Indian Institute of Technology, Delhi

Design Practices in Computer Science
COP290

Electronic Voting System Design

April 18, 2018
Department of Computer Science and Engineering
Indian Institute of Technology, Delhi

Author :
Udit Jain
(2016CS10327)

Supervisor :
Prof. Subhashish Bannerjee

ABSTRACT

I am going to design and present a model for an Electronic Voting System for India. In this document , I'll talk about many vital and essential issues that have to be taken into account while designing a Digital Voting system for India.

The Model will satisfy many properties which make it a good model. Then I will argue thet why is it a very good model to be implemented.
In this design project, I shall work as observers, developers and algorithm enthusiasts to understand the ways and finding different means to approach and tackle the objectives in a more well defined mathematical way.

Contents

Chapter 1

Introduction

The problem of Electronic Voting is one that is not limited to India, but a global problem. Using the cutting edge technology I hope to present a solution to this problem which will save us plants, workforce and sheer administrative manpower by a once effective and efficient investment by the governing body.

I survey the current voting system of Indian and I reconginse the potential concerns that need to be addressed before it can really be called a foolproof system. The following objectives are aimed to be discussed in this paper:

- Problem Description
- Current Voting system and it's safeguards
- Desirable properties
- Helpful Systems/Algorithms
- Model
- Correctness , scaling , feasibility and Implementation
- Epilogue/Conclusion

Chapter 2

Problem Description

2.1 Introduction

India is a constitutional democracy with a parliamentary system of government, and at the heart of the system is a commitment to hold regular, free and fair elections. These elections determine the composition of the government, the membership of the two houses of parliament, the state and union territory legislative assemblies, and the Presidency and vice-presidency. Elections are conducted according to the constitutional provisions, supplemented by laws made by Parliament. The major laws are Representation of the People Act, 1950, which mainly deals with the preparation and revision of electoral rolls, the Representation of the People Act, 1951 which deals, in detail, with all aspects of conduct of elections and post election disputes. The Supreme Court of India has held that where the enacted laws are silent or make insufficient provision to deal with a given situation in the conduct of elections, the Election Commission has the residuary powers under the Constitution to act in an appropriate manner.
The democratic system in India is based on the principle of universal adult suffrage; that any citizen over the age of 18 can vote in an election (before 1989 the age limit was 21). The right to vote is irrespective of caste, creed, religion or gender. Those who are deemed unsound of mind, and people convicted of certain criminal offences are not allowed to vote.

2.2 Current Voting System of India

2.2.1 Election Overview

Elections in India are events involving political mobilisation and organisational complexity on an amazing scale. In the 2004 election to Lok Sabha there were 1351 candidates from 6 National parties, 801 candidates from 36 State parties, 898 candidates fromofficially recognised parties and 2385 Independent candidates. A total number of 38,99,48,330 people voted out of total electorate size of 67,14,87,930. The Election Commission employed almost 4 million people to run the election. A vast number of civilian police and security forces were deployed to ensure that the elections were carried out peacefully.

Conduct of General Elections in India for electing a new Lower House of Parliament (Lok Sabha) involves management of the largest event in the world. The electorate exceeds 670 million electors in about 700000 polling stations spread across widely varying geographic and climatic zones. Polling station

Elections to the Lok Sabha are carried out using a first-past-the-post electoral system. The country is split up into separate geographical areas, known as constituencies, and the electors can cast one vote each for a candidate (although most candidates stand as independents, most successful candidates stand as members of political parties), the winner being the candidate who gets the maximum votes.

Candidates are required to file their nomination papers with the Electoral Commission. Then, a list of candidates is published. No party is allowed to use government resources for campaigning. No party is allowed to bribe the candidates before elections. The government cannot start a project during the election period. Campaigning ends at 6:00 pm on the second last day before the polling day.

2.2.2 How the voting takes place

The polling is held between 7:00 am and 6:00 pm. The Collector of each district is in charge of polling. Government employees are employed as poll officers at the polling stations.

