Joakim Gustavsson
900209-3830
CDATE3
joagusta@kth.se

Project specification:
Net voting

Introduction

Technology has come a long way in our modern society. We trade stocks online, order food and groceries online and use the internet for sharing our social experiences. Yet in one particular area the reality is far behind what it could have been, and this area is our elections. Every election the process of getting people to go to election places, the counting of the votes and the final anouncement involves a staggering amount of work.

A way to get rid of this whole process would be to use modern technology to allow the voters to vote from home, using the internet. So far no one has been able to realize such a system in practice as there have been significant security and integrity flaws with previously proposed solutions. This essay will attempt to identify the main issues of previously suggested schemes, as well as suggest possible solutions and propose an ultimate voting system solution for the internet.

Problem statement

Two main aspects of net voting security will be addressed in the essay, namely that of prevention of ballot rigging, and that of voter anonymity. The problem statements accompanying the concerns are formulated below:

1. How would one design a net-voting system in a way where it is impossible, or at least highly unfeasible, for the election officials to in any way compromise the integrity of the election through means such as fake votes or removal of votes?
2. How should the net-voting backend be designed so that submitted votes can not be associated with the voter that submitted them, thus guaranteeing voter anonymity in the system?

Approach

To get a general overview of the subject I will first attempt to find previous research on the subject and investigate what has been proposed in the past. Since no actual solution for the problem posed has been put in effect (we still vote using pieces of paper and an urn), it is evident that these suggested solutions have contained flaws in one form or another. I will thus attempt to identify the flaws of these solutions, and see what benefits each one has, and what the flaws are, and see if it is possible to combine ideas from these solutions in order to create a solution where the flaws do not exist.

In order to address the problem of officials interfering with the voting system in order to fulfill their own agendas I will attempt to identify a suitable scheme for vote signing, i.e a means for the system to verify that the vote originated from a particular voter, while still trying to limit the visibility of this signature to election officials. The method of public-key cryptography and message signing seems like a good angle to approach the subject from, where a voter would have a key-pair signed and verified by a number of election officials to guranatee that no identity spoofing is taking place. This signature would then need to be stripped somewhere in order to preserve voter anonymity.

I will attempt to outline a procedure for what needs to be done before the voting can take place, and how the digital vote will pass through the election system in order for the system to finally be able to determine a winner, and also guarantee that no cheating has taken place. Security holes in this procedure will also need to be identified and addressed.

References

There is a project called Verificatum.org that attempts to solve the second problem of my essay, and contains links to a few research papers published in the area, making this seem like a good place to start for the background research:

http://www.verificatum.org/verificatum/prot.html

It is important to note that the verificatum project aims to create what is known as a mix-net, which is one anonymity aspect of net-based voting, while my focus in this essay will be more of a general system and voting procedure, covering anonymity, security against tampering and also convenience for the user. The essay will as such go into less detail than the verificatum project, but instead provide a better overview of how all components fit into the grand election system.

Time plan

- Feb 12 - 19: Reviewing reference material and identifying the pros and cons of previously suggested solutions.
- Feb 20 - Mar 4: Construction of scheme for signing of votes in order to guarantee tamper proof system, and authenticity (Problem 1)
- Mar 5 - Mar 18: Preserving anonymity in the system, stripping of signature from step 1, possible uses of Mixnet-like schemes and evaluation of such schemes (Problem 2)
- Mar 19 - Apr 2: Implementation and design of prototype of full system.
- Apr 3 - Apr 12: Merging written content into final essay, formatting and tuning.
- Apr 13 - Apr 23: Review of other essay and preparation of opposition
- Apr 24 - Start of May: Final tweaks of essay based on opposition.