Thesis compiled by:

Joakim Gustavsson

Title of thesis:

Net Voting

Opponent:

Karl Johan Andreasson

Was it easy to understand the underlying purpose of the project? Comments.

The purpose of the project was very well defined and easy to understand, mainly because of the section 1.2. The writer return to the problem statement in the text and discuss how the current part helps to solve the problem at hand. This helps making the purpose, of not only the whole report but also purpose of the sections etc., crystal clear.

Do you consider that the report title justly reflects the contents of the report?

The title Net Voting is a accurate description of what the report is about. With the sub-title "A proposal for an internet-based election scheme resistant to identity theft while preserving voter anonymity" the reader is given a very good picture of the content of the report.

How did the author describe the project background? Was there an introduction and general survey of this area?

The introduction was quite brief. It was used to give an introduction to the common use of Internet (such as stock trading and groceries shopping) and compare it to using the Internet to vote in elections. Then the three main sources (forth source is a bit strange: "Ibid. pp. 21-22") are described and in doing so covering the different known algorithms, approaches as well as an election using net voting. No background to as why no other than Estonia has used the Internet for voting in elections are covered. No clear transitions in the introduction are present which makes the chapter seem scrambled together.

To what degree did the author justify his/her choice of method of tackling the problem?

There was no explicit method described in the report. Guessing from reading the report the approach was to analyse old algorithms and past elections using the net voting system and then figuring out somehow (no alternative are presented) the optimal solution. There are brief introductions to the different sub-parts of the project in the beginning of chapter which gives an idea of how the conclusions are conceived. This approach to the method of the project is quite lacking in a scientific report.

Did the author discuss the extent to which the prerequisites for the application of such a method are fulfilled?

As there was no explicit method described there was no discussion of the method used in the project. There are sections discussing the drawbacks of the voting system and sub-systems but these does not discuss the method used for establishing the voting system.

Is the method adequately described?

A summary of how the voting system was conceived would be a good idea to include. This would enable a discussion part of why the different choices was made while designing the voting method. In the project specification the approach is described well, to include this section would have helped the understanding of the approach by a great deal.

Has the author set out his/her results clearly and concisely?

The results in this report is a net voting system which is described in great detail, as well as in a summary in the end. This gives the reader a good (final) conclusion. The author might want to rename the other sections named conclusion to discussion or something along those lines, as that would be more in line of the content of the sections.

Do you consider the author's conclusions to be credible?

The conclusions are motivated and discussed throughout the text and I consider the net voting system suggested to be sufficient to fulfil the requirements in the problem statement. The example usage where the reader gets to follow Alice through her first net voting experience provide the reader with a good summary of the system proposed. A more thoroughly revision of the possible drawbacks and sources of errors in the voting system would been preferred.

What is your opinion of the bibliography? What types of literature are included? Do you feel they are relevant?

The first three sources used has great relevance to the subject and are motivated in the chapter Introduction. The forth source however seems to be the same as the third, and in my opinion should be better referenced.

Which sections of the report were difficult to understand?

The only chapter that was difficult to understand was the chapter Introduction. The first section in chapter 3 could have been moved to the introduction to make it easier to understand. In general the report was well written. The more complicated parts of the report were well explained. Perhaps both figure 4.1 and figure 4.2 could be introduced earlier in the report and not in the chapter Putting it all together.

Other comments on the report and its structure.

Having three different sections called conclusions was a bit misleading at first. The sections do provide useful information and contribute to the purpose of the project, the name discussion might be more appropriate.

What are the stronger features of the work/report?

The stronger features of the report are how well described the net voting system are in the report. Overall this project was easy to read and interesting, the subject seems to be relatively unexplored and this project provide a good first step to implementing net voting in a secure manner.

What are the weaker features of the work/report?

The lack of method and approach used in the report is weakest part of the project. The author should not have to find out how the conclusions was determined by finding the project specification.

The formality of the language used in the report could have been better. Frequent usage of the word 'we' and 'our' as well as referring to the report as "this essay" makes the report not seem as professional as desired. There are some really obvious spelling errors such as "whicg" in the section 1.3 Mägi. When referring to the Internet, the 'i' should be capitalized in my opinion.

What is your estimation of the news value of the work?

If the security aspects are as solid as stated and the system is secure from any sort of DDoS (Distributed Denial of Service) attack the system presented has great news value. This is because of the thoroughly review of the complete system and it does not rely on an already existent infrastructure. I could see myself voting using this system and would appreciate if the option was presented to me.

Summarize the work in a few lines.

The core of this project is to enable voting in elections online without enabling tampering with the results. The system to provide this voting has to be tamper-proof from the inside (election workers) and from the outside. To create such a method the author has explored an election using net voting in

Estonia and combining this with known research in the subject to create the optimal net voting system. The different hardships of enabling a voting systems are identified. First the proof of identity are discussed and a solution to the problem is presented. Then the issue with anonymity of the voters are discussed and a solution using an already known approach is chosen. Lastly these two parts are put together to form the final solution to the net voting problem. Some drawbacks are discussed, such as physical identification is needed.

Questions to author:

1. Has there been any work done to as why there is no more widespread usage of net voting systems? And why are governments reluctant to introduce these kind of systems?

2. What happens if a server crashes? Would this lead to a re-election? Does this lead to a possible DDoS attack (the IP of the server you are talking to would be known from the activeX och Java program), where every attempt at conducting the election is ruined by server crashes and such?

3. Would you say that your system is safer than the classical urn model?

4. If the system detects a number of false login attempts similar to a brute force attack, how does the system handle this? Would this lead to a re-election? Would not this provide a very easy way to prevent the election from happening?

5. Could a person sniffing the Internet traffic disclose what the voters are voting for?