Information Security Assignment: Securing web-based electronic elections

Bert Vankeirsbilck (Bert.Vankeirsbilck@UGent.be)

March 6, 2019

Introduction

One might have noticed that Belgian politicians are currently in "election mode". End of May 2019, the masses will set direction towards an Electoral Office to cast their vote. People need to volunteer to supervise the correct voting procedures, and all votes are manually counted. All of these procedures currently deployed might seem like a task screaming for automation and benefiting from a web-based approach.

However, it is key to thoroughly analyze the viability of such a system first. Your task is to investigate what it would take, if at all possible, to implement a web-based electronic voting system in a secure, fair and democratic manner. The goal of this assignment is to focus on the security aspects of online elections, and the arguments against or in favour of such an approach in comparison to the traditional voting process.

Objectives

Report

The main objective of this assignment is that you consider the correct security choices you have to make for such a system:

- Which security services are required (confidentiality, authentication, data-integrity, non-repudiation, etc.)?
- Against which attacks should these security services protect the system?
- Which countermeasures have been taken against these attacks?
- What are possible limitations and remaining vulnerabilities of your system?
- Which concrete security mechanisms (encryption algorithms, key lengths, etc.) do you use to implement these security services? Be sufficiently specific in the description of your choice.

You are expected to justify these choices in the report you write about this. The report need not be lengthy (I do not expect a novel, 8 to 12 pages using normal font size and line spacing is typically sufficient), but it shall be sufficiently complete: someone reading the report should be able to understand how your Web-based election system works and how it can be implemented. A couple of additional tips to aid the draw-up of this report:

- Do not forget to mention the sources of your inspiration in the references.
- Do not forget to write a conclusion to the assignment report.
- "a picture is worth a thousand words". Adding a schematic explaining how messages are exchanged in a protocol is usually very useful.

Demonstration software

Besides the report you will write about the project, I also expect some proof-of-concept demonstration software.

- The main purpose of the software is to demonstrate the operation of the security mechanisms and the operation of the election system.
- Show how the required security services can be verified.
- It may be useful to illustrate a few possible attacks and how the security of your systems prevents them from being successful.
- Do not implement the cryptographic algorithms yourself. Rather use existing implementations.
- Your proof-of-concept demonstration may slightly differ from the system you've worked out in the report if this simplifies the implementation (e.g. using RSA instead of ECC), but dont forget to mention and explain the differences.
- You need not set up any server or develop a specific app for smartphones.
- A proof-of-concept demonstration on a PC is sufficient. The purpose is that at the end of the assignment you can give me a demonstration of how your system works (e.g. on a laptop).
- You will be able to demonstrate how the software works during the presentation (see next section).

Presentation

You will also show your results in a presentation, where you explain how the security works and show the demonstration of the proof-of-concept software. The presentations will be done in one of the meeting rooms at iGent. A 30 minutes time slot will be scheduled for each group in the second half of May or in June. Well try to find a time slot which is sufficiently

convenient for most group members and the supervisors. Not all group member need to be present during the presentation (although that would be better of course), but at least a majority of the group.

Practically

Deadlines

Groups

This project is to be performed in groups of 6 (if needed 5) students. The first task is to agree upon the composition of these groups. A single report and a single demonstration is expected per group. Forming groups is left to the responsibility of the students. We expect the groups to be formed by **Thursday, March 14, 2019 (22h00)**. The composition of the different groups should be materialized through Minerva's "Groups" functionality.

Intermediate Reports

From each group, a *concise* intermediate report is expected by e-mail on the following dates:

- Friday, March 22, 2019 (22h00)
- Friday, April 5, 2019 (22h00)
- Friday, April 26, 2019 (22h00)
- Friday, May 10, 2019 (22h00) (coinciding with the final report)

Please, insert [InformationSecurity] in the subject of your email to allow for easy filtering on my behalf. In the intermediate reports you are expected to briefly mention the contributions of each group member in the previous period (task + estimate of time spent) and the planning for the next period.

Be honest in your reporting. There may be periods where some of you havent been able to do much because of other obligations, or you may not have achieved the goals of your previous planning. Your score wont depend on these intermediate reports. The goal of these intermediate reports is for me to keep an overview of the assignment progress in all groups and to identify possible free-rider problems in time.

Final Report

The final deadline for the report of this project is **Friday, May 10, 2019 (22h00)**. For this report, the preferred submission channel is Minerva's "Dropbox". I intend to provide feedback on the assignments before the exam period starts, i.e. May 24.

Questions

Questions regarding this assignment can be directed to Bert.Vankeirsbilck@UGent.be