Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Issues and Challenges in Electronic Voting and Direct Recording Electronic Voting Systems

Anil Pandit
Research Scholar, Punjab Technical University
Jalandhar, Punjab, India

R. C. Gangwar
Associate Prof. (Department of Computer Science & Engg.)
BCET, Gurdaspur, PTU, Jalandhar Punjab India

Abstract - Recently voting over the Internet has become a hot research topic. E-Voting appears to be a reasonable alternative to conventional elections. This paper focuses on various security flaws in the design of EVM hardware for voters and voting protocols that support the voting process, without implementing the security mechanisms required for preventing fraud and protecting voter's privacy. Slew of security concerns have been raised and various references have been added in this paper to support our issue of security in EVMs'. This paper describes the overall security issues in the hardware of EVMs' , microprocessor of the EVMs', the EVM's firmware is stored in masked read-only memory inside the microcontroller chips, and there is no provision for extracting it or verifying its integrity. The main objective of this paper is to describe the primary role of E-Voting (Internet Voting) and its security in securing the voters privacy, verifiability, coercion and accountability by implementing cryptographic algorithms while transmitting Electoral Voting Data in a Centralized Pool.

Keywords – EVM, DRE, E-Voting, Ballot, Cryptography

I. INTRODUCTION

In a democratic setup, freedom and democracy are often used interchangeably, but the two are not synonymous. Democracy is indeed a set of ideas and principles about freedom. It also consists of a set of practices and procedures that have been shaped through a long, often tortuous legacy.

People for Parliament are elected for a fixed term using the 'preferential' voting system. Under this system, the candidate who finally secures majority votes is elected.

However, because there are multiple candidates for each constituency, it is necessary to use a process of elimination, and whoever gets majority votes is elected. Elections allow the public to choose their representatives and express their preferences for how they will be governed. Naturally, the integrity of the election process is fundamental to the integrity of democracy itself. The election system must be sufficiently robust to withstand a variety of fraudulent behaviors and must be sufficiently transparent and comprehensible so that voters and candidates can accept the results of an election. Unsurprisingly, history has several examples of elections being manipulated in order to influence their outcome.

Our objective in this paper is to explore the security related issues and flaws in DRE and particularly in EVM and its alternative is to use e-Voting i.e. Internet Voting as a major replacement.

We believe that this paper provides a valuable analysis of e-voting which in all likelihood become real in near future. Specifically, it describes how a voter , election commission, election candidates and whole nation can rely on this environment which is meticulously secure and robust. Cryptography, authentication, verifiability can be enhanced in E-voting to a level, which would be cross examined by the authorities time to time.

The Design of a good voting system, whether electronic or traditional paper ballots or mechanical devices, must satisfy a number of sometimes competing criteria. The anonymity of a voter's ballot must be preserved, both to guarantee the voter's safety when voting against a malicious candidate, and to guarantee that voters have no evidence that proves, which candidates received their votes. The existence of such evidence would allow votes to be purchased by a candidate. The voting system must also be tamper-resistant to thwart a wide range of attacks, including ballot stuffing by voters and incorrect tallying by insiders.

Main Objectives of an Efficient Voting System

a) Eligibility: The system should be "democratic" in the sense that it will permit only eligible voters to vote and will ensure that each eligible voter can vote only once (un-reusability).

b) Privacy: The system should ensure that none of the stakeholders viz. organizers, administrators, voters etc. involved in the voting process can link any ballot to the voter who cast it, and that no voter can prove that he or she voted in a particular way.

c) Integrity: The necessary mechanism should be employed in order to guarantee that none can duplicate his or someone else's vote and none can change someone else's vote

d) Accuracy: The system functionality should ensure that none can falsify or modify the result of the voting by eliminating a valid vote or counting an invalid vote in the final tally.

e) Verifiability: The system should ensure independent verifiablity that all votes have been counted correctly.

f) Convenience: The system should allow and assist voters to cast their votes quickly, within the stipulated time and with minimal equipment or special skills.
g) Flexibility: The system should allow a variety of ballot formats and it should be customized to the specific characteristics of the voting processes.
h) Mobility: The system should not pose any restrictions on the location from which a voter can cast a vote.
i) Efficiency: The election can be held in a timely manner (i.e. all computations during the election are done in a reasonable amount of time and voters are not required to wait on other voters to complete the process).
j) Scalability: The size of the election should not drastically affect performance.
Privacy issues and cryptographic issues are also covered in this paper.
Since there are, currently, no open standards in the area nor any directly related working groups on the issue of E-Voting.

