two Agency Protocol publishes a list of voted ballots and the corresponding encrypted files containing the identification tag and the ballot. The mechanism used by both Sensus and Two Agency Protocol may result in vote buying and coercion. Two Agency Protocol even allows the voter to correct any mistakes in their ballot after the election, thus making it more feasible for vote buying and coercion [2]

Table 1 summarizes the EVS requirement in several EVS implementations as discussed above.

4.2 Implementation of Blind Signature Protocol in EVS

A blind signature is similar to a digital signature except that it allows a person to get another person to sign a message without revealing the content of a message. In EVS, a ballot is blinded in order to achieve its confidentiality requirement. For simplicity, a protocol with two authorities, mainly a validator and a tallier are used to demonstrate how a blind signature is employed in EVS. A voter is required to get the signature of a validator when he votes. To ensure the secrecy of his ballot, a voter cast a ballot, B, blinds a vote using a random number and sends it to the validator. Let (n,e) be validator's public key and (n,d) be his private key. A voter generates a random number r such that gcd(r,n) = 1 and sends the following to the validator:

$$B' = r^e B \bmod n.$$

Table 1 Properties of Various Electronic Voting System

	Nurmi (1991)	**Fujioka (1992)**	**Davenport et.al. (1995/7)**	**Radwin (1995)**	**Cranor (1996)**	**Cramer et. al (1997)**	**Du Rette (1999)**
Double Vote Prevention	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ballot Confidentiality	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Universal Verifiability	Yes	Yes	Yes	Yes	Yes	Yes	Yes
No. of Authority	2 authorities	2 authorities	2 authorities	1 authorities	3 authorities	n-authorities with the same roles	n-authorities with different roles
Non Manipulability	No	No	No	No Conclusion	No	No	No

The random number r conceals the ballot from the validator. The validator then signs the blinded ballot after verifying the voter, the signed value is,

$$S' = (B')^d = (r^e B) \bmod n$$

After receiving the validated ballot, the voter unblinds the ballot, to get the true signature of a validator S by computing,

$$S = S' r^{-1} \bmod n$$

The voter then sends his ballot together with the validators' signature to the tallier. The tallier verifies that if the ballot was correctly validated, then the ballot is valid. Figure 1 illustrates the employment of blind signature in EVS.

