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.

The following objectives are aimed to be discussed in this paper:

- Defining the problem.
- Desirable properties
- Technical and Political Aspects
- Helpful Systems/Algorithms .
- Model
- Correctness , scaling , feasibility and Implementation
- Epilogue

Chapter 2

Defining the problem

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.

Before 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 very little details on technical build of EVM (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 were 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. Effctive against preplanning of increasing count.
- Mock Poll
- Poll Day Checks
- Poll Closure Transportation
- Storage Security
- Counting Day Protocol

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 engineereed (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 $I_2Cinterfaceisusedin IC'sanditisnotstoredcyrptographicallyinmemory(EEPRO$

- 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 key-presses 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.

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. What should be some properties of an EVM ? And how should we decide them ? Certifiablity of hardware , software and firmware checks. Verifiability

4.2 Properties

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

1. Coersion - Freedom : What is it ? More of a Social vs Comp sc problem, will be the first to go when we go for feasible systems .
2. Secrecy : My vote shouldn't be visible to the public. Just who I voted to, but it should be counted (verifiably). ? As anonymouty is already a point, this point might be refering to design of the EVM itself, it should be open source and could be easily checked by anyone.
3. Non-Repudiation :
4. Veriafiable :

5. Cryptographic : (No one central authority should have access to the data?) (Blockchain kind of?)

6. Audit :

    - Proving there is no bias/unfairness . [Weightage of votes?] [1 person 1 vote]
    - Proof of Correctness of entire voting process .

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 prof of being tamper free and being correct]

9. Infomation Leakage : The model should have no sensitive information leakage . But at the same time, 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.

Chapter 5

Technical and Political Aspects

Can a model like this really be implemented ? Who has the power to do this ? Who will conduct this ? Social aspects ? Proof at every step ?

5.1 Key Aspects

Chapter 6

Useful Systems

6.1 RSA Cryptosystem

What is it ? Why is it secure ? Proof of it's security ? Why breaking it is infeasible ? Why does it work ? Basic level ? What are the current use cases ? Ex Wifi : Key is already in the air, but you can't reach it :) . WPA2 security

6.2 Blockchain

What is it ? Why is it secure ? Proof of it's security ? Why breaking it is infeasible ? Why does it work ? Basic level ? What are the current use cases ? Ex : Bitcoin : How will it change the conventinal currency system, no central governing body and other advantages.

Chapter 7

Model

7.1 Software Aspect

7.2 Hardware Aspect

7.3 Correctness

How many desirable properties does it satisfy ? How is it feasible for Implementation in the whole country ?

7.4 Scalability

7.5 Implementational feasibility

Chapter 8

Epilogue

8.1 What does it accomplish ?

What changes does it bring in the Elections that weren't there previously ?

8.2 Applications

Where else can this system be applied ?

8.3 Future Scope

Chapter 9

Conclusion

What are some key learnings throught this excercize ? That even thought algorithm is fully open source, no one can break it .