ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
December 2012,
Vol. 5, No. (2):
Pgs. 161-168

A Secure and Robust Prototype for Electronic Voting System

ASHRAF DARWISH, MAGIDALGENDY and EMAN MOHAMED

Faculty of Science, Helwan University, Cairo, Egypt.

(Received: November 05, 2012; Accepted: November 25, 2012)

ABSTRACT

Electronic voting (EV) refers to the use of computers or computerized voting equipments to cast ballots in an election EV has been in development for more than 20 years, during which it has produced outstanding results both in theory and in practice. This paper presents a new secure preferential e-voting scheme. In this paper we will present an e-voting scheme that covers most of the e-voting requirements were implemented to guarantee voter's privacy and authentication. A prototype implementation of EV protocol over the Internet which fulfils some electronic voting system requirements such as efficiency, transparency and mobility has been presented.

Key words: Electronic voting, Cryptography, Blind signatures.

INTRODUCTION

Varity kinds of application technologies are tending towards digitization, such as e-commerce, e-democracy, or e-government, etc due to the rapid development of technologies and popularity of the internet.

To minimize costs and red tape in public departments, the contemporary states are seeking to provide people have the ability to participate and benefit from online services by increasing the number of activities associated to this new medium.

Electronic voting is one of the most important Internet-related activities. Recently the contemporary states moved to electronic voting instead of a traditional one for more than one reason for example: (1) use of electronic voting has the ability to reduce or eliminate undesirable human errors, (2) in addition to its reliability, e-voting does not need geographical proximity of voters which increase the number of participating voters, (3) e-voting saves a lot of time for voters and reduce a cost when counting the voted ballots.

Different electronic voting systems have been suggested to support elections and voting namely

Computer counting

Is a way that enables voters to mark their choice on a paper with a pencil or marker. Then ballot cards are examined and counted in a central computer site.

Direct-recoding electronic voting machine (DRE)

Is an implementation of an electronic voting system. Where the voter chooses the candidate by marking the choice of possible options on the electronic storage device. All votes are stored on a memory cartridge, smart card, or a floppy disk. Then they moved to a central location to be counted and get the result.

On line-voting: this system encompasses three types

Poll Site Internet Voting: this kind of election requires the presence of the polling stations where voters go there to cast their ballots by using suitable computers and the officials supervise the election. At counting stage, a network is used to transfer ballots from each polling place to a center location, where votes are counted and election results are posted.

Remote e-voting system: indicates casting of ballots from any computer or digital device connected to Internet. This type of open network is related to neither time nor place but the associated risks are great.

Kiosk e-voting system: in this model, polling station were controlled by election officials where located in suitable locations such as offices, schools, etc .The observers oversee and cameras monitor the kiosk voting to overcome the security vulnerabilities and prevent coercion. Challenges related to kiosk voting system are considered less threat than those associated with remote voting.

At the present time electronic voting has become more popular in all over the world. Some countries that used electronic voting are: the United States of America, Brazil, Australia, Canada, Belgium, Germany, Romania, France, Venezuela, the Philippines, and the European Union, Switzerland, Italy, Norway, Romania and the United Kingdom. 3

Chaum (Chaum, 1981[9, 10] was the first person who proposed e-voting and there were several experiences have been done in the last few years to facilitate the voting process in elections besides the traditional paper based, for example of the new voting interfaces and systems are touch screens, SMS messages from cellular phones and distributed voting system using the Internet (Monteiro 2001, UK-e-Democracy 2003).

Internet voting systems are more acceptable than the traditional one for more than one reason for example: people are getting more used to work with computers to do all kinds of things, especially sensitive operations such as shopping and home banking, as they allow people to vote far from where they usually live.

On the other hand, internet voting system is encountered by some problems that many prevent this system from being wide spread today (CIVTF 2000, CALTECH-MIT 2001, Cranor 2001, IPI 2001, Rivest 2001, Rubin 2002). There are three main categories by which we can divide these problems. The first class contains security and fault tolerance issues inherited from nowadays internet architecture. The users of internet can be forged to be deceived in the vital services such as DNS name resolution (Lioy *et al.,* 2000). The assumptions which come out of protocols about execution environment leads to the second class of assumption, namely voters must trust the client machines which they use so as to act as trusted agents" in personal or multi user computers with different hard to be ensured.