Before EVM's

Voting is by secret ballot. Polling stations are usually set up in public institutions, such as schools and community halls. To enable as many electors as possible to vote, the officials of the Election Commission try to ensure that there is a polling station within 2km of every voter, and that no polling stations should have to deal with more than 1500 voters. Each polling station is open for at least 8 hours on the day of the election.
On entering the polling station, the elector is checked against the Electoral Roll, and allocated a ballot paper. The elector votes by marking the ballot paper with a rubber stamp on or near the symbol of the candidate of his choice, inside a screened compartment in the polling station. The voter then folds the ballot paper and inserts it in a common ballot box which is kept in full view of the Presiding Officer and polling agents of the candidates. This marking system eliminates the possibility of ballot papers being surreptitiously taken out of the polling station or not being put in the ballot box.

After EVM's

Electronic Voting Machines (EVMs) are being used instead of ballot boxes to prevent election fraud. After a citizen votes, his or her left index finger is marked with an indelible ink. In 2003, all state elections and bye elections were held using EVMs. Encouraged by this the Commission took a historic decision to use only EVMs for the Lok Sabha election due in 2004. More than 1 million EVMs were used in this election.

Chapter 3

Electronic Voting Machine

Note :- I surprisingly found little details on technical build of EVM on the election commision's EVM website (because ideally it should be open source for anyone and everyone to verify and srutnize)[Why should we take the TEC for their promises ?], whereas administrative arguments are quite prominently displayed.

3.1 Techincal Experts Comitee (TEC)

- Giving technical advice to build specs and newer vesions of EVM and VVPATs before they goes into production.
- Offers improvement in design and mentors companies in design and manufacturing process.
- Do Independent Evaluation and System Verification of EVM's integrity and submit detailed reports to Election Commision.
- Answers to the Election Commission about any queries like EVM's tamparibility that may be raised on EVM's design, manufacturing and processing.

3.2 Manufacturing

Two Public Sector Undertakings(PSUs) deal with manufacturing of safety critical , sensitive equipment and therefore have stringent security protocols.

3.2.1 *Secure* Design Features

- **Standalone Machine** : No wireless communication possible. Problems
- **One time programmable Chip** : No READ / WRITE possible after this being programmed. Problems
- **Clock** : Real time clock (standalone) to timestamp the keypresses. Problems
- **Diagnostics** : Automated self diagnostics introduced from 2013 M3 models . (But they are only as good as their components)

3.2.2 *Secure* Development process

- **Contract** : Software design and approved by TEC is never subcontracted. Problems
- **Software Validation** : Carried out as per SRS by Independent Testing group. Problems
- **Surveillance** : Entry and exit monitored by CCTV, electronic gadgets restricted. People frisked at checkpoints. Access Data and process data logging, alert generation during manufacture. Third party testing as per TEC quality standards. In the whole process the source code was only accesible to *"Authorized Personnel"* Problems

3.3 Administrative Safeguards

These may *possibly* prevent the many techincal flaws to be unearthed by attackers. But nevertheless they are only as good as the integrity of people enforcing these safeguards. That is to say , the techincal design model cannot sufficiently safeguard itself against tampering, vulnerabilities and other attacks.

- **Stakeholder Participation** : Participation of political parties and candidates in all processes. They try to not let other cadidates cheat.

- **Allocation Movement** : EVM's allocated to poll going states by commision. *Always* transported under 24/7 police escort.
- **First Level Checking** :
  1. Complete Physical checkup (swithces, latches, functional test etc).
  2. Mock poll on all EVMs. Defective ones escored to manufacturer. Results of mock polls shared with representatives.
  3. CU sealed after FLC with pink paper seal. *Which is inadequately secure against attacks* Signatures are not checked properly and can be forged after replacement of parts .
  4. Stored in Strong Rooms in 24/7 security.
- **Randomization** : Twice randomized using EVM tracking software at the district and then at constituency level, then 3rd randomization of polling station officials. If implemented properly, effctive against preplanning/fixing of increasing counting to a particualar voter, becuase of randomizaion they won't know which candidate gets which slot.
- **Mock Poll** : Before the actual voting with 1000 votes. A testing procedure but by no means a security safeguard, as the malicious code can easily be instructed to run after a preset number of votes.
- **Poll Day Checks** : By polling agents, CCTV, webcasting, observers and senior officers visiting, Media coverage
- **Poll Closure, Transportation and Storage Security protocols** : Close button on CU, EVMs sealed in carrying cases signed by polling agents. Transported back to reception centers under armed escort. Kept in strong room, observed by candidates, Double lock system, sealed rooms, and other security measures. VVPAT's paper slips sealed in black envelopes with the EVM's.
- **Counting Day Protocol** : Strong room opend in presence of candidates, videography. ID's of CU's and signed seals are verified.

