Innovative Way of Internet Voting: Secure On-line Vote (SOLV)

Dr. Shalini Vermani[1], Dr. Neetu Sardana[2]

[1]Department of Information Technology, Apeejay School of Management, Dwarka, New Delhi, India

[2]Department of CSE&IT, Jaypee Institute of Information Technology, Noida, India

Abstract

With the rapid growth in Information Technology, internet voting system has been evolved. This is a web based system that must provide high level of security. In this paper we have proposed Secure On-line Vote (SOLV), an internet voting system. SOLV gives voters a reliable and highly secure environment to cast their vote on web. This system ensures authentication of voters and guarantees the secrecy and integrity of each vote.

Keywords: *Voting, Biometric, Authentication, Public Key, Private Key.*

1. Introduction

Internet voting enables a person to vote over the network in secure manner by making use of Information Technology. It is a natural step in evolution of conventional voting system. To cast vote in conventional system, voter may face unpleasant conditions such as bad weather, traffic jam, long queues in voting booth etc. It is also possible that the voter is not in his country or do not have enough time to go for voting at the voting booth. These situations resulted in continuous decline of voters' turnout at the voting booth over a period of time. There are many countries that have experienced it eg. in Canadian Federal elections turnout of voters declined from 80.65% in 1958 to 61.2% in 2000[8]. Similar cases are also noted in Presidential Elections in US where the turnout of voters were declined from 95.8% in 1964 to 51.2% in 2000[9] and in General Election of UK where the turnout of voters were declined from 83.6 % in 1950 to 59.4% in 2001[9]. Continuous decline in the voters' turnout at the voting booth resulted in the development of internet voting.

Internet voting provides convenient and flexible way of voting that saves time and cost. It enables people to cast their vote from the place of their choice like home, office or they can cast vote even when abroad. Internet voting allows eligible voters to logon to a web portal, authenticate themselves and submit their ballots via the portal. It must provide integrity of the election result and the secrecy of voters' choices. Voting system must remain uncompromised on an open network. In designing and deploying internet voting systems, advanced cryptographic techniques and state of the art web technologies can be employed to protect such systems. Many such systems [1][3] are developed in the past to implement voting over web.

In this paper we are proposing a scheme **Secure On-line Vote (SOLV)** for secure and reliable internet voting. Paper is sectioned in following manner:

Section 2 describes different ways to conduct internet voting. Section 3 discusses various possible challenges in internet voting. Section 4 introduces Secure On-line Vote (SOLV) , a new internet voting system. Section 5 details security analysis of SOLV. Section 6 ends the paper with conclusion.

2. Internet Voting Ways

There are three ways in which internet voting can be implemented

2.1 Internet Voting in Voting Booths

In this method the polling booths have the computers connected to the internet and a voter has to go to the polling booth to cast his vote. Election officers are being appointed at voting booths to assist voters. This method helps the people who have technophobia, no technology in hand or their software in incompatible with the security system used in the election.

2.2 Internet Voting from Remote Location

In this method voter can cast his vote from location of their choice.

2.3 Dual Implementation

This is a hybrid approach in which voters are given freedom to vote either from any polling booth or place of their choice.
Internet voting should only be adopted once all the technical challenges have been overcome. Following section elaborates the various issues while implementing internet voting.

3. Challenges in Internet Voting

Internet voting takes place in a distributed, nontransparent electronic environment that is not controlled by election officials, it raises the potential for attacks on the voting system to come from anywhere in the world. An electronic voting system via the internet must fulfill the following five basic requirements:

3.1 Voter's Authentication

This captures two important issues: 1) only eligible voters can vote, and 2) each eligible voter can only vote once. To satisfy this secure online procedure is required with which voters must be authenticated prior to voting, and marked as having voting after their ballots are cast.

3.2 Server Side Attack

Servers are used for maintaining and processing the electronic ballots. If the attacker overloads the election web server and prevents citizens from voting, the meaningfulness of the election is compromised. Such an attack is known as Denial of Service attack (DoS). Server must be protected against DoS attacks which could threaten any voter access to their ballot or their ability to transmit their ballot back to the elections office server.