The voting process's controlling servers cannot be unsuccessful, inaccessible or distort the voting protocols. Reacting properly to client requests or trying to effect the election by acting as a voter can do protocol distortion. The problems of communication or machine failures don't prejudice the voting protocol. The third category of problems includes the difficulties that may arise due to specific attacks against a voting protocol or a running election. Useful results may be got from such attacks by undermining the voting protocol, or damage an election using DoS (Denial of Service) attacks against the involving machines or applications.

On the other hand, there is another type of attack that may happen is the coercion of voters; such attack is due to the lack of supervision of electoral commissions.

Because Internet is insecure medium and this causes incorrect implementations, many secure electronic voting schemes have been suggested[18, 22,25,28,30] to achieve a real electronic voting. 4

The prototype that mentioned in this paper claims to be secure and practical over a network whereas designed to tackle these problems.

This paper identifies the requirements of a secure electronic voting such as: only eligible voters should be able to vote, an eligible voter should not vote more than once, no one should be able to know how another one vote.

EV system is a blind signature electronic voting system based on RSA and national Public Key Infrastructure (PKI), which improved the Estonian e-voting system (2007) but the voters in EV system insert an e-token for the authentication (instead of a Smart card), which has public and private keys, then type their own password to be identified by the authentication server and the eligible voters receive an e-certificate from a certificated authority (CA) server. This would be stored in the voter machine to be used in vote casting to digitally sign the vote. The using of the e-token and e-certificate make the design faster and more secure.

In this paper we review the major current approach for the electronic voting systems. Then offer a new design that improves the previous work. In section 2 the related work is stated. In section 3 the requirements for a secure election system is discussed. In section 4 the proposed protocol is explained. In section 5 the details of new EV protocol is explained. Finally conclusions are displayed and future work is proposed.

Related Work

There are three types of the cryptographic electronic voting scheme which is identified by their privacy policy as follows: protocols using mix-nets, protocols using homomorphic encryption and protocols using blind signature (Forsythe 2005). On the other hand most of them are not practical and unworkable over internet (Sampigethaya 2006). Here we remember a few examples of each type.

The main idea of the voting scheme based on the homomorphic encryption is to encrypt the total votes (using some procedure) and then decrypt the sum without decrypting individual votes[16,27].

The homomorphic voting is incompetent for election widely due to the cost of calculation and communication in order to demonstrate and validate the vote is relatively high. By the way the voting scheme depends on homomorphic encryption is far from real life because the lack of secure. The main idea in the voting scheme based on the mix-network is as follows: the voters authenticate and display encrypted vote then the votes are sent through the mix-network which in turn doing permuting and shuffling processes the votes by doing specific operations to conceal the relationship between the vote and its voter [12]. The major problem in mix-network's server is efficiency of proof technique as the servers suffer from cost of calculation for proving that their mixing is true. The 5 blind signature based on voting scheme divides the election authority in to two parts, the first is named as an administrator and the second is named as a tallier, the administrator is allowed to authenticate a voter by signing the encrypted vote by the administrator's signature. The voter then unblinds the signed vote and sends it to the tallier who is responsible for counting the votes through an anonymized channel[7, 23-24].

