ISSN No. 0976-5697

Volume 2, No. 6, Nov-Dec 2011

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Security Analysis and Issues in an Internet Voting: A Review

Kalaichelvi V*
Department of Computer Science and Engineering
Shanmugha Arts, Science,Technology & Research Academy
Kumbakonam, Tanjore, TN, INDIA
kalaichelvi2k@gmail.com

Dr.RM.Chandrasekaran
Department of Computer Science and Engineering
Annamalai University
Chidambaram, Cuddalore, TN, INDIA
aurmc@sify.com

Abstract: Internet Voting (i-Voting) can play a really vital role in the democracy of our life. This paper analyzes the various security issues involved in an i-voting like privacy, authentication, anonymous, uniqueness, accuracy and Uncoercibility. This paper also discusses about what we need to achieve the above requirements to implement an internet voting. This paper also discusses what are all the problems will occur while implementing an i-voting system and the solutions are also discussed.

Keywords: i-voting, Privacy, anonymous, authentication and Un-coercion

I. INTRODUCTION

A. Traditional Voting Process:

Traditional voting process that can be divided into four phases:

- ***a. Authentication–*** Alice walks into a voting precinct and authenticates herself by showing her voting credentials; this step is public and verified by the officials present in the room. At the end of the authentication process, Alice is given a paper ballot on which to write her vote.
- ***b. Vote–*** The vote takes place in a protected booth where she cannot be seen by anyone. Alice casts her vote by writing it with a pencil on the paper ballot; she then folds the paper ballot and puts it in the ballot box where all the votes are mixed. Since no one can see what Alice writes and there are no marks on the paper ballots, Alice's vote is anonymous.
- ***c. Counting the votes–*** At the end of the voting time, the officials open the box containing the paper ballots and publicly count the votes; the results are then announced.
- ***d. Verification–*** Various types of verification are used or possible; most procedures are indeed public and overseen by representatives of competing parties. The opposite interests of the parties warrant the first level of protection against fraud. A recount is also possible if there is a presumption of fraud or error.

In an electronic voting system, which is advancement over the conventional voting system, the problem of printing ballots and the problem of counting are solved, but maintaining convenient poll booths is still difficult. So there must be another way to solve these problems or reduce it as possible, and give the voters the confidence to believe of the system, from this point we think to use a new technology to improve the election by building a new system that is convenience for environment. The only alternative to overcome these problems is to make use of online voting system. With the advent of Internet and World Wide Web (W3), it is easy to design a secure online voting system. In the Online Voting system the paper registration is supplemented by online registration. Manual Signature is replaced by digital signature and blind signature [1-3].

II. RELATED WORK

In the last few years a numerous number of researches propose different e-voting systems, and some countries and states around the world implement their e-voting system. However, this numerous number of e-voting schemes can be categorized into three main categories. The categories based on the cryptography mechanism used to build the system. The first category is e-voting system based on blind signature technique [1-3] the second category is e-voting system based on Mix-Nets [5-6]. The third and the last category is e-voting system based on homomorphic signature Properties [4-11]. Chaum was the first one to introduce blind signature and mixed nets. In general this different proposed system agree that the system should not be verifiable voting system (which mean the voter has no way to prove their voting activity) as a prevent technique against vote buying problem. However, some other e-voting system allows voter to prove their voting activities. Since the voting buying and the privacy of the voter is a critical problem in the Jordanian voting system we design our scheme as anonymous and unverifiable e-voting system, which categorize under the first category "blind signature-based e-voting system".

III. PROPERTIES / ISSUES / REQUIREMENTS OF AN ELECTRONIC VOTING

The requirements in conventional voting (paper vote) are also apply for electronic voting, the requirements can expected to be universal, any system must try to apply these requirements:

Fairness : No one can learn the voting outcome before the tally.

Eligibility : Only eligible voters are permitted to vote.

Uniqueness : No voter should be able to vote more than once.

