Asian Journal of Information Technology 10 (2): 47-50, 2011
ISSN: 1682-3915

Implementation Issues in an Online Voting

[1]V. Kalaichelvi and [2]R.M. Chandrasekaran
[1]Department of Computer Science and Engineering, SASTRA University,
Kumbakonam, Tamilnadu, India
[2]Department of Computer Science and Engineering, Annamalai University,
Chidamabarm, Tamilnadu, India

Abstract: Online voting can play a really vital role in the democracy of the life. As cheating is an inherent threat to voting, it is essential that an e-voting system provides a high level of security. This study analyzes the various security issues involved in an online voting like privacy, authentication, anonymous, uniqueness and coercion. This study also discuss about what we need to achieve the above five requirements to implement an online voting.

Key words: E-voting, privacy, anonymous, authentication, coercion, requirements

INTRODUCTION

Now a days, one of the most important government services like elections became a severe pressure on people involved in that process, according to many constraints that must be applied to the beneficiaries of this service and who are divided into two parts, candidates and voters. Voting is an efficient method for the public to show their opinion about a given topic or issue. In other words, voting is the key of democracy. The traditional election is normally held under the supervision of the government to assure the right application of the constraints during the election process and to assure that only eligible voters are permitted to join the election process avoiding any kind of forgery and the attempts of multi-voting.

One of the most famous violations of any government is vote buying which is too difficult to control. In addition, the process of human supervision over the election process requires a lot of efforts and money in order to achieve the desired level of privacy, security and trust. Moreover, when the election is done, another problem appears which is vote checking and counting.

These require great efforts that are supposed to be exerted by humans and no single mistake is accepted during this process. This phase of the election is considered as a time consuming process and its accuracy is always mistrusted. These drawbacks enforce the public to think about another voting system that could overcome them. According to all what is previously mentioned, the whole world is moving on towards the trend of e-voting. E-voting systems are expected to be the solution for the weakness in traditional voting systems. The use of computer networks and modern state of the art cryptography techniques to build e-voting systems is expecting to result with a voting system which confirms that only people with the right to vote are able to cast a vote emphasizing that every vote cast is counted only once. In addition, the system can run in unverifiable voting mode (where the voter cannot prove his voting cast) which prevents the voters from selling their votes to candidate.

An ideal e-voting system should allow the voting process to be available on a public communication channel such as the internet that will encourage more voters to cast their vote remotely and increase voter participation with the help of internet voting that can be done on workdays. Even citizens aboard can cast their voting. In general, e-voting system can replace obsolete voting system by providing a suite of features including the privacy of the voter, the fraud detection and prevention, the security of the voting process, the ability of remote voting and the guarantee of a fair election process. E-voting is supposed to deliver many requirements that are needed to achieve the e-voting system applicable over the traditional voting system. E-voting must be easy for the beneficiaries (candidates and voters) to follow without recognizing any change in the traditional system saving much time and costs. E-voting must deliver a very high degree of security such as privacy, integrity beside accuracy to avoid the same

Corresponding Author: V. Kalaichelvi, Department of Computer Science and Engineering, SASTRA University, Kumbakonam, Tamilnadu, India

problems faced by traditional voting by rooting them out completely. E-voting is promising to achieve the required level of security so as to be applicable to be used for holding election processes saving man effort, cost and of course time. No doubt, the system will facilitate a lot of work that was too hard, serious and confidential like vote checking and counting since there is a dedicated server for that process that cannot commit human mistakes resulting accurate outputs.

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 (Fujioka *et al*., 1992; Juang and Lei, 1997; Kazue, 1994). The second category is e-voting system based on Mixed nets (Jakobsson, 1998; Abe, 1999).

The third and the last category is e-voting system based on homomorphic signature properties (Okamoto, 1997; Jakobsson, 1998; Abe, 1999; Benaloh and Tuinstra, 1994; Cramer *et al*., 1996, 1997; Sako and Kilian, 1994, 1995). 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 the scheme as anonymous and unverifiable e-voting system which categorize under the first category blind signature-based e-voting system.