II. ELECTRONIC VOTING

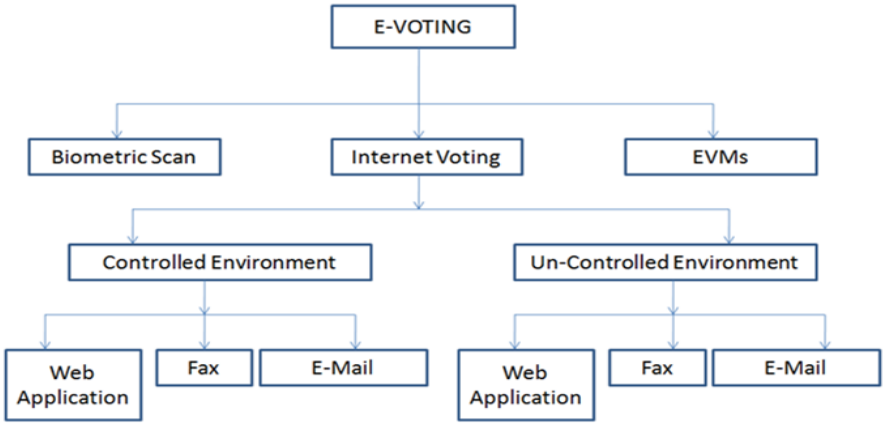

Figure-1 depicts the taxonomy of E-Voting systems.

There have been several studies on using computer technologies to improve elections [11, 5, 12, 14, 15]. These studies caution against the risks of moving too quickly to adopt electronic voting machines because of the software engineering challenges, insider threats, network vulnerabilities, and the challenges of auditing. Despite the opposition of computer scientists, this has led to increasingly widespread adoption of "direct recording electronic" (DRE) voting systems e.g. Electronic Voting Machines (EVMs). DRE systems, generally speaking, completely eliminate paper ballots from the voting process. As with traditional elections, voters go to their home precinct and prove that they are allowed to vote there,perhaps by presenting an ID card or a voter card. After this, the voter presses the button on the ballot unit of EVM of his / her choice containing the list of candidates.
Figure shows an EVM used in Indian Elections.

Figure-2 of an Electronic Voting Machine (EVM).

The most fundamental problem with such a voting system is that the entire election depends on the correctness, robustness, and security of the software within the control unit. Software have security flaws, which may be exploitable either by unscrupulous voters or by malicious insiders. Such insiders may be election officials, the developers of the voting system, and the developers of the embedded operating system on which the voting system runs. If any party introduces flaws into the voting system software or takes advantage of pre-existing flaws, then the results of the election cannot be assured to accurately reflect the votes legally cast by the voters.
Although there has been cryptographic research on electronic voting [13], and there are new approaches such as [6], currently the most viable solution for securing electronic voting [12]. EVM's (Electronic Voting Machines) are being used in some countries including India.

Security Issues in DRE (EVMs)
Many technology security experts, believes it is necessary to consider four required characteristics that a successful votin g system must have. These are accuracy, anonymity, scalability and speed.

Two major security attacks that are described briefly [1] involve physical tampering with the EVMs' hardware. In this paper it is very well demonstrated as how dishonest election insiders or other criminals could alter election results by replacing parts of the machines with malicious look-alike components.