Several models of electronic voting have been proposed in the last few years. The most important features of some of them will be mentioned in here. The first implemented electronic voting system is named SENSUS system (Cranor 1997). The protocol is based upon a scheme proposed by Fujioka *et al.,* (1992). Sensus is based on a blind signature scheme known as FOO92 [21]. The main problem for the Sensus is the vulnerability which enables one of the entities participated in the election process refrain to vote and this leads to the fall of these illegal votes into the final tally. Seas protocol was proposed by Fabrizio et.al 2005 to overcome this weakness but it was proved to be inefficient and unrealistic by a protocol is named as " Secure Electronic Voting Protocol Based On Bilinear Pairings (2005)" [14]. EVOX is another implementation depend on the Fujioka *et al.,*, scheme Herschberg described the first version in his Master's thesis[3], and then the EVOX system was improved by EVOX Multiple Administrators (Durette (1999)), it was proved that the robustness of EVOX-MA is higher than the one of EVOX because of the weakness of authentication protocol it is not as good as it could. There was another version of EVOX that is presented by Ko_er, Krimmer and Prosser in 2003 which is the main basis of an e-voting system improved at the Vienna University for Business Administration and Economics (Austria) [KKP03]. This proposal is depending on the blind signature technique and divides the voting protocol into two parts: the registration part and the voting part. REVS (Robust Electronic Voting System) (Joaquim *et al.,*, (2003)) extends EVOX-MA to overcome the failed of distributed components, but does not deal with coercion[26, 29]. Votopia project[19] is proposed for the Soccer World Cup 2002. It is based on PKI, is used to distribute key pairs for each server, using java applet for cryptographic process, but it has been proved that the Votopia project has problems in proving non-disclosure of the identity of voter. Another project is the Serve (Secure Electronic Registration And Voting Experiment)[13] which is based on a PKI, but the project was cancelled because problem in anonymity (Schwartz, 2004). GNU.FREE (Free Referenda and Elections Electronically (GNU, 1999)) [17] which is stand-alone I-voting system and based on java program and Blowfish encryption algorithm, but it is showed security vulnerability. ElectMe [5] is based on blind signatures and claims to be coercion resistant, but it is showed that an enemy is able to damage the election authority because if the enemy learns the ciphertext of a voter's ticket, the scheme is not able to be receipt free. It is showed that ElectMe is not verified in 6 a universal way because the voters can verify their votes are registered properly but the computation of the tally is not verified overtly. The Qatari government began working to develop E-voting system (Khalaf and Luciani, 2008; BTI, 2010). Qatar I-voting project [2] based on blind signature. It was proved that failure of the counting stage in providing evidence that all the votes were counted, which participated in the electoral process. ADDER system [1] is a free and open source electronic voting system which is a free open source electronic voting system which based on homomorphic encryption. Adder system consists of bulletin board server, an authentication server which is done by a Kerberos such as the gatekeeper and client software. In Adder system, it is possible that the authentication server is disrupted by an adversary and causing a vote- buying and coercion. A prototype of DynaVote e-Voting protocol used PVID (Pseudo-Voter Identity) scheme (Cetinkaya 2007-1) is based on blind signature. The counter authority of DynaVote e-Voting prototype may be corrupted if an adversary can know the voter's IP over the internet causing coercion. The electronic voting schemes which based on mix-net schemes are: (1) VoteHere [4] which is built using the VHTi's cryptography (Neff, 2001). However this implementation was keen on voter-verifiability, the voter couldn't verify that the voting machine did not exchange candidates before providing the codes to him. (2) Scytl Pnyx [6] (Riera and Brown, 2004) was implemented in some government systems in Europe but a source code that used in the implementation is not accessible to the public and (3) SureVote[11] (Chaum, 2004; Vora, 2004) is introduced by Chaum (2004) which does not have to permit voters to demonstrate how they voted, but they can verify that their vote was registered in the election system. Homomorphic encryption was implemented in many European Union projects (e.g. CyberVote (2008). It has been

