Electronic Voting Machine

COP290

Samarth Aggarwal
2016CS10395

Prof. Subhashis Banerjee
CSE IITD
suban@cse.iitd.ac.in

1 Aim

I intend to design of an Electronic Voting Machine (EVM), that satisfies the properties that an ideal Electronic Voting Machine should satisfy.

2 Abstract

An elections is the core pillar of any democracy. The Election Commission of India has enforced that the voting must be conducted using Electronic Voting Machines. However, in the recent past, EVM's have been stuck in various controversies.

Before moving on to designing a new EVM model, let's first look at the current EVM model and evaluate its positives and negatives.

I have discussed different methods of voting in this document along with their limitations. I have also discussed the key features that an EVM must have in order to be deemed as ideal. Further, I have dwelled on whether all these properties are satisfiable at the same time or not. I have also shed light on the performance of the current system in light of these properties. Finally, I have proposed a new design for EVM model that overcomes most of the vulnerabilities of the present design. The proposed design is reasonably close to the ideal EVM that we intended to design. Hence, I have tried to enlist all the vulnerabilities of the present design and have tried to cure them in my proposed design.

3 Present EVM Model

In the present system, an Electronic Voting Machine consists of a Control Unit and a Balloting Unit, joined by a five-meter cable. The Control Unit is with the Presiding Officer or a Polling Officer and the Balloting Unit is placed inside the voting compartment. Instead of issuing a ballot paper, the Polling Officer in-charge of the Control Unit will press the Ballot Button. Only when the officer presses this button, will the voter be able to cast his vote by pressing the blue button (corresponding to the candidate of his/her choice) on the Balloting Unit. During counting, control units are sealed off and votes are counted through a device. During voting, the current EVMs also print a ticket that act as a VVPAT and is displayed for about 7 seconds. The ticket is then stored and sealed in a container. VVPAT essentially acts as a verification token to the voter thereby validating the correctness of the machine.

3.1 Evaluation of the Current EVM Model

The present design is highly prone to hardware level attacks although it is reasonably secure towards software level attacks and hacks. This is because the chips used in these machines are one time programmable chips and hence cannot be reprogrammed by any individual.

- **Software Tampering before chip programming** There is no check on whether the software is what it was intended to be. There is be a possibility that political parties are using the software creating firm to sneak in malicious code into the hardware and thereby influencing the election process.

- **Replacement CPUs with their look-alikes** CPUs are a commodity and can easily be replaced when being moved from one place to the other. There should be a way to ensure cryptographically by the firmware that the CPU is not tampered with using some private keys and that the CPU received is the same as what was intended to be received. This security is not present in the current EVMs.
- **Replacement circuit boards with their look-alikes** This attack is even simpler than the previous one. Attacker needs to replicate the whole circuit board with his malicious circuit board within the control unit.
- **Replacement units with their look-alikes** Currently there is no mechanism to test whether the EVM machine arrived is the authenticate machine or some exchanged and tampered machine.
- **Ease of use** Process should be simple enough for an illiterate to cast a vote with ease. The present EVM model fulfills this requirement very well.
- **Safeguard against Booth Capture** One needs to ensure that even if the booth is captured by some party, then there is a way to maintain all the properties. Presently, if a booth is captured then the Election Commission declares election in that constituency null and void. The elections have to be conducted again in that constituency which costs the government a lot.
- **History Independence** Process should not store history of processes and should be random enough to make it time independent. The present EVMs do not ensure this property.
- **Evidence of Tampering** We cannot say whether an EVM has been tampered or not during the election process. However, such an statement should be easy to make in case of an ideal EVM.

4 Key Features of an Ideal EVM

- **Authentication and Authorization** Machine should be able to authenticate the correct voters and authorize them to cast their vote.
- **Coercion Freedom** Coercion is the practice of forcing an individual to act in an involuntary manner by use of threats or force. Coercion freedom means that there should be no way to force someone to vote for the candidate he/she doesn't want to.
- **Secrecy** Secrecy refers to maintaining the confidentiality of the data(vote) of every person. There should be a way to ensure that no one can see or deduce other's vote. This could be done through proper methods of cryptographic layers.

- **Non-Repudiation** Non repudiation is a property by which the rightful owner of the vote/data cannot claim the falseness of his data. There should be a mechanism to prove that he had voted for that particular candidate against whom his vote is counted in the database.

- **Uniqueness of Votes** - One Vote per voter. Machine should be able to dismiss/ not allow more than one votes from a person.

- **Verifiability** Voter should somehow be able to verify that his vote increases the vote count of the candidate for whom he has voted and not any other candidate. This also includes proving to the voter that his vote was taken care of in reaching the result of election, ie. his vote was considered while counting.

- **Anonymity** Anonymity is the phenomenon in which its not possible to get the details of the vote caster from the voting data. In complete anonymity, the data/vote has no relation with the person in space or time, but it somewhat clashes with non-repudiation.

- **Self-Certifiability** Machine should be able to check itself for its correctness and integrity and thus provide a proof. In case the integrity of the machine fails at any point of time, the machine should itself alert about the fault.

- **Auditability** There should be a digitally signed/ authorised text/electronic document to confirm the candidate that I voted for.

- **Message Integrity** Message integrity is the assurance that the data is tamper proof and can't be altered.

4.1 Other Factors to consider

- **Cost** Only the solutions the are financially feasable are possible to implement hence the budget itself acts as a constraint.

- **History independence** Process should not store history of processes and should be random enough to make it time independent.

- **Natural hazards** EVM should work in extreme weather conditions as well. They should be tested in diverse weather conditions.

