A Case Study on Electronic Voting Machine(EVM)

Mohit Gupta(2016CS50433)

April 28, 2018

1 Introduction :

India is the largest democracy in the world and no other country in the world has used electronic voting in as large scale as India has. Elections constitute an important part of India's democracy and so it is important that the election procedure is fair. For this, the Electronic Voting Machine should satisfy some important functionalities while also trading off between some if all can't be satisfied simultaneously.

This paper focuses on the current Electronic Voting System, Important functionalities EVM should meet, fallouts in the cuurent EVM and finally proposes a new one satisfying the functionalities discussed earlier.

2 Electronic Voting System in India and EVM Operation :

India's EVMs have two main components :

There is a **control unit**, used by poll workers, which stores and accumulates votes, and a **ballot unit**, located in the election booth, which is used by voters. These units are connected by a 5 m cable, which has one end permanently fixed to the ballot unit. The system is powered by a battery pack inside the control unit. The EVMs are designed for one or two-race elections, as are typical in India.

The ballot unit has 16 candidate buttons. If any are unused, they are covered with a plastic masking tab inside the unit. When there are more than 16 candidates, an additional ballot unit can be connected to a port on the underside of the first ballot unit. Up to four ballot units can be chained together in this way, for a maximum of 64 candidates. A four-position slide switch under the ballot unit door selects the unit's position in the chain.

2.1 Election Procedure :

- Prior to the election, workers set up the ballot unit by attaching a paper label that shows the names of the candidates and their party symbols (to aid illiterate voters) next to the candidate buttons.

- On the morning of the election, poll workers perform a small mock election to test the machine. They then publicly set the totals to zero by pressing the clear button, after which the control unit display shows that a total of zero votes have been cast. Workers can check this count at any time by pressing the total button.

- Seals are then placed on various parts of the control unit to block access to counting and clearing functions until later in the election process.

- When a voter arrives, workers verify his or her identity and record the voter's presence by obtaining a signature or thumb print. To prevent double voting, they mark the voter's right index finger with indelible ink.

- Next, a poll worker presses the ballot button on the control unit to allow one vote.The voter enters the polling booth and presses the button for the candidate of his or her choice. A red light next to the candidate button glows, the ready light turns off, and the control unit emits a loud beep to indicate that the vote has been cast.

- This process repeats for each voter. On the **counting day**, the control units are delivered to a counting center. In public view, an election official breaks a seal on the control unit and presses the result button and The display on the control unit shows a sequence of outputs: the number of candidates, the total votes, and the number of votes received by each candidate. Officials manually record the totals from each machine and add them together to determine the election result.

3 Challenges(Fallouts in current EVM :

1. **Cryptographic Methods :** The EVM doesn't make use of cryptographic methods which are much more secure than relying on raw information to be transported which is susceptible to various threats.

2. **Hardware Integrity :** The EVMs once designed, can't be checked for hardware integrity. The manufacturers may plant a bug in the system which transmits data to them or may be even open to changes remotely.

3. **Tampering with Machine State :** Even if every component of the system behaves honestly, attackers could still attempt to manipulate the system by directly accessing or manipulating the internal state of the machine in ways not contemplated by its designers. This is made easier because the machines are designed to use a simple I2C serial interface to link the CPU to the memory chips, and because the simple software design does not attempt to cryptographically pro- tect or authenticate the data stored there.

4. **Is the output displayed correct? :** Integrity of the display is also another issue. The display can be replaced to display votes entirely different from those recorded.

5. **Mechanical Seals :** The EVMs rely on mechanical seals with stamps which can be easily broken, the data tampered with, and replaced without anyone being able to make that out.

6. **Substituting Look-Alike Units :** Voters and poll workers have no practical way to verify that the EVMs they use are authentic, so attackers might try to build identical looking but dishonest control units or ballot units and substitute them before an election.

4 Important Functionalities of Electronic Voting Machine :

1. **Uniqueness :** No voter should be able to vote more than one time. Each eligible voter should vote only once, and only for the office for which she is authorized to cast a vote.

2. **Secrecy(Anonymity) :** It is the responsibility of the Election Commission to maintain the secrecy of votes cast by the voters.Votes must be protected from external reading during the voting process.All communication between voter and election authorities occurs over an anonymous channel.

3. **Coercion-Freedom :** Coercion is the practice of forcing another party to act in an involuntary manner by use of threats or force. In any voting system it says that the voter cannot be forced to cast his vote to some party or even cast his vote if he doesn't wish to do so.

4. **Non-Repudiation :** Non-repudiation is also necessary, preventing the voter from later saying that the authentication had been wrong. Hence, there should be a mechanism to prevent the voter from later denying that he didn't vote or he voted to someone else.

5. **Verifiability and Auditability :** It should be possible to verify that all votes have been correctly accounted for in the final election tally, and there should be reliable and demonstrably authentic election records.

   An auditable process is one where a proof of correctness can be given to everyone affected by the process. In our case, it will be each and every citizen of our country. It should be provable that there is no bias or unfairness in the entire voting procedure including recording and counting of votes. Most of the systems satisfying auditability issue a receipt to the voter whom he voted for.

6. **Integrity :** Votes should not be able to be modified, forged, or deleted without detection. It should be impossible for a validated vote to be eliminated from the final tally. It should also be impossible for an invalid vote to be counted in the final tally.