Privacy: No one can access any information about the voters vote.
Accuracy: All valid votes should be counted correctly.
Soundness: Any invalid vote should not be counted.
Uncoercibility: No voter can prove how he voted to others to prevent bribery.
Anonymity: There should be no way to derive a link between the voter's identity and the marked ballot.
Efficiency: The computations can be performed within a reasonable amount of time.
Robustness: A malicious voters cannot frustrate or disturb the election.
Verifiability: Voters can check if their ballots have been correctly counted.

IV. METHODOLGY TO BE USED IN AN I-VOTING SYSTEM

This section describes about how the internet or web or online voting system can guarantee the above requirements.

A. Authentication and Un-coercions:

In Authentication step, there is a problem. Certainly, since the voter is at a remote location, we cannot be sure that the voter is who she avows to be, unless we use a biometric authentication protocol. Without biometrics, one can sell or be forced to sell her voting credentials to Eve without anybody realizing. Even with the use of biometrics to authenticate, both eligible person and Eve sit in front of the same system (reserved for election) doing the authentication and Eve voting or monitoring the votes, as he wants. If voter wants to sell her vote, and Eve is not present, she can take a visual rendering of his voting and give it to Eve as evidence. In any case, the remoteness of the voter makes the eradication of the sale of votes impossible to fulfill for online voting.

Problem: In practice, this means that online voting cannot be used in elections or polls where fraud by the sale of votes or coercion is concern, like in political elections.

B. Uniqueness and Anonymous:

After being authenticated, one can casts his single vote in such a way as to maintain his privacy, i.e., the protocol must guarantee the vote cannot be cast twice and it has been privately done. We need to prevent double voting but at the same time guarantee that all votes are anonymous on the vote web server. A simple solution to this problem is as follows:

Eligible voter is given one digitally signed document by the authentication authority or server. The Digital Authorization is the equivalent of the blank official paper ballot in traditional election as it allows voting anonymously.

Then voter presents the Digital Authorization to the vote Web server which checks the digital signature verifying that it has been made by the authentication authority/server, and also that this is the first time that it is presented to it for voting. If these two conditions are met, voter is allowed to cast her vote on the Web server.

Solution I: To guarantee voter's vote is anonymous, cryptography encounter in this process. For example, there are various cryptographic protocols that allow the digital signage of a document without knowing its contents, as in the ***blind signature [1-3] scheme.***

Problem: But these protocols are more difficult to implement and it is very difficult for the average user to follow it correctly.

Solution II: To avoid these problems, some researchers have taken a different approach to online voting by keeping together the identity of the voter and vote until it is time to count them.

Problem: In practice, this means that online voting cannot be used in elections or polls where the voter's vote is derived or anonymous concern, like in political elections.

Solution III: To avoid these problems, some cryptography researchers have taken a different approach to internet voting by decoupling the identity of the voters and vote, and votes are mixed and then counted, as in the mix-net scheme[5-6].

Problem: In the case of online voting, it is believed that this procedure is difficult to implement correctly. In practice, if the vote is casted twice means, it is not easy to delete the duplicated votes.

C. Anonymous and Privacy Network:

To guarantee voter's privacy and voter's vote is anonymous, we also need to consider the network ie., IP address of voting machine should be concealed from the web vote server. But the connection is encrypted with SSL / TLS, no one can learn or modify the voter's vote. Not all standard browsers send basic information about themselves to the vote Web server. Usually this information leak is not vital, but in some cases it could still give hints on who the voter is.

Solution: The only way to remove this information is to prepare a custom-made browser reserved only for voting.

D. Privacy and Anonymous:

Once the Vote Web server receives a vote, it stores it securely until the time when all votes are counted and it stores sequentially in the order that they are cast. Whenever vote is casted by the voter, vote is encrypted with the public key of the electoral committee. Similarly, the votes can be decrypted with the Corresponding private key. This key information should be kept secret until the moment of counting the vote arrives.

Certainly, there is the risk of loss of privacy and anonymous and by correlating the order of authentication of the voters with the order in which the votes are recorded. Again cryptography is involved to shuffle the recorded vote based on the concept of mix-net Scheme[5-6]. Finally the encrypted anonymous votes are decrypted and counted by the authority.

Solution: The anonymous network reduces this risk. Even then, to guarantee privacy we need to mix up the encrypted votes.