3.3 Client Side Security

Providing security at the voter terminal is important and challenging.

3.4 Secrecy of Vote

Confidentiality of vote needs to be maintained. In other words voter must be unobserved while casting his vote.

- ✓ Anonymity: No one can determine whom voter has voted for.
- ✓ All votes remain secret up to the end of the voting process.

3.5 Transmission Channel Security

Transmission channel provides communication media between various voters to the election web server. Channels are more susceptible to varied attacks. It is utmost important that the channel through which vote is sent from voter to server should be kept secure.

The following section introduces a new online voting scheme Secure On-line Vote (SOLV) that addresses all the above mentioned issues.

4. Secure On-line Vote (SOLV)

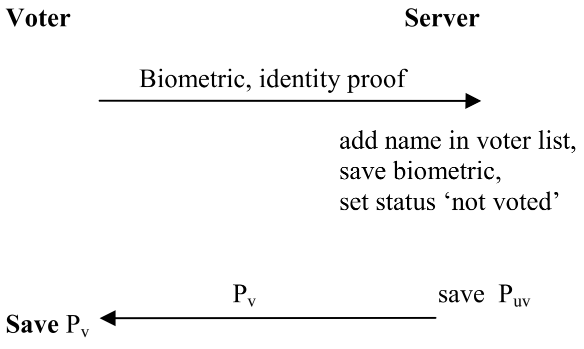
The voting procedure of SOLV that has three stages are described below:

4.1 Prior to Voting

Initially voter needs to register online on the election website. Registration is done before the commencement of voting. All the voters are required to register online to the election server. During registration, voter is required to submit his biometric and required details as a proof of his identity to server. In return, voter will get the private key and server will kept the corresponding public key with itself. The server maintains the list of all the authentic voters along with their public key. Initially all the voters will be assigned status as 'not voted'.

Figure 1 Graphical Representation of Registration Process

Abbreviations:
P_v – Private key of voter
P_{uv} – Public key of voter
P_s – Private key of server
P_{us} – Public key of server
$P_x(y)$ – message y encrypted with key x

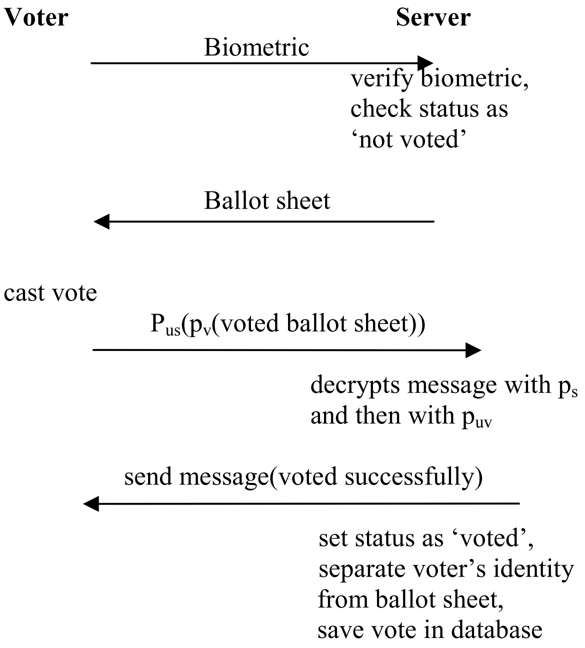


4.2 Voting Process

On the day of election, voter logins at the voting site using his biometric identification. Once server will verify his biometric it will check his status. If the status is 'not voted', server will send him a ballot sheet. Now voter will cast his vote in the ballot sheet and encrypt it first with his private key and then with the public key of the server and submit it to the server. As soon as successful submission takes place the voter will get the message 'voted successfully'.

As ballot sheet is being received at the server, it will first be decrypted using server's private key and then with the public key of the voter. Finally server will change the status of the voter from 'not voted' to 'voted'. Then Server will separate the identity of voter from the ballot sheet and saves the voted ballot sheet in its database.