3.4 Problems in Current EVM design

Critical flaws/loopholes/debatable things in current model are :

- In other countries, there are EVM's which are fully connected to the network Ex. Netherlands . Because our EVM is closed, we(the public) cannot monitor in realtime what is actually going on inside. But every kepress is logged and timestamped. And we are to belive even that can't be tampered with .
- We get the chips made from and outside contractors (Japan and America) because we don't have the technological infrastructure in India to manufacture the chips ourseleves. Ironically, the OTP doesn't allow the code to be read after burning, so we actually don't know if it actually contains the desired code, which is verified. It may constitute malicuous code for all we know, and may be triggered after say 1200 votes to bypass the mock poll criteria. The source code with is burned on chips is small(supposed to be security feature) and directly runs on the hardware. Because it is small, it can be reverse enginereed (that too in a matter of weeks) and this has been done by various labs for different chips. And they could then send a programmed chip *almost* identical in function. Also, chip replacement (substitution by look alike chips) can be done anywhere and anytime in the process, well before the elections. Even the whole control unit can be replaced with identical looking units . This opens up a big window for tempation and fraudlent activity.
- A simple I2C interface is used in IC's and it is not stored cyrptographically in memory(EEPROM), so other IC's can be made which will intercept the votes to the output (say the display unit) and directly compromise the authenticity and anonymity of votes.
- The clocks can be modified and substituted. And as each unit has a built-in self clock, they are not synchronized, which further enables any attacker to substitute or temporarily-shutdown the clock to do certain illegal keypresses which won't be time-logged.
- Who is to say that the contractor, manufacturer and validator(independent testing unit) themselves aren't rigged ? They ideally should test on

every possible test case, which is impossible. That happens because they don't ***prove*** the integrity of EVM model.

- Who are these *"Authorized Personnel"* having access to the source code ? What is to happen when an attacker gets their hands on it ? That is why it'll be much better to keep the code open sourced and under scrutiny by everyone.

- Remote alteration of CU's display is possible if we replace some parts inside, like replace a display unit with a look alike, which has a IC with a wireless module inside it which intercepts the votes, keeps the vote count same and increases the count of a candidate which is remotly selected on a mobile device. This attack was demostrated by Hari K Prasad, without any knowledge of source code. So it can be imagined that what vulnerabilities could be introduced by source code leakage.

- Without the desing open-sourced, we have trust issues like are VVPAT's *really* a secure way of authentically checking where the vote was cast ? And other problems in interconnections of various units of EVM like BUs CUs and VVPATs.

- Current EVMs are horrible at storing the data, they store it without any encryption in memory, that is horrendous and leads to information leakage, of the voters and maybe more security vulnerabilities.

Some vulnerabilities can be addressed as here.

Chapter 4

Desirable Properties

4.1 Introduction

After review of the security vulnerabilities in the current EVM design, we reach upon the following conclusive and complete rules which should guide our EVM design.
Things like Certifiablity of hardware , software and firmware checks are obviously needed, but here we look for more abstract level of properties. We also discuss which properties are hard to implement, and with reasonable administrative assumptions may be waived off. Because we may not be able to satisfy all the properties in a single design and there will be tradeoffs.

4.2 Properties

Now let's formally list the ideally desirable properties of an Electronic Voting System.

1. **Coersion** : Coersion freedom is when a candidate cannot force the voters to vote them and in any case shouldn't be able to forcibly see the candidate's vote. This is more of a social problem, and this will coflict with Verifiability of vote by self, because technically if you can correctly see your vote then, anyone can point a gun to your head and ask you to see what you voted for.
   So for practical systems, this property may be the first to go.