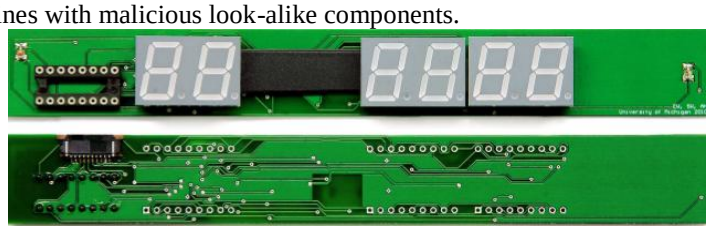

Figure No. 3 of Display Board of an EVM

Such security attacks are made far simpler and cheaper by the EVMs' minimalist design, and they could be accomplished without the involvement of any engaged poll officials. Another attack shows how attackers could use portable hardware devices to extract and alter the vote records stored in the machines' memory, allowing them to change the election figures and outcomes which also violate ballot secrecy. These EVMs' are not even have a secure cryptographic protocol to save its vote contents inside its memory. The goal of cryptography has been to render messages unintelligible and their use certainly predates digital computer systems. But this attack is technically straightforward because the EVMs do not use even basic cryptography to protect vote data internally. There is no use of Symmetric or Public Key cryptography in EVMs'. DRE (direct recording electronic) voting systems have been widely criticized elsewhere for various deficiencies and security vulnerabilities: that their software is totally unsecure and proprietary; that the software undergoes insufficient scrutiny during qualification and certification; that they are especially vulnerable to various forms of insider (programmer) attacks; and that DREs have no voter-verified audit trails (paper or otherwise) that could largely circumvent these problems and improve voter confidence. On the one hand, election security has to be viewed as a component of national security, since the very legitimacy of democratic government depends on elections that are fair, open, trustworthy, and seen to be so. This would argue for the very highest security standards—ideally that not a single vote be lost, forged, spoiled, miscounted, bought, or sold, and that the voter not be coerced or have his/her privacy compromised under any credible threat scenario, even if the attacker has significant resources, full knowledge of the voting system , and an inside confederate.

On the other hand, absentee voters vote from somewhere other than the precinct polling location, traditionally by marking or punching a paper ballot and mailing it back to the county officials, although faxing is sometimes permitted. In some western states 30% or more of all votes are absentee; Oregon in particular has eliminated its precinct polling places, so all votes there are absent. Any truly democratic voting system must have ways of dealing with five important threats. A first serious threat is disenfranchisement, either of individuals or of classes of voters. A major concern is that particular classes of voters could be disenfranchised, based on the likelihood of their voting a particular way. A second threat is that a voter's ballot could be modified by a third party. With conventional paper ballots, this could be done by, say, adding a vote for an office for which the voter had not voted or by invalidating the voter's ballot by adding too many additional votes. A third threat is the loss of privacy—the undermining of the secret ballot. Voting at a properly-managed precinct polling station on paper ballots that are mixed with others in a physical ballot box is the best protection for privacy. But what when an insider poll official breaks the seal and destroys the ballot papers. But the things become more vulnerable when it is an EVM machine. Since the ballot is immediately mixed with other ballots in the box, it is virtually impossible to reconstruct who cast which ballot within a precinct. It is much harder to protect the absentee voter's privacy when voting is done using paper absentee ballots filled out at home or at work and sent through the mail, and harder still when an electronic absentee ballot is processed by a large amount of software on several different computers.

A fourth threat, a well-known type of voter fraud, is that a voter may vote more than once. This offers tremendous opportunity for vote fraud, particularly to those who have access to the ill or infirm or those who do not have the ability to resist the influence of another as they are urged to vote in a"required" manner. It also encourages those inclined to commit voter fraud to seek to utilize absentee ballots provided to those whose interest in voting is marginal or non-existent.2

A fifth threat, intrinsic to absentee voting, is vote buying, selling, and trading.

Finally, a theme that all these threats have in common is the issue of scale. Computers are extremely good at automating repetitive tasks, but this cuts both ways: It is also easy to use computers to automate attacks. When computer security systems fail, typically they fail on a large scale. A major risk in any centralized Internet voting scheme like SERVE is that a single failure could affect hundreds of thousands of voters. SERVE (A Security Analysis of the Secure Electronic Registration and Voting Experiment) an Internet-based voting system being built for the U.S. Department of Defense's FVAP (Federal Voting Assistance Program)[16].