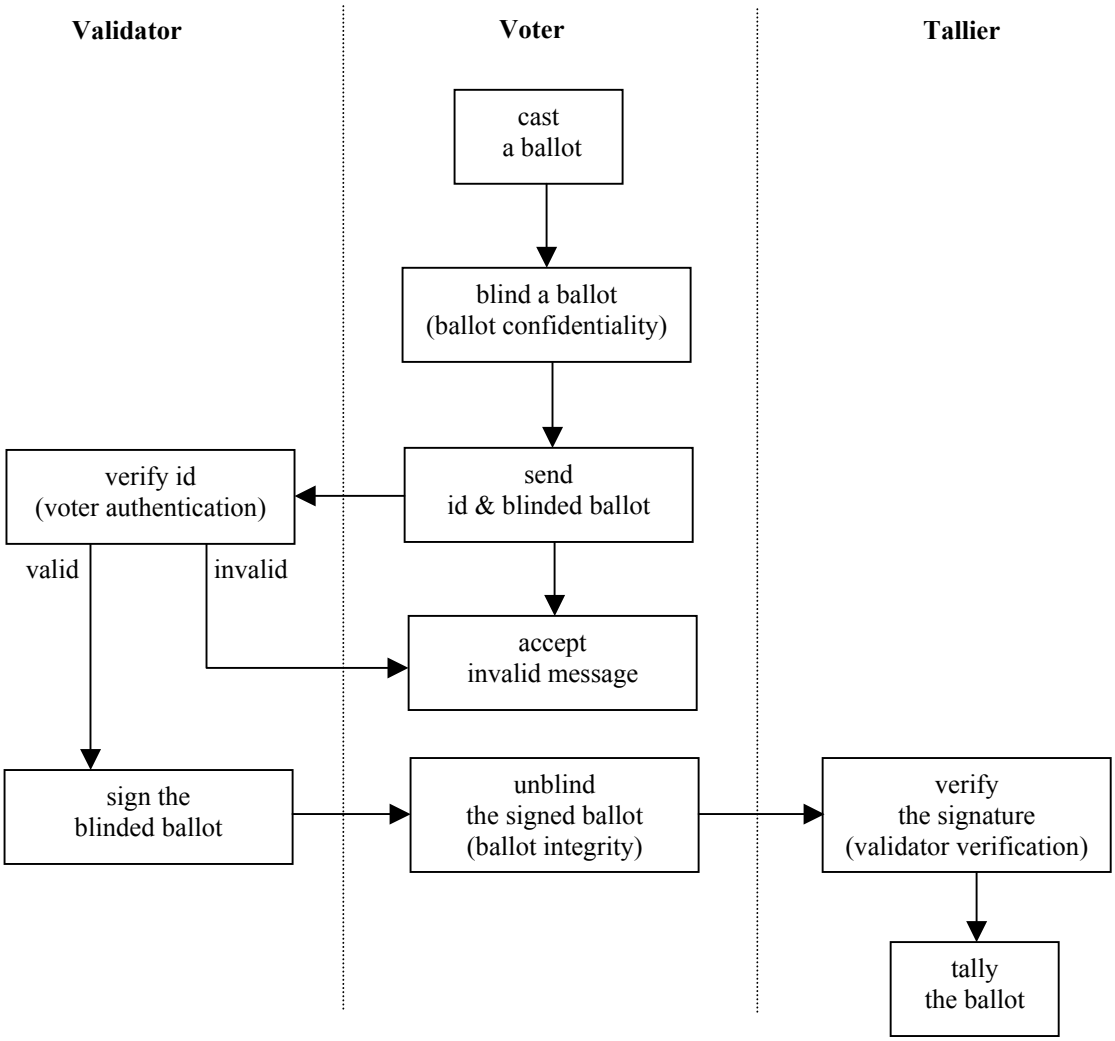

Figure 1 Conceptual View of Blind Signature Protocol in EVS

5.0 Conclusion and Future Directions

This paper focuses on the security issues of EVS. Like in traditional election systems, EVS also maintain important issues of confidentiality, integrity and authenticity when designing the system so that it cannot easily be compromised. In addition to these issues, EVS can also provide verifiability of the result, which is not generally obtainable in traditional voting systems. Thus it provides full reliability of the election results and making it impossible to forge the results. Moreover there are several benefits that EVS can provide which include paperless voting, automatic counting of the voting results, prevention of illegal voting and consumed less time for managing the election.

EVS is suitable for campus elections and now has become increasingly popular due to the easy accessibility of computers on campuses. The use of EVS can be extended to a large-scale election such as the national election provided the design of the system include all the security requirements and the program developer and administrator can be trusted. But if the system does not meet any of these requirements then the election as a whole will be compromised.

Based on this preliminary study, we will develop multiauthority electronic voting system for campus election. The system to be developed will consider all the security requirements needed for secure electronic elections. Besides using blind signature protocol we will also consider other cryptographic algorithms such as Diffie-Hellman key exchange, SHA-1 and additional authentication mechanisms.

Biblography

1. http://www.sos.state.tx.us/funstion/projecttv/pvote/

2. Cranor, L.R and Cytron R.K. " Design and Implementation of a Practical Security-Conscious Electronic Pollind System", Washington University Computer Science Technical Report, wucs-96-02, Febuary 1996.

3. Cramer, R., Franklin, M., Schoenmakers, B. and Yung, M. "Multi-Authority Secret-Ballot Elections with Linear Works", 1996, Eurocrypt '96, LNCS 1070, pp 72 – 83.

4. Radwin M.J. "An Untraceable, Universally Verifiable Voting Scheme". Seminar In Cryptology, 1995

5. Davenport, B., Newberger, A. and Woodard, J. "Creating a Secure Digital Voting Protocol for Campus Election".
   http: // www.princeton.edu/~usgvote/techenical/paper. 13 – 06 – 99

6. DuRette, B.W. "Multiple Administators for Electronic Voting".
   http: //thoery.lcs.mut.edu/~cis/voting/voting.html

7. Waskell, E. "Overview of Computers and Election", CEP 1993
   http: //www.cpsr.org/conferences/cfp93/waskell.html. 16/06/99

8. Cranor, L. "Electronic Voting: Computerized Polls May Save Money, Protect Privacy".
   http:// www.acm.org/crossroads/xrds2-4/voting.html. 17/05/99

9. Shamos, M.I. "Electronic Voting – Evaluating the Threat" http: //www.cpsr.org/conferences/cfp93/shamos.html

10. Lei, C.L. and Juang, W.S. "A Collision-Free Secret Ballot Protocol for Computerized General Elections". Computer & Security Vol 15, No. 4, pp339 – 348, 1996.

11. Lin, R.H. and Jan, J.K. "A Secure Anonymous Voting by Employing Diffe-Hellman PKD Concept". IEEE 1995.

12. Horster, P., Michels, M. and Petersen, H. "Blind Multisignature Schemes and Their Relevance to Electronic Voting". Department of Computer Science, Theoretical Computer Science and Information Security, University of Technology Chemnitz-Zwickau. Technical Report TR-95-16-F, August 1995.

13. Pointcheval, D. and Stern, J. "Security Arguments for Digital Signatures and Blind Signatures". Journal of Cryptology, 1998.

14. Pfleeger, C. P. Security in Computing. Prientice Hall, 1989.