Figure 2 Graphical Representation of Voting Process



4.3 Processing of Ballots

After the completion of the voting process, counting of votes is done at the server and then all the voting details are sent to the election head office.

5 Security Analysis of SOLV

This section describes, how SOLV is secure against all the above mentioned challenges.

5.1 Voter's Authentication

Only Authentic Voter can Vote: SOLV is using biometric identification. Voter is required to proof his identity using biometric. If biometric is verified only then voter is allowed to move ahead.

One Voter-One Vote: An important issue in voting is that a voter can cast vote only once. In SOLV when a voter cast a vote his status in the server's database will changed from 'not voted' to 'voted'. Next time if the same voter will try to vote again, server will check his status in the database and will find the status as 'voted'. So the server will disconnect the connection.

5.2 Server Side Attack

Denial of Service Attack **(*DoS*):** The purpose of DoS is to block the channel used for communication between the voter and the election web server. To accomplish this, attacker can congest the channel by sending many requests to the server that in turn prohibits the intended voter to reach the server and disrupts the election process.
To counteract DoS attack, we can have two solutions either we can configure backup servers to take over the charge as soon as the main server is overloaded or stops working [1]. Another solution is to extend the voting procedure for a span of 30 days starting 30 days before election day and extending till the poll ends on election day[3].

5.3 Client Side Attack

To provide security at the voter's terminal, server will transmit a tool to voter's terminal that will automatically stop all the processes running on the voter's machine except for the processes the election system will use [1].

5.4 Secrecy of Vote

Server decrypts the ballot sheet and separates the identity of the voter from the ballot sheet and then voted ballot sheet is stored in the database. Hence only the vote details are stored in the database so no one can determine to whom voter has voted for. In this way anonymity is ensured.
Moreover secrecy of voting pattern is maintained during the voting process. In SERVE[3], election officer can request the server for voting details of voters who have voted and the list of encrypted ballots during the voting process. If the election officer makes the request frequently, it might be

possible for him to know the voting pattern. But in case of SOLV no information is complied and transmitted till the poll ends. Hence all votes remain secret till the end of the voting process.

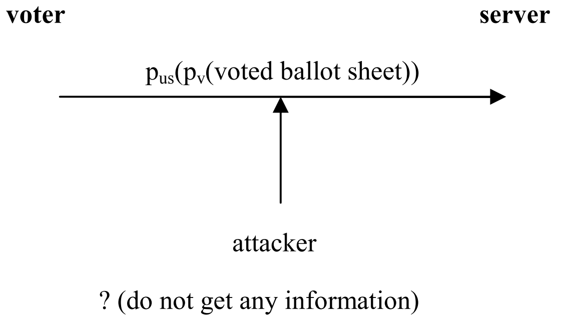
5.5 Transmission Channel Security

Attacker can harm transmission channel in three ways.

5.5.1 Eavesdropping

Attacker may intercept and read the data transmitted over the network. In case of SOLV as data transmitted over network is dual encrypted, so even if attacker eavesdrop the data he could not make sense out the data.

Figure 3 Graphical Representation of Eavesdropping


voter
server
$p_{us}(p_v(\text{voted ballot sheet}))$
attacker
? (do not get any information)

5.5.2 Masquerading

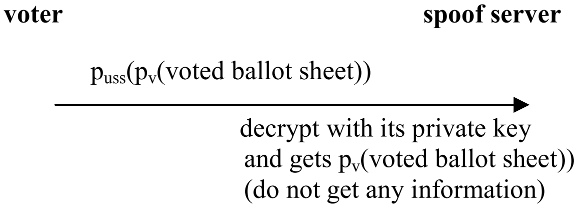
Masquerading is sending the data using another's identity. In SOLV, voter logins using biometric identification for authentication. As soon as user is being authenticated, server sends a ballot sheet to voter to cast his vote. Voter can send vote only after encrypting it using his private key which is being provided by server during registration process. Hacker trying to masquerade needs to have both biometric identity and voter's private key.