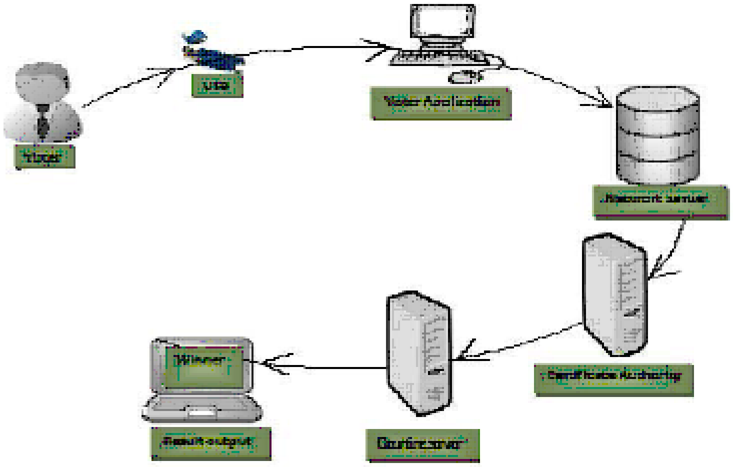

Fig. 1: Indicates to the previous steps

showed that CyberVote[8] is vulnerable to attack from the client side and such attacks lead to loss of privacy of voters, vote buying Which affects on the integrity of the election.and E-Vote [15](Gilberg, 2003) which is based on Paillier homomorphic encryption (Damgård, Groth and Salomonsen, 2003.

Requirements for an election system

Researchers have identified a set of requirements for a secure electronic voting protocol:

Security Requirements

The security has an important role in any voting process and as especially e-voting process because the internet seems to be unsecure environment.

In order to that the electronic voting system works without vulnerabilities, it must be implemented according to safe design. Despite the complexity of the design and 7 implementation of this system, it appears that some standards are accepted completely as the basic security requirements for e-voting.

Voter authentication

It must be ensured that only eligible voter is allowed to vote and that just one vote per voter is tallied.

´

Voter privacy

While it must be ensured that a just the eligible voters can cast a ballot, it must be impossible to connect the voter identity with the content of his/her cast vote.

Accuracy of the Election Results

The system is accuracy when all caste votes cannot be modified, copied, validated votes cannot be removed from the final result and invalid votes should not be counted from the final result. Digital signature is used to prevent any attack on the votes. For accuracy, uniqueness should be applied in the election system by using a token which is unique.

Intermediate result privacy

A system is private if no casted ballot can be linked to its voter (anonymity) neither by election authorities nor by anyone else, and no voter can prove that he or she voted in a particular way (receipt-freeness).

Vote Verifiability

votes must be verified independently by their voters that were inserted in final tally and must be counted correctly.

No coercion

it occurs when an adversary ordered the voter who may relate to him to vote in a certain way, the voter can deceive the adversary. Even if the adversary forced the voter to reveal his keys or to refrain from voting, the adversary cannot be able to determine whether the voter cast according to the adversary's instruction or not.

Democracy

Each eligible voter has the right to cast his vote and is not allowed for anyone to vote for others.

Robustness

The system must be secure and non-infiltrated by adversaries by preventing any harmful behavior of voters, authorities or strangers. A token is necessary to participate in the voting protocol.

There are additional requirements that deal with public security properties of the system implementation. For example the system should be trusted, user friendly, transparency, based on open computer architectures and open source software etc.

Some of the above mentioned requirements are contradicting each other. For example, in the voter privacy the ballot cannot be connected to the voter. This contradicts with the verifiability property which is requiring that each voter can verify his/her vote is counted.

System Wide requirements

In this section the system wide requirements is mentioned that are related to the implementing voting protocols.

Voter convenience

The voters should vote without reference to the voting authorities complete the voting procedures. This must happen with the existence a minimum of skills and equipments[8].

Voter mobility

The voter can participate in an election from any location without constrains.

Flexibility

A flexible system is achieved if a variety ballot question formats is permitted with the existence of different languages and the possibility of dealing with many types of election processes.

Efficiency

The system is effective if the number of voters and the participation of the authorities in the protocols is equivalent to the amount of computer and communications.

Proposed protocol

The proposed protocol in this paper can explain the stages of the electronic voting are as follow:

- Voter Registration
- Voter Authentication
- Voting process
- Counting Phase

The electronic voting system must meet the requirements of the voting so the proposed EV system will try to focus on solving security requirement such as integrity, authentication, confidentiality and verifiability by implementing some protocols that guarantee a more secure and stable e-voting system.

The EV system is based on blind signature, which is not associated with the real identity of the voter to achieve anonymity in electronic voting protocol. The basic scenario of the protocol over Internet is as follows:

- Voter obtains a token from the CA government. Voting token like a secure USB, this is valid for the voting process only that contains the voter name, his public and private key. The verification code is different for every voting token.
- He accesses to the voting web page to make the registration.
- He enters the token to the voting machine to provide his personal data for authentication.

