

A Brief Study of the Concept of E-Voting

Neeru Kamboj^{1*} Dr. Omprakash²

¹Research Scholar

²Associate Professor, OPJS University, Churu, Rajasthan

Abstract – This paper gives the explanations of the term “e-voting”. The term “e-voting” is used, in variety of different ways mainly and it encompasses all voting techniques involving electronic voting equipment, including voting over the internet, using booths in polling stations and sometimes even counting of paper ballots. Electronic voting (e-voting) is any voting method where the voter’s intention is expressed or collected by electronic means. There are considered the following electronic voting ways.

-----X-----

INTRODUCTION

Kiosk voting means the use of dedicated voting machines in polling stations or other controlled locations. Voters mark their choice electronically (perhaps on touch sensitive screen) rather than on paper ballot. The votes are counted on individual machines, known as Direct Recording Electronic (DRE) machines, and the votes cast are transferred to the central tallying point by unspecified means. A ballot paper can be printed and retained in confidence in a ballot box as an additional check.

Remote electronic voting is the preferred term for voting that takes place by electronic means from any location. This could include the use of the Internet, text message, interactive digital TV or touch tone telephone.

Internet voting (i-voting) is a specific case of remote electronic voting, whereby the vote takes place over the Internet such as via a web site or voting applet. Sometimes also used synonymously with Remote Electronic Voting. That usage is however deprecated and it will be used instead as a strict subset of remote electronic voting.

In this work, we use the term e- voting with the specific meaning of Internet voting. If we use it as a general term, then we specify the meaning.

SECURITY PROPERTIES OF E-VOTING

High security is essential to elections. Democracy relies on broad confidence in the integrity of elections. There has been a lot of attention to an electronic voting by cryptographers. Many scientific researchers have been done in order to achieve security, privacy

and correctness in electronic voting systems by improving cryptographic protocols of e-voting systems. Currently, the cryptographic schemes are not the main problem. The main interest is the practical security in e- voting systems. Which properties must be justified in order we could say that the system is secure for implementing? One of the main interests is seemingly contradicting security properties. On the one hand, voting must be private and the votes anonymous. On the other hand, voters must be identified in order to guarantee that only the eligible voters are capable to vote. Hence, e-Voting should be uniform, confidential, secure and verifiable. In the following, we define the most important requirements of e-voting.

1. **Eligible voters are capable to cast ballots that participate in the computation of the final tally.**
2. **Non-eligible voters are disfranchised.**
3. **Eligible voters are not capable to cast two ballots that both participate in the computation of the final tally.**
4. **Votes are secret.**

This is the property of privacy. This property is apparently contradicting property with correctness. On the one hand voting must be private and the votes that are counted anonymous. On the other hand, voters must be identified in order to guarantee that only the eligible voters are capable to vote.

5. **It is possible for auditors to check whether all correct cast ballots**

participated in the computation of the final tally.

This requirement says that a group of dedicated auditors or Electoral Committee can check the correctness of voting.

6. The result of an election must be secret until the end of an election.

The third party must not be capable to reveal the results of the election. Additionally, the system should guarantee that official votes' counting office cannot reveal the final tally before the end of voting. Otherwise, the result of voting could affect voters' decisions during the voting.

7. All valid votes are counted correctly and the system outputs the final tally.

8. It must be possible to repeat the computation of the final tally.

State of the art

In this chapter, we give a brief overview of different kinds of electronic voting systems. This list is not perfect; however it gives us a glance of how electronic voting is implemented in Europe and in the United States.

The main reasons for a government to use electronic elections are:

- to increase elections' activity by facilitating the casting of votes by voters;
- to reduce elections' and referendums' expenses;
- to accelerate vote counting and the delivery of voting results;
- to enable voters to cast their votes from different places, not from only a particular polling station.

The Internet voting system [22] was used in the national referendum in Geneva canton of Switzerland in 2004. In Switzerland, elections or referendums are held four or five times a year. There are 580.000 Swiss citizens living abroad, to compare with 7 million inhabitants in the country. It is important to provide them with an efficient and simple voting system. Approximately 52% of the Swiss population has Internet access, both at home and at the workplace. For all these reasons, the governments, both in Geneva and at the Federal level have decided to develop Internet-voting solutions.

The voting cards were sent to voters a few weeks before the voting day. The voting cards were smartcards with private keys validated by a local Public Key Infrastructure service provider. The voting cards were valid for voting operation only. Voters made their choices and confirmed these with the private keys and personal data (date of birth and place of birth). The votes were encrypted in the voting servers by using special public voting keys. The voting system separated voters' personal data and ballots to guarantee the principle of voting privacy. The political parties, in order to check democracy of the votes delivering process, share the keys for triggering votes' counting process.

By the polling of 2003, the 73% of the Swiss population support online Internet voting. However, the Internet voting system has been applied only in referendums. More than 80% of the voters want the system to be implemented for the elections too [22].