REQUIREMENT OF E-VOTING

The requirement in conventional voting (paper vote) are also apply for e-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
- Completeness/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
- Efficiency: the computations can be performed within a reasonable amount of time
- Robustness: a malicious voters cannot frustrate or disturb the election

Here online voting system can guarantee these requirements are discussed next

ISSUES IN ONLINE VOTING

Authentication: 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 picture of his voting and give it to Eve as proof. In any case, the remoteness of the voter makes the abolition of the sale of votes impossible to fulfill for online voting.

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.

Privacy, 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 study 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.

To guarantee voter's privacy and 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 scheme (Fujioka *et al*., 1992; Juang and Lei, 1997; Kazue, 1994). But these protocols are more difficult to implement and it is very difficult for the average user to follow it correctly.

To avoid these problems, some researchers have taken a different approach to web voting by keeping together the identity of the voter and vote until it is time to count them. The identity of the voters and vote are then decoupled and votes are mixed and then counted.

In the case of web voting, it is believed that this procedure is difficult to implement correctly and to guarantee the privacy of voters. In practice if the vote is casted twice means, it is not easy to delete the duplicated votes.

Anonymous and privacy network: To guarantee voter's privacy and voter's vote is anonymous, we also need to consider the network i.e., 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. The only way to remove this information is to prepare a custom-made browser reserved only for voting.

Counting: 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 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 mixnet (Jakobsson, 1998; Abe, 1999; Benaloh and Tuinstra, 1994). Finally the encrypted anonymous votes are decrypted and counted by the authority.

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

Verification: 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.

Any digital system (complex) has bugs so as voters, we cannot trust the digital voting machine. 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. We can build such receipts using cryptography one-way hash function or Zero-Knowledge protocols.

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

CONCLUSION

Online voting can play a really vital role in the democracy of the life. We cannot participate in an election because we are not physically present at the moment of election. 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 i.e., we cannot guarantee that a web server has no bugs. To ensure correct user protocol, adopt simpler user steps during the web voting process. If any electronic voting system fulfills the above issues, we can recommend that system for large-scale-elections.

REFERENCES

Abe, M., 1999. Mix-networks on permutation networks. Lect. Notes Comput. Sci., 1716: 258-273.

Benaloh, J. and D. Tuinstra, 1994. Receipt-free secret-ballot elections (extended abstract). Proceedings of the 26th Annual ACM Symposium on theory of Computing, May 23-25, Montreal, Quebec, Canada, pp: 544-553.

Cramer, R., M. Franklin, B. Schoenmakers and M. Yung, 1996. Multi-authority Secret-ballot elections with linear work. Lect. Notes Comput. Sci., 1070: 72-83.

Cramer, R., R. Gennaro and B. Schoenmakers, 1997. A secure and optimally efficient multi-authority election scheme. Lect. Notes Comput. Sci., 1233: 103-118.

Fujioka, A., T. Okamoto and K. Ohta, 1992. A practical secret voting scheme for large scale elections. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, Dec. 13-16, Springer-Verlag, London, UK., pp: 244-251.

Jakobsson, M., 1998. A practical mix. Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, May 31-Jun. 4, Espoo, Finland, pp: 448-461.

Juang, W. and C. Lei, 1997. A secure and practical electronic voting scheme for real world environment. IEICE Trans. Fundam., E80-A: 64-71.

Kazue, S., 1994. Electronic voting schemes allowing open objection to the tally. Trans. IEICE, E77-A: 24-30.

Okamoto, T., 1997. Receipt-free electronic voting schemes for large scale elections. Proceedings of 5th International Workshop on Security Protocols, April 7-9, Springer-Verlag, London, UK., pp: 25-35.

Sako, K. and J. Kilian, 1994. Secure voting using partially compatible homomorphisms. Lect. Notes Comput. Sci., 839: 411-424.

Sako, K. and J. Kilian, 1995. Receipt-free mixtype voting scheme. A practical solution to the implementation of a voting booth. Lect. Notes Comput. Sci., 921: 393-403.