

Internship Report: Protocol verification

Romain Soumard

5 mai 2020

1 Introduction

Coming...

2 Organisation presentation

Coming...

3 Study of the properties of protocols

3.1 Preparations

In computer science, verification refers to a discipline that uses formal methods to study the properties of systems and check whether they fulfill certain specifications.

During the course of this semester, I was assigned with the study of the protocols used in the belenios system. Belenios is an electronic vote sytem which was developed by the researchers from INRIA (**préciser l'acronyme**). Before being able to take care of the task at hand, I had to learn the tools used in this field of research.

Throughout my studies and researches, I have learnt the existence of several mathematical and logical abstract tools, techniques and properties :

- The use of cryptographic primitives, modeled by an equational theory
- Process algebras (or process calculi), use to model concurrent systems. Especially important since it allows us to study certain properties of protocols, notably **authentication**.
- The use of proofrees to prove deducibility, which, intuitively, refers to the ability to deduce of message from a set of terms (in the logical meaning of the way.).

4 Conclusion

Coming...

5 bibliography

Coming...