Formal Verification of Secrecy, Coercion Resistance and Verifiability Properties for a Remote Electronic Voting Protocol

Khaoula Marzouki, LIP2-LR99ES18, Faculty of Science of Tunis, Tunis-El Manar University, Tunis, Tunisia

Amira Radhouani, LIP2-LR99ES18, Faculty of Science of Tunis, Tunis-El Manar University, Tunis, Tunisia

Narjes Ben Rajeb, INSAT, LIP2-LR99ES18, Carthage University, Tunis, Tunisia

ABSTRACT

Electronic voting protocols have many advantages over traditional voting but they are complex and subject to many kinds of attacks. Therefore, the use of formal verification methods is crucial to ensure some security properties. We propose to model a recent protocol of remote electronic voting in the applied Pi-calculus. We focalized on some security properties such as fairness which expresses the impossibility of obtaining partial results, eligibility which requires that only legitimate voters can vote, coercion resistance which ensures that no voter may vote under pressure, and verifiability which supposes that anyone can verify the accuracy of the final result. We proved either manually or using the automated verification tool ProVerif that the protocol satisfies these security properties.

Keywords: Applied Pi-Calculus, Bisimulation, E-Voting Protocols, Formal Verification, ProVerif, Security Properties

INTRODUCTION

Electronic voting promises many advantages over the traditional way of voting. It aims to simplify the voting procedure, to guarantee a lower cost and to have faster tabulation. In fact, electronic voting supporters believe that these systems are more accurate and efficient than traditional paper ballots, while critics are concerned with their security. Indeed, error design and hiatus in protocols security schema have raised considerable concerns with the safety of the electronic voting systems. That’s why electronic voting protocols security should be verified.
Among the security properties which electronic voting protocols should satisfy, are the following (Delaune & Kremer, 2009):

- **Fairness**: no early results can be obtained which could influence the remaining voters.
- **Eligibility**: only legitimate voters can vote, and only once.
- **Privacy**: the system cannot reveal how a particular voter voted. In other terms, no one can do the match between a voter and her vote.
- **Receipt-freeness**: a voter does not gain any information (a receipt) which can be used to prove to a coercer that she voted in a certain way, in order to prevent against the vote-buying.
- **Coercion-resistance**: a voter cannot cooperate with a coercer to prove to him that she voted in a certain way. Thereby, a coercer cannot force any voter to vote against her intentions.
- **Individual verifiability**: a voter can verify that her vote was really counted (Chevallier-Mames, Fouque, Pointcheval, Stern, & Traore, 2006).
- **Universal verifiability**: anyone can verify that the published outcome is the sum of all the votes (Pieters, 2006).

It has been proved (Delaune, Kremer, & Ryan, 2009; Delaune & Kremer, 2009) that formal verification of electronic voting protocols gives an efficient way to check their security, so we drive here a formal verification using manual or automated tools for a newly designed electronic voting protocol of Araujo et al. (2010) which has not been yet verified in the symbolic model.

Note that, due to the complexity of electronic voting protocols, only few automated tools have been proposed for verifying such protocols. ProVerif (Blanchet, 2006) is among these tools. It was developed by B. Blanchet to analyze cryptographic protocols. It can accept as input a model in Pi-calculus which is translated to Horn clauses in classical logic, and then, it uses resolution on these clauses. ProVerif was successfully used by S. Kremer and M. Rayan (2005a) to prove fairness and eligibility properties of the FOO protocol (Fujioka, Okamoto, & Ohta, 1992). It was also used by M. Bakes et al. (2008) to prove coercion-resistance property of the JCJ protocol (Juels, Catalano, & Jakobsson, 2005) even though its limitations. Indeed, ProVerif excels at solving reachability problems, but it is unable to prove some equivalence properties and fails to model protocols which require synchronization.

So, we propose, in this paper, a modeling of the remote e-voting protocol of Araujo et al. (2010) in the applied Pi-calculus and we construct a formal proof for the properties mentioned above (Kremer & Ryan, 2005b). We use the automatic tool ProVerif (Blanchet, 2006) to verify fairness and eligibility properties, however, we drive manual proofs for the coercion-resistance (Delaune et al., 2009; Delaune, Kremer, & Ryan, 2006) using bisimulation (Delaune et al., 2009), as well as for the verifiability (Kremer, Ryan, & Smyth, 2010) using deduction proofs. Finally, we show how the protocol verifies privacy and receipt-freeness properties according to Delaune et al (2009).

This paper is organized as follows:

- First, we briefly introduce the applied Pi-calculus and equivalence properties, especially the notion of observational property or bisimulation used for modeling such security properties.
- Second, we present the remote electronic voting protocol that we aim to study and we roughly explain its steps.
- Third, we model the considered protocol in the applied Pi-calculus in order to verify later fairness, eligibility and coercion-resistance properties.
- Finally, we model each property separately and we prove that our protocol verifies each of them.
Related Content

Building an Effective Approach toward Intrusion Detection Using Ensemble Feature Selection
www.igi-global.com/article/building-an-effective-approach-toward-intrusion-detection-using-ensemble-feature-selection/232667?camid=4v1a
A Unified Use-Misuse Case Model for Capturing and Analysing Safety and Security Requirements
www.igi-global.com/article/unified-use-misuse-case-model/62313?camid=4v1a

Privacy and Security in the Age of Electronic Customer Relationship Management
www.igi-global.com/article/privacy-security-age-electronic-customer/2457?camid=4v1a

Developing Secure Business Processes: A Model Driven Approach
www.igi-global.com/chapter/developing-secure-business-processes/61499?camid=4v1a