E. Anonymity and Verifiability:

In traditional voting, the voter cannot directly verify their vote has been counted correctly. Instead, they trust the electoral officials for the integrity and correctness of the procedure. In case of any complaints, all or only the particular booth ballots can be recounted. In digital voting most of the work like Verification, casting of vote and counting is done by the machines. So, the voter should trust the people who designed and build the hardware and software.

To guarantee verifiability, the voter's encrypted vote will be sent to the voter with the key value to decrypt that vote. By decrypting that vote, the voter can verify that the voter's vote has been counted correctly.

But in digital voting there is new possibility that gives each voter receipt that allows one to verify that the vote has been counted correctly. It should be unique for each vote and it does not contain reference to who the voter is.

Solution: To avoid these problems, some researchers have taken a different approach to online voting by building such receipts using cryptography one-way hash function or Zero-Knowledge protocols.

Problem: But if the receipt contains any reference related to the candidate and voter means that it is impossible to prevent coercion and anonymity.

Solution: We advocate that voters not be allowed to verify their votes by themselves. It is not necessary to allow voter voters to verify (or Show to bribers) their votes in the announcement phase.

V. CONCLUSION

Online voting can play a really vital role in the democracy of our life. But, comparatively it increases the voting rate. Even then, there are some intrinsic limitations and security issues. We cannot unconditionally trust digital systems to guarantee the authenticity of a protocol ie., we cannot guarantee that a web server has no bugs. This paper discussed about how the internet voting system can achieve the following requirements such as fairness, uniqueness, accuracy, privacy, anonymous, authentication and un-coercion and it also discussed what are all the problems will be occurred while implementing internet voting system. If any electronic voting system fulfills the above issues, we can recommend that system for large scale elections.

VI. REFERENCES

[1] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. "A practical secret voting scheme for large scale elections". In Advances in Cryptology |AUSCRYPT '92, pp. 244-251, 1992.

[2] W. Juang and C. Lei, "A secure and practical electronic voting scheme for real world environment," IEICE Trans. On Fundamentals, E80-A(1), January 1997.

[3] Kazue Sako. Electronic voting schemes allowing open objection to the tally. In Transactions of IEICE, vol. E77-A No.1, Jan.1994.

[4] Tatsuaki Okamoto. Receipt-free electronic voting schemes for large scale elections. In Proc. Of Workshop on Security Protocols '97, vol. 1361 of LNCS, pp. 25-35.Springer-Verlag, 1997.

[5] Markus Jakobsson. A Practical Mix. In Advances in Cryptology | EU-ROCRYPT '98, vol. 1403 of LNCS,pp. 448-461, Springer-Verlag, 1998.

[6] Masayuki Abe. Mix-networks on permutation networks In Advances in Cryptology |ASIACRYPT '99, vol. 1716 of LNCS, pp. 25-273. Springer-Verlag, 1999.

[7] Josh Cohen Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections (extended abstract). In Proc. 26th ACM Symposium on the Theory of Computing (STOC), pp. 544-553.ACM, 1994.

[8] Ronald Cramer, Matthew K. Franklin, Berry Schoenmakers, and Moti Yung. Multi-authority Secret-ballot elections with linear work. In Advances in Cryptology | EUROCRYPT '96, v ol. 1070 of LNCS, pp.72-83.Springer-Verlag, May 1996.

[9] Ronald Cramer, Rosario Gennaro, and Berry S choenmakers. A secure and optimally efficient multi-authority election scheme. European Transactions on Telecommunications, 8:481-489, 1997. Preliminary version in Advances in Cryptology | EUROCRYPT '97.

[10] Kazue Sako and Joe Kilian. Secure voting using partially compatible homomorphisms. In Advances in Cryptology | CRYPTO '94, vol. 839 of LNCS, pp.411-424. Springer-Verlag, 1994.

[11] Kazue Sako and Joe Kilian. Receipt-free mixtype voting scheme A practical solution to the implementation of a voting booth. In Advances in Cryptology | EUROCRYPT '95, vol. 921 of LNCS, pp. 393- 403. Springer-Verlag, 1995.