The remote voting system was applied in the European Parliamentary elections in the Netherlands in 2004. The target group consisted of the Dutch electors' resident abroad and electors resident in the Netherlands who are temporarily abroad on business on the Election Day and members of their family who accompany them. There was a registration procedure before the elections where eligible voters had to choose the way of elections: by post, by proxy holder, by Internet or by telephone. 41% of the eligible voters preferred the Internet voting system [18]. Nevertheless, the activity of Internet voting was not so high. The main reason why eligible voters did not vote electronically was that they did not receive the voting documents in time.

In the United States of America, there were many attempts made to use electronic voting systems. The project named Voting over the Internet (VOI) was one of them. VOI was used in the general elections of 2000 in four states (Florida, South Carolina, Texas and Utah). The votes given via Internet were legally accepted, but their amount was small (84 votes) [17]. VOI's experiment was so small that it was not a likely target of attacks.

Another Internet voting project named Secure Electronic Registration and Voting Experiment (hereafter SERVE) was developed for primary and general elections in 2004. The SERVE system would have allowed the eligible voters to vote via Internet [1]. The eligible voters of SERVE were mainly overseas voters and military personnel. The target group was 6 million voters. The US Department of Defence terminated the SERVE project in the beginning of year 2004 because a group of security experts had found that the SERVE system was not sufficiently secure.

The projects of the kiosk voting systems have been more successful in the USA. In these systems, like in the paper-based elections, a voter goes to one's home precinct and proves that he/she has a permission to vote there by presenting one's identity card. After that, PINs, smartcards, or some other tokens for authentication are given to voters. Having a token, a voter is able to cast a vote by using a direct recording electronic machine [19].

A public opinion poll held in 2004 showed that 68% of American voters had supported kiosk voting systems while 15% were against it. On the other hand, the positive trust in relation to remote voting systems was 32% and negative attitude was 47% [21].

In Great Britain, many different electronic voting methods have been experimented since 2002, for example, polling booth, telephone, SMS, remote electronic voting via Internet and digital television. Remote electronic voting systems were used in the local election in 30 municipals in 2003. There were 27% of the voters who voted electronically (146 000 votes) [20]. The majority of all the voters are in favor of Internet voting while only a small group of the voters is against it. Many non-voters are against it too. Even though many eligible voters would not use e-voting methods by themselves, there was a widespread support for making it available to the others.

In 2004, there was an intention to develop the e-voting systems for the European Parliamentary elections and local elections. However, in spring 2004 the decision was made to terminate the development of e-voting systems and concentrate on the voting system via post. The decision was influenced by recommendations of the American security experts, which caused the termination of the Secure Electronic Registration and Voting Experiment project (SERVE).

Estonia has been developing an online Internet voting system since 2003. There were many political discussions whether to allow the implementation of an e-voting system. The Estonian e-voting system was involved in the municipal elections in autumn 2005. On the other hand, a public opinion poll said that general support to e-voting is 73% of voting age inhabitants [13], but the real result was 1.8% e-votes of all votes. There were not successful attacks against the e-voting system. The target group of the e-voting system was 1 million voters.

The security experts are more skeptical about e-voting than the public. Their greatest worries are not related to malicious attacks against e-voting servers, but the system and programming errors and the security of private computers. Another complicated problem seem to be the contradicting properties of correctness and privacy harmony. Additionally, a majority of countries

does not apply e-voting to all citizens, but solely to electors' resident abroad. This property expresses also some kind of unreliability.

DESCRIPTION OF E-VOTING SYSTEMS

This chapter presents the detailed descriptions of an e-voting system. In the beginning, we describe how e-voting systems work. Next, we give the descriptions of the Estonian e-voting system and the Internet voting project Secure Electronic Registration and Voting Experiment (SERVE) in the United States of America. Finally, we point out the main differences between the two e-voting systems.

There are many other relating phases, which were not mentioned. To list some: storing and managing the list of candidates, key generation and management, storing and managing the list of eligible voters, the installation of system initial position, taking down and archiving the system. For the sake of simplicity, we assume that all these phases are secure, and work properly.

REFERENCES

- A. Ansper, A. Buldas, M. Oruaas, J. Piirsalu, A. Veldre, J. Willemson, K. Kivimurm (2003). The Security of Conception of E-voting: Analysis and Measures. E-hääletamise kontseptsiooni turve: analüüs ja meetmed. 2003.
<http://www.vvk.ee/elektr/docs/Analüys-01.pdf>. 21.01.2007.
- A. Buldas, P. Laud, J. Piirsalu, M. Saarepera, J. Willemson (2006). Rational Choice of Security Measures via Multi-Parameter Attack Trees. In Critical Information Infrastructured Security First International Workshop - CRITIS 2006, LNCS 4347, pp. 235-248, 2006.
- D. Jefferson, A.D. Rubin, B. Simons, D. Wagner (2004). A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE). 2004.
<http://www.servesecurityreport.org/>. 21.01.2007.
- Estonian National Electoral Committee home page, www.vvk.ee. 21.01.2007.
- Estonian National Electoral Committee. General Description of the E-voting
<http://www.vvk.ee/elektr/docs/Yldkirjeldus-02.pdf>. 21.01.2007.

System. E-hääletamise süsteemi
üldkirjeldus. 2004.

Corresponding Author

Neeru Kamboj*

Research Scholar

E-Mail –