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

2.1.1 Why do we need a Voting system ?

2.2 How do we Currently Vote ?

Chapter 3

Desirable Properties

3.1 Introduction

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

3.2 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 4

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 ?

4.1 Key Aspects

Chapter 5

Useful Systems

5.1 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

5.2 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 6

Model

6.1 Software Part

6.2 Hardware Part

6.3 Correctness

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

6.4 Scalability

6.5 Implementational feasibility

Chapter 7

Epilogue

7.1 What does it accomplish ?

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

7.2 Applications

Where else can this system be applied ?

7.3 Future Scope

Chapter 8

Conclusion

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