The authentication server checks if the voter is eligible or not. A Certificate Authority (CA) server sends an e-certificate to the eligible voters. The e-certificate would be stored in the voting machine to be used in vote casting to digitally sign the vote.

The authentication of e-voting system and voter's digital signature are applied by using the EV's Public Key Infrastructure.

- An authenticated voter selects his candidate from the network server
- The EV system encrypts the vote by using his public key.
- The voter signs the encrypted ballot by using his private key in the token.
- Network Server compares whether the session owner is the same person who had signed the encrypted ballot and in case of positive acknowledgment, transfers the signed and encrypted ballot to Votes Storing Server. Votes Storing Server connects to the Certification Authority and provides the attestation of digital signature validation. The system replies to each correctly cast vote with a receipt *Response*. *Response* is a text type file and consists of the information about reception of ballots.
- The EV system received the signed and the encrypted votes to the counting server
- The counting server decrypts the signed and the encrypted votes by using his private key
- Non-accepted encrypted votes are saved into the log file.
- The counting server counts the valid votes and saves it into the log file.
- After that the counting server outputs the final result of the election.

Prototype

In section 3, we briefly described the requirements of e-voting system and note that there are some contradictions between the requirements, so we try to overcome these difficulties by implementing EV system. In this section, we created a prototype for this scheme. The prototype imitates user interaction with the remote authority and with the local voting machine. VS was fully implemented in java, enabling it to be installed and executed on an computational platform .In order to implement this scenario we have developed a client/server web application with java.

For encryption we used RSA based national public key infrastructure (PKI) and we used also a database namely MySQL5.0 to store election data.

For authentication, a voter connects to NS by using https protocol. After election times out, all election data in server databases are exported by authorities. These exported data are sent to counter server in an offline way. Counter server starts counting process and after tabulation process it opens a pop window that show the winner and the number of cast votes for each candidates and their percentage.

CONCLUSION

In this paper we have proposed a secure electronic voting scheme. The prototype has been developed that implements the entire EV protocol over Internet. The prototype includes implementation of EV scheme component as well. In addition, the scheme also meets all the electronic voting requirements: anonymity of voters, accuracy of voters, collision freedom, tally correctness, verifiability, and double voting detection. So far, there are few methods to meet all the electronic voting requirements, especially double voting detection. Moreover, the scheme is suitable for large-scale elections and does not require any special voting channel.

REFERENCES

1. Aggelos Kiayias, Michael Korman and David Walluck. An Internet Voting System Supporting User Privacy. In Annual Computer Security Applications Conference, pages 165–174, Miami Beach, *Florida,* (2006).
2. Alkhelaifi, M, Alja'am, J. and Al-Sayrafi, M. Towards an Electronic Voting System for the State of Qatar (2009).
3. A.M. Shubina and S.W. Smith. Design and prototype of a coercion resistant, voter verifiable electronic voting system. In Proc. of Conference on Privacy, Security and Trust, pages 29–39 (2004).
4. A. Neff and J. Adler, Verifiable e-Voting, www.votehere.net/vhti/ documentation/ verifiable e-voting.pdf (2003).
5. Anna M. Shubina and Sean W. Smith. Design and Prototype of a Coercion-Resistant, Voter Verifiable Electronic Voting System. In Proc. of Conference on Privacy, Security and Trust, pages 29–39, Fredericton, New Brunswick, Canada (2004).
6. A. Riera and P. Brown. Bringing Confidence to Electronic Voting. EJEG, 2(1), CHAUM, D. Secret ballot receipts: true voter-verifiable elections. IEEE: Security and Privacy Magazine **2**(1): 38-47 (2004).
7. Atsushi Fujioka, Tatsuaki Okamoto and Kazuo Ohta. A Practical Secret Voting Scheme for Large Scale Elections. In International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), pages 244–251, Balatonfured, Hungary, (1992).
8. CyberVote, Deliverable D6: Report on Review of Cryptographic Protocols and Security Techniques for Electronic Voting" Version 1.0, European Commission Research Contract IST-1999-20338, 55 (2002).
9. D.Chaum, Blind signature systems, in Proceedings of Advances in Crypto'83, New York, USA, p.153 (1983).
10. D.Chaum, Election with unconditional-secret ballots and distribution equivalent to breaking RSA, in Proceedings of Advances in EURO-CRYPT'83, Davos, Switzerrland, pp.177-182 (1988).
11. D. Chaum. Secret-Ballot Receipts: True Voter-Verifiable Elections. *IEEE Security & Privacy,* **2**(1): 38-47 (2004).
12. D.Chaum, Untraceable electronic mail, return addresses and digital pseudonyms, *Communications of the ACM,* **24**(2): pp.84-88 (1981).
13. D. Jefferson, A.D. Rubin, B. Simons, D. Wagner. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE). 2004.