- **System integrity :**The computer systems must be tamperproof. Vote counting must produce reproducibly correct results. Ideally, system changes must be prohibited throughout the active stages of the election process. That is, once certified, the code, initial parameters, and configuration information must remain static. No run-time self-modifying software can be permitted. End-to-end configuration control is essential.
- **Data Integrity and Reliablity :** All data (including votes, vote counts ...) involved in entering and tabulating votes must be tamperproof. Votes must be recorded correctly without being altered during transit, processing, or in storage.

7. **Cryptography(To prevent Information Leakage) :** An effcient way to maintain security of our data is to encrypt it as soon as it is recorded and decrypt it only if needed at a later time point. Data not sensitive to voters would be enough to declare election results.

5 Proposed Electronic Voting System

The system we are going to propose in this paper will address all these security concerns by using open source code to develop our e-Voting system, and rely on Blockchain technology to secure votes, and decentralize the system.

Using Blockchain Technology :

Blockchain is an ordered data structure that contains blocks of transactions. Each block in the chain is linked to the previous block in the chain. The first block in the chain is referred to as the foundation of the stack. Each new block created gets layered on top of the previous block to form a stack called a Blockchain.

Each header contains information that links a block to its previous block in the chain, which creates a chain linked to the very first block ever created, which is referred to as the foundation. The primary identifier of each block is the encrypted hash in its header. A digital fingerprint that was made combining two types of information: the information concerning the new block created, as well as the previous block in the chain.

As soon as a block is created, it is sent over to the Blockchain. The system will keep an eye on incoming blocks and continuously update the chain when new blocks arrive.

Hardware Developments :

- **Verification of Hardware and Software** While manufacturing, the EVM will be verified to have the correct memory chip, display and the software.
- **Replacing Mechanical seals :** In the existing system, the EVMs rely on mechanical seals at each and every step. As discussed in the limitations, these mechanical seals are easy to tamper with. We plan to introduce electrical seals instead of mechanical ones. At each and every step where want to seal our system, the seal can be imposed by clicking a button and if someone tries to tamper an alarm turn on.

5.1 Procedure of the Electronic Voting System

- **Requesting to vote :** In our proposed system, the EVM contains an encrypted key mapped to a particular voter ID and the information of the encrypted key is with the Election commision.

  The user will have to log in to the voting system using his credentials, and the voting confirmation numbers provided to registered voters by the Election Commission. The system will check all information entered and, if matched with a valid voter, the user will be authorized to cast a vote. Our e-Voting system will not allow participants to generate their own identities and register to vote. Systems that allow identities to be arbitrarily generated are usually vulnerable to attacks.
- **Casting a Vote :** After authentication, the machine has the encrypted key that was mapped to the Voter ID of the candidate. Voter will have to choose to either vote for one of the candidates or cast a NOTA. Casting the vote will be done through a friendly user interface.
- **Encrypting and storing votes :** After the user casts his vote, the system will generate an input that contains the mapping between encrypted key and the voter identification number followed by the complete name of the voter as well as the the candidate ID.. This way

each input will be unique and ensure that the encrypted output will be unique as well.

- **Adding the vote to the Blockchain :** After a block is created, and depending on the candidate selected, the information is recorded in the corresponding Blockchain. Each block gets linked to the previously cast vote.

6 Evaluating the design against required functionalities :

- Blockchain technology is extremely secure till date. The hardware doesn't work if the electronic seals are broken. So, our system cannot be tampered with, if they are, they become non-reusable for that election.

  Hence the functionalities of System Integrity and tamper-proofness are satisfied.

- If the voter comes and claims that he had voted but his vote is not counted, the EC can instantly check the blockchain to see if the block correcsponding to the private key of voter is there or not. If it is not there, it is proved that he didn't vote as it is impossible to delete a block from blockchain. Same holds for the case that voter says he didn't vote. The proposed system does provide later the individual voter the details of whom he had voted and this is just to make the system *Coercion free* as now the user can't be forced to vote as the data is encrypted.

  Hence the functionalities of Non Repudiability(To some extent) and Coercion freedom and Verifiability and accountability are satisfied.

- Since each voter first authenticates and has a unique private key assigned by the EC, *Uniqueness functionality is satisfied.*

  Moreover,Since, we are using blockchain technology which have been verified to be 100and even if it is, it can't be tampered or even be read since we are using secure encryption.

  So, the functionalities of Secrecy and Cryptography(Information Leakage) are satisfied.

6.1 There are Limitations too :

- Since, we are relying on the online mechanism of uploading various nodes of blockchain(from EVM), the threat of hacking does creep in.
- We assume that if any seal is broken, the system goes off which may cause problem for the authorities to reconduct the election.

7 References

1. Scott Wolchok, Eric Wustrow, J. Alex, Hari K. Prasad, Arun Kankipati, KrishnaSakhamuri, Vasavya Yagati, Rop Gonggrijp : *Security Analysis of India's Electronic Voting Machines*
2. Ahmed Ben Ayed : *A Conceptual Secure Blockchain-Based Electronic Voting System, International Journal of Network Security and its applications.*
3. Peter G. Neumann : *Security Criteria for Electronic Voting, 16th National Computer Security Conference, September, 1993*