Malfunctioning of EVMs' is eminent everywhere in India during elections and due to this strong fact Election Commission is not considering the seriousness of the Voting by the general public when country's resources are at sake. One such letter[8] which was written by the Under Secretary (India) to all the Electoral Officers of India regarding the necessary protocol to be followed as the cases of malfunctioning of EVMs' during elections were reported from many places across India [8].

"Democracy at Risk" a book by GVL Narshimha Rao [2] published in 2010 briefly explained the major flaws in our EVMs' and stated many vulnerable security flaws which is open to public and Government as well.

This book is a truth about the false impression of EVMs' and acknowledged by Sh. L.K.Advani, Indian Leader, Sh. Chandra Babu Naidu, former Chief Minister of Andhra Pradesh state of India and Prof. in Computer Science Department David L. Dill, Stanford University.

This book states that, "Election integrity cannot be assured without openness and transparency. But an election without voter-verifiable ballots [physical proof of voting] cannot be open and transparent: The voter cannot know that the vote eventually reported is the same as the vote cast, nor can candidates or others gain confidence in the accuracy of the election by observing the voting and vote counting processes." "There is no reliable way to detect errors in recording votes or deliberate election rigging with these machines. Hence, the results of any election conducted using these machines are open to question."

E-Voting (Internet Voting)

Internet voting means the casting of a secure and secret electronic ballot that is transmitted to Election officials over a secure channel using Internet network as a medium for reliability.

In the year 2000, the State of Geneva began to develop an internet voting application. Geneva is therefore the public entity with the longest experience of internet voting in the world. People are more and more mobile, these days, whether we are educationist, doctors, engineers, bankers, nurse or working in the field of tourism, living abroad for a few years has almost become a necessity in a modern career. We maintain cross-border friendships, our relational networks span several countries and we often identify with more than one state. So people can vote from anywhere they want over internet network.

Security issues in E-Voting (Internet Voting) and their solutions.

Every voter can confirm that their vote is accurately counted, without violating ballot secrecy. Voters are provided with an encrypted ballot. Encrypted ballots are posted to a secure web bulletin board. A (universally) verifiable, anonymous tabulation is performed on the posted receipts.

Case I:

Scratch & Vote (S&V)[3], a cryptographic voting system. The main issue in the Electoral process discussed earlier in this paper was designed to minimize cost. Country's financial resources, manpower, time etc are being at disposal while conducting Elections. Day by day election process is getting more complex. Ballot papers can be printed in such a way that nobody can duplicate it using today's technology (1) ballots are paper-based and can be printed using today's technology, (2) ballots are universally verifiable without election- official intervention, and (3) tallying requires only one trustee decryption per race, thanks to homomorphic aggregation. The Paillier public-key cryptosystem [4] provides semantically secure encryption, efficient decryption, and an additive homomorphism by cipher text multiplication.

Case II:

Internet Voting needs to combine the apparently conflicting requirements of privacy and verifiability, briefly explain the privacy required that a vote cannot be traced back from the result to a voter, while on the other hand, verifiability states that a voter can trace the effect of her vote on the result. Many privacy enabled cryptographic primitives are formulated, which also offer verifiability. It is sure from this paper that first we must address the problem of privacy and later the issue of verifiability. Various methods pertinent to aforesaid issues are illustrated in this paper. The building blocks that are demonstrated are homomorphic encryption, re-encryption, blind signatures, zero knowledge proofs, designated verifier proofs, secret sharing, mixnets, communication channels with privacy properties, and tamper-resistant hardware.

Case III:

One more research paper [10] drew the attention towards a new kind of receipt which is a type of security as well as verifiability by letting voters verify the election outcome even if all election computers and records were compromised. The system preserves ballot secrecy, while improving access, robustness, and adjunction, all at lower cost.