- **Safeguard against Booth Capture** One needs to ensure that even if the booth is captured by some party, then there is a way to maintain all the properties.

- **Ease of Use** Process should be simple enough for an illiterate to cast a vote with ease.

- **Evidence of Tampering** One should be able to detect if an EVM was tampered during the election process.

- **Electricity** Electricity supply cannot be assumed to be consistant especially in a country like India. Hence, the machine should not be affected due to power failures.

5 Proposed Design

5.1 Assumptions

- Booth capturing has to be controlled by the police.
- Every candidate is visible as an option to every voter.

5.2 Brief Description of Whole Voting Process

Each voter is assigned a specific polling booth. He/she cannot vote in any other polling booth. Although the voter is free to have his polling booth changed in future in case his address changes or if some other booth is more approachable for him. The voter enters the booth on his/her turn. The voter id card contains a barcode, which is needed to be scanned in order to vote. Initially the buttons for voting are disabled. The software checks that the voter votes only once. If the voter is registered to vote at that booth and the voter is not recasting his vote in the same elections then the voting buttons are enabled. The screen shows a unique screen id and a random enumeration of check boxes with the names of candidates beside it. As soon as the voter clicks a button, a VVPAT showing the name of the candidate he/she has voted for shows up and goes back inside the machine. A slip containing the screen id and the selected check box no. (without candidate name) is printed.

After the voting process ends, a list is released in which the voter can compare his/her screen id with the checkbox no. which acts as a proof of the fact that his/her vote has been counted.

5.3 Database Structure

My model of Electronic Voting Machine contains three databases which contains the following data :

1. **Voters Information** - The list of all eligible voters in any specified polling booth along with their barcode and the information of whether they have already voted or not.
2. **Candidate Information** - A list containing the candidate name, corresponding parties, party symbol and vote count.
3. **Hash Information** - A hash containing the Screen Id as key and selected checkbox number as value.

5.4 Hardware Integrity

I plan to have a BIST for my EVM model to be able to check its correctness anytime, anywhere. A built-in self-test (BIST) or built-in test (BIT) is a mechanism that permits a machine to test itself. We can use Logic built-in self-test (or LBIST) which is a form of built-in self-test (BIST) in which hardware and/or software is built into integrated circuits allowing them to test their own operation, as opposed to reliance on external automated test equipment. The advantage of this is that we have excluded the possibility of an external testing agent tampering with the machine or providing false test results. The Logic of LBIST involves a multi-level encryption. For example, using a 3-level hashing with the key as model number of EVM, Date of Manufacturing and a random salt. This will be unique for each EVM and can be stored in a secure database.

eg.

- Model No. : 2016CS10395
- Salt : NaCl
- Manf. Date : 01052018
- MD5 hash1 (of Model using Salt) : 6df71d11fbe7970e88cb46d206ebc3d5
- MD5 hash2 (of hash1 using Manufacturing Date) : 629e09aa56a1ac3d41867f1fb9b41634

The untampered EVM's BIST should run some program on the circuit / or use it's inherent properties and should be able to generate the MD5 hash2. Then the OS hash this output using another inbuilt salt and then use this as and input for another program. If the hash is incorrect, an alarm / led is turned on. If it fails any of these tests (display hash or alarm / led), it is known that the EVM has been tampered with.

5.5 Proving that Counting of votes is Correct

The candidate name shown over VVPAT does not come from the button pressed, but rather comes from the computation done on the backend. Hence it represents the data received by the system, not merely what has been entered by the voter. Ofcourse, a mismatch indicated error in counting.

Let count1[i] = no. of votes of candidate 'i' before pressing button

Let count2[i] = no. of votes of candidate 'i' after pressing button

Check : $\Sigma(count2[i] - count1[i]) = 1$

If the check fails than error is reported.

If count2[i] - count1[i] = 1, then the slip shows candidate[i]

5.6 Key Features Satisfied by my Design

- **Coercion Freedom** The printed slip provided to the user contains only the checkbox no. and the screen id. Since the checkbox list is random, there is no way for the voter to prove to whom did he vote. Since, any goon cannot verify the vote of an individual even if the voter is kept at gunpoint, hence there is no guarantee for the goon that even after threatening the voter to vote for a particular candidate, the voter has voted for that candidate. So coercion is prevented.
- **Authentication and Authorization** The voter information database of EVM handles the authenticity and authorization of the voters.
- **Verifiable** The voter can verify that his/her vote has been counted by checking the checkbox corresponding to the screen id published after the voting process.
- **Anonymity** Anonymity is ensured since there is no relationship between the voter and the vote he/she has casted.
- **Secrecy** The vote is casted in a closed room which contains the voter alone and no one can get to know about the candidate he/she has voted for. So secrecy of the voting procedure is intact.
- **Message Integrity** Message integrity is ensured as every process in EVM has to pass through hashing mechanism.
- **Auditable** The VVPAT shows the name of the candidate whom the voter has voted for.
- **Uniqueness of Votes** The EVM dismisses the voter who has already casted the vote by not enabling the voting buttons. Hence one voter can vote only once in the proposed design.
- **Self-Certifiable** The EVM model uses BIST to test their own operation, rather than relying on external automated test equipment.

6 Citations

- http://shodhganga.inflibnet.ac.in/bitstream/10603/118518/8/08_chapter-iii.pdf
- https://indiaevm.org/evm_tr2010-jul29.pdf

Discussed With :-

Ayush Patel (2016CS10396)
Atishya Jain (2016CS50393)
Mayank Singh Chauhan (2016CS50394)
Ansh Sapra (2016CS50392)
Mankaran Singh (2016CS50391)
Avaljot Singh (2016CS50389)