5.5.3 Web Spoofing

Web spoofing is the act of creating a website, with the intention of misleading voters. The spoof website adopts the design of the election website and can have a similar URL. This attack is generally done to know the voting pattern. In other words, attacker is interested to know whether the voters are voting in the favor of his party or not. In this attack, attacker will send the URL of the spoof website to the voter which is very much similar to the URL of legitimate election website. Voter will think that this is the legitimate URL and will cast his vote. On receiving the vote, attacker will check the vote and if it is not in his favor then he will discard it otherwise will send an error message 'Try Again' and the legitimate URL to the voter. Next time voter will login to the legitimate website for casting his vote, which is in favor of the attacker. SOLV is secure against spoofing attack, as the voter will send the vote encrypted using his private key which can only be decrypted using corresponding public key that is only with the legitimate server.

Figure 4 Graphical Representation of Web Spoofing

Abbreviation: p_{uss} public key of spoof server


voter
spoof server
$p_{uss}(p_v(\text{voted ballot sheet}))$
decrypt with its private key
and gets $p_v(\text{voted ballot sheet})$)
(do not get any information)

SERVE [3] is not secure against web spoofing attack where as SOLV is secure against this attack.

6. Conclusion

Internet has the potential to make the voting more convenient and thus in turn will increase the voter's participation. In this direction we have proposed Secure On-line Vote (SOLV), an internet voting system. SOLV is a secure and reliable method for internet voting. It provides more mobility and convenience to voters. Security and secrecy issues are resolved at all possible points like server, client or transmission channel.

References

[1] K.M. Elleithy and I. Rimawi, 'Design, Analysis and Implementation of a Cyber Vote System.' Book Chapter, Advances in Computer, Information, and Systems Sciences, and Engineering: Proceedings of IETA 2005, TeNe 2005 and EIAE 2005, Springer, 2006.

[2] C.Hoke, 'Internet voting: structural governance principles for election cyber security in democratic nations', Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies, ACM New York, NY, USA, 2010.

[3] D. Jefferson, A.D. Rubin, B. Simons, and D. Wagner, 'A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)', ETS 300 506. Security aspects (GSM 02.09 version 4.5.1), Digital cellular telecommunications system (phase 2), 2004.

[4] N.Meißner, V. Hartmann, and D. Richter, 'Verifiability and Other Technical Requirements for Online Voting Systems' Electronic Voting in Europe, volume 47 of LNI, page 101-109. GI, 2004.

[5] G. Schryen, 'Security aspects of internet voting', System Sciences. Proceedings of the 37th Annual Hawaii International Conference on , 5-8 Jan. 2004, Pages:116 – 124, 2004.

[6] A. Yasinsac, J.Childs, 'Analyzing Internet security protocols', High Assurance Systems Engineering, 2001. Sixth IEEE International Symposium, 22-24 Oct. 2001, Pages:149 – 159, 2001.

[7] Online Voting, Postnote, Number 155, 2001. Available at www.parliament.uk/post/home.htm

[8] International institute for Democracy and Electoral Assistance, Voter turnout from 1945 to date, Available at http://www.idea.int/vt/country_view.cfm

[9] International institute for Democracy and Electoral Assistance, Voter turnout – A global Survey, Available at http://www.idea.int/vt/survey/voter_turnout3.cfm

Dr. Shalini Vermani is Associate Professor in Apeejay School of Management, New Delhi. She has more than 11 years of experience in teaching and research. Her area of research is Network Security and Cryptography. She has published more than 15 papers in various national and international journals. She has also published a book on Discrete Mathematical Structures in Imperial College Press, London. She had participated and organized number of Conferences and seminars and also co-chair various conferences.

Dr. Neetu Sardana is Assistant Professor in Jaypee Institute of Information Technology, Noida. She have done Doctorate in the area of databases. During her teaching career of more than 10 years, she taught subjects like Database Management System, Management Information System, Computer Networks, Software Engineering and Foundation of Information Technology. She had participated and organized number of Conferences and seminars. She has been also actively involved in organizing International Conference on Contemporary Computing in year 2012 as publicity co-chair. She had already supervised various projects at graduate and postgraduate levels.