2. **Secrecy** : The design and modelling of the entire process should be open-source yet secure. Ex RSA Cryptosystem, the algorithm is well known yet resonably - unbreakable. This will also enable many more people to properly scrutnize and fix the voting process, as will it increase the number and knowledge of possible attackers.

3. **Non-Repudiation** : Policies must be implemented which would prohibit, and won't allow a voter to pose as someone else and that should be verifiable ie a user who voted is the one who he clamis to be.

4. **Veriafiable** : The users who voted, must be counted to the correct cadidate, no switching of votes or wrong accumulation. It should also verify to be fair, un-baised and fair, ie each and every voter gets one vote only.

5. **Cryptographic** : Data should be encrypted at each stage so any unauthenticated attacker cannot view the data (without the secure keys) even if the database is somehow leaked (worst case).

6. **Audit** : Proof of Correctness of entire voting process. And no one should be able to question it, as it should be reliable and veriafiable to that voter ie if someone comes, that prove to me my vote was casted to this particular party, the system should be able to give a proof of truthfullness / falsifyability of his statement.

7. **Anonymity** : My vote shouldn't be visible to anyone else, and should be correctly visible to me.

8. **Self Certifiablity** : The EVM's hardware, software and firmware should be self-certifiable. A proof of being tamper free and being correct.

9. **Infomation Leakage** : The model should have no sensitive information leakage .

Chapter 5

Useful Systems

5.1 RSA Cryptosystem

RSA is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem".
A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, and if the public key is large enough, only someone with knowledge of the prime numbers can decode the message feasibly.

5.2 Blockchain

A blockchain, originally block chain, is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data. By design, a blockchain is inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for internode communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority. Blockchains are secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain. This makes blockchains potentially suitable for the recording of events, medical records, and other records management activities, such as identity management, transaction processing, documenting provenance, food traceability or ***Voting***. Blockchain was invented by Satoshi Nakamoto in 2008 for use in the cryptocurrency bitcoin, as its public transaction ledger. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has been the inspiration for other applications.

Chapter 6

Model

As I currently gather, the security and technical flaws in the EVM are being shadowed and protected by the administrative safeguards. There may be a security flaw in the EVM's design, and it could theoritically be exploited, but the administrative safeguards make it impossible or very hard. The job the entire Technical Comitee (TEC) was to come up with a good EVM design, their design is far from perfect, some may even say sub-optimal. But being a undergrad student with very limited time, I am not able to create an entierly new model which rivals that of current Indian EVM. But these are the security vulnerabilities I would like to address :-

- Open sourcing the design, iterating and fixing the flaws until it becomes secure enough
- Manufacture of Chips in India, bring the change in necessary infrastructure so that atleast this type of chips can be manufactured in India itself.
- Cryptographic Storage

I also went through serveral existing government systems and theoritical systems online, one was a novel system at Cornell called CIVITAS . Links : 1 and 2.

These papers contain detailed algorithms and their proofs, which when implemented will satisfy almost all of the *desirable* properties listed above. It'll be secure, auditable, veriafiable, cryptographic, anonymous among other things.

But this model is not implementable in India, because it'll invole huge monetary and infrastructural resources, will require us to educate people how to use the new voting system. Taking into account the vast electorate and that many of the people in rural areas, simply don't have network connectivity and we then would have to make a simple enough hardware(yet secure enough) frontend so the general populace can easily vote on the system.
And by having network in the mix, we are introducing the model to a whole new plethora of problems.

6.1 Software Aspect

6.2 Hardware Aspect

6.3 Correctness

6.4 Scalability

6.5 Implementational feasibility

Chapter 7

Conclusion

By researching on this topic extensively, I can conclusively say :-
There is a diffence between coming up with an extremely good design with theoritically satisfies all the constraints but, it still may not be implementable in a country with as many challanges and barriers as India.

Bibliography

[1] Security Analysis of Indias Electronic Voting Machines - Hari K. Prasad, J. Alex Halderman, Rop Gonggrijp

[2] Election Commision Website

[3] Bitcoin paper - Satoshi Nakamoto

[4] CIVITAS Paper and Proofs - Michael R. Clarkson, Stephen Chong, Andrew C. Myers

[5] Wikipedia articles on Indian Elections, RSA and Blockchain