14. F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Pet-rocchi and A. Vaccarelli, SEAS, a Secure e-Voting Protocol: Design and Implementation, Computers & Security, Vol. 2, No. 8, 2005, pp. 642-652. doi:10.1016/j.cose.2005.07.008.
15. J. Gilberg. E-VOTE: An Internet-based Electronic Voting System: Consolidated Prototype 2 Documentation. Technical Report e VOTE/WP 7/D7.4/3.0/29-05-2003, May 2003. http://www.instore.gr/evote/evote end/htm/ 3public/doc3/public/public deliverables/d7 4/Consolidated Docu final.zip.
16. Josh Daniel Cohen Benaloh. Verifiable Secret-Ballot Elections. Ph.D. Thesis, Yale University, September 1987.
17. J. Kitcat , GNU, 1999, Gnu. free referenda and elections electronically. Available on: http://www.gnu.org/software/free/ (abandoned).
18. Karro J, Wang J. Towards a practical, secure, and very largescale online election. In: Proceedings of ACSAC'99. IEEE; p. 161e9 (1999).
19. K. Kim. Killer Application of PKI to Internet Voting. In IWAP 2002. Springer Verlag, Lecture Notes in Computer Science No. 1233 (2002).
20. K. Sako and J. Kilian. Secure Voting Using Partially Compatible Homomorphisms. In International Cryptology Conference (CRYPTO), pages 411–424, Santa Barbara, *California*, (1994).
21. L. F. Cranor and R. K. Cytron. Sensus: A security-conscious electronic polling system for the Internet. In Proc. of IEEE Hawaii *International Conference on Systems Science*, 561-570 (1997).
22. Magkos E, Burmester M, Chrissikopoulos V. Receipt-freeness in large-scale elections without untappable channels. In: 13E. Kluwer; p. 683-94 (2001).
23. Miyako Ohkubo, Fumiaki Miura, Masayuki Abe, Atsushi Fujioka and Tatsuaki Okamoto. An Improvement on a Practical Secret Voting Scheme. In Information Security Workshop, pages 225–234, Kuala Lumpur, Malaysia, (1999).
24 Tatsuaki Okamoto. Receipt-Free Electronic Voting Schemes for Large Scale Elections. In Security Protocols Workshop, pages 25–35, Paris, France (1997).
25. Ray I, Narasimhamurthi N. An anonymous electronic voting protocol for voting over the internet. In: Proceedings of WECWIS'01. IEEE;. p. 188-91 (2001).
26. Ricardo Lebre, Rui Joaquim, Andr´e Z´uquete, and Paulo Ferreira. Internet Voting: Improving Resistance to Malicious Servers in REVS. In Proc. of IADIS International Conference on Applied Computing, Lisbon, Portugal, (2004).
27. Ronald Cramer, Rosario Gennaro and Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Scheme. In International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), pages 103–118, Konstanz, Germany, (1997).
28. Rubin AD. Security considerations for remote electronic voting Communications of the ACM **45**(12): 39-44 (2002).
29. Rui Joaquim, Andr´e Z´uquete, and Paulo Ferreira. REVS—A Robust Electronic Voting System. In Proc. of IADIS International Conference on e-Society, Lisbon, Portugal, (2003).
30. Ryan P, Bryans J. Security and trust in digital voting systems. In: Proceedings of FAST'03. Tech Rep. IIT TR-10/2003; p. 113e20 (2003).