Digital signatures are printed in the barcode on the last inch of the receipt layer. Such signatures have legal standing in many countries, and are considered irrefutable proof of the signed message's origin. A verifier outside the polling place can scan your receipt to immediately check, among other things, that its signature is valid, that an authorized voting station generated it, and that it correctly covers all the data printed. If the signature doesn't pass, the physical receipt is direct evidence of system failure. If the receipt does check, however, it cannot be credibly denied a place in the definitive receipt batch. Cryptographic techniques are classified as either un- conditionally secure or computationally secure.

The receipt system uses computationally secure encryption to form the layers, which ultimately encrypt the data in receipts and batches, and thus protect privacy and ballot secrecy. After voting, the codes protecting receipts and posted batches, which are only readily linkable to ballot numbers and not people (apart from perhaps the case of provisional ballots), can easily be as good as those protecting comparable and much more identifiable, sensitive, and detailed data traveling on networks today.

III. CONCLUSION

In this paper we have analyzed issues of security in EVM used in many countries in their election process. Strong demerits were reported in our paper regarding the hardware and functioning of EVMs'.

Traditional authentication and authorization mechanisms cannot fully cover the security requirements of the administrative workflow in EVM. An extension of the authentication-authorization scheme is necessary only when cryptographic mechanism is put in place. Three cases were discussed in Internet Voting, which requires Privacy, Verifiability and Coercion and could be easily put in place in Internet Voting, which requires strong cryptography and willingness of the Governments to make this change happen.

REFERENCES

[1] Wolchok, Scott, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp. "Security analysis of India's electronic voting machines." In Proceedings of the 17th ACM conference on Computer and communications security, pp. 1-14. ACM, 2010.

[2] GVL Narshimha Roa, "Democracy at Risk" in Title of His Published Book, Ist ed. New Delhi, India, Sharp Prints, 2010.

[3] Adida, Ben, and Ronald L. Rivest. "Scratch & vote: self-contained paper-based cryptographic voting." In Proceedings of the 5th ACM workshop on Privacy in electronic society, pp. 29-40. ACM, 2006.

[4] Stern, Jacques, ed. Advances in Cryptology-EUROCRYPT'99: International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceedings. No. 1592. Springer, 1999.

[5] David Baltimore and Charles M. Vest," Voting: What Is; What Could Be," California Institute of Technology and Massachusetts Institute of Technology,Report of the Caltech / MIT voting technology project, California July 2001.

[6] Chaum, David. "Secret-ballot receipts: True voter-verifiable elections." IEEE security & privacy 2, no. 1 (2004): 38-47.

[7] Jonker, Hugo, Sjouke Mauw, and Jun Pang. "Privacy and verifiability in voting systems: Methods, developments and trends." Computer Science Review 10 (2013): 1-30.

[8] K.N.Bhar, (2007, October, 14). Letter No. 51/8/16/4/2007 PLN-IV Dated: 12th October, 2007. [Online] Available:www.eci.nic.in

[9] Shubina, Anna M., 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, pp. 29-39. 2004.

[10] Chaum, David. "Secret-ballot receipts: True voter-verifiable elections." IEEE security & privacy 2, no. 1 (2004): 38-47.

[11] Gibson, Rachel. "Elections online: Assessing Internet voting in light of the Arizona Democratic primary." Political Science Quarterly 116, no. 4 (2001): 561-583.

[12] Mercuri, Rebecca. "Electronic voting." URL http://www. notablesoftware. com/evote. html (visited 2004, December 6) (2001).

[13] Gritzalis, Dimitris A. "Principles and requirements for a secure e-voting system." Computers & Security 21, no. 6 (2002): 539-556.

[14] C.D. Mote, Jr. , Report of the National Workshop on Internet Voting:Issues and Research Agenda, Conducted in cooperation with the University of Maryland and hosted by the Freedom Forum, March, 2001.

[15] A. D. Rubin, Report on Security considerations for remote electronic voting. Communications of the ACM,45(12):39–44, Dec. 2002.

[16] Jefferson, David, Aviel D. Rubin, Barbara Simons, and David Wagner. "A security analysis of the secure electronic registration and votingexperiment (SERVE)." New York Times (http://www. servesecurityreport.org) (2004)

