Internship Report: Protocol verification

Romain Soumard

12 mai 2020

1 Introduction

Coming...

2 Organisation presentation

Coming...

3 The study case of Belenios

3.1 Description of Belenios

Part of my intership consisted in studying the case of the Belenios system. Belenios is both the name of the electronic voting system and the name of the protocol used by it. It is mainly developed by Stéphane Glondu since 2012, and was proven to respect several security protocols properties.
Before we dig deeper into the functionning of the system, we'll first have to define several notions related to the study of security protocols, such as privacy and verifiability. We'll then study a use case of Belenios and try to determine whether or not this system would be suited to administer an election at university level.

3.2 Brief introduction to security protocol glossary

Before we can analyse the properties of Belenios, we need to define a few terms.
By looking at the website and the related research and specifications papers, the security protocol used by Belenios is said to respect several properties :

- **Privacy :** In the context of voting systems, privacy refers to the inability of someone to know how you voted.
- **Strong verifiability :** The notion of verifiability is still debated, however, in the context of Belenios, a voting system is said strongly verifiable is the result of the election reflects :
  - All the votes of the honest voters who checked their votes
  - Some of the votes of the honest voters who did not checked their votes
  - If k additionnal voters were involved in the election, then at most k additionnal votes
- **Authentification :** Intuitively, authentification is the act of proving an assertion. For example, providing your credential and your password can be a way to prove your identity.
- **Cryptographic primitves :** Intuitively, cryptographic primitives are basic functions that are used as the base brick to build several security protocols. They allow us, for example, to encrypt or decrypt data, using asymetric or symectric encryption.

- **Pi-Calculus :** Pi calculus is a process algebra used to modelize concurrent systems and their interactions. It is especially useful in the case of security protocol study, since, with cryptographic primitives, it allows us to modelize protocols efficiently with an abstract tool.

3.3 Organization of an election

Now that we defined a few terms, we are first going to study the way an election works, then we'll dive at a deeper level and study the protocol used in Belenios itself.
An election organized with Belenios consists in up to three entities :

- The voters, who are provided with a credential and password, allowing them to authentificate to the election server so they can vote.
- The election server, which is responsible with administering the election.
- Optionnaly, a registrar authority which can generate and send the credentials to the voters instead of the election server.

A lot of the proofs on Belenios are based on the presence of a registrar authority, which we'll analyze later.

4 Conclusion

Coming...

5 bibliography

Coming...