Development of A Formal Security Model for Electronic Voting Systems

Katharina Bräunlich, Department of Information Systems Research, University of Koblenz-Landau, Koblenz, Germany

Rüdiger Grimm, Department of Information Systems Research, University of Koblenz-Landau, Koblenz, Germany

ABSTRACT

Trust that an electronic voting system realizes the security requirements in an adequate manner is an essential premise for electronic elections. Trust in a system can be achieved by controlling the system security. There are two ways to assure system security. One way is the evaluation and certification of the implementation’s security by neutral experts. Another way is the verification of the outcome by the users. Both approaches, verification and certification, should be combined to reasonably justify the voter’s trust in the electronic voting system. In this paper a formal security model with respect to the requirements of Fairness, Eligibility, Secrecy and Receipt-Freeness, Verifiability and Protection against Precipitation is given. This formal model helps to clarify and truly understand these requirements. Furthermore, it can be used for the evaluation and certification of online voting products according to the Common Criteria.

Keywords: Common Criteria, Development of a Formal Security Model, Electronic Voting, System Evaluation and Certification, Fairness, Eligibility, Receipt-Freeness, Secrecy

INTRODUCTION

Security is an elementary property of electronic voting systems. Security objectives for electronic voting were first collected in an informal way, for example by a European-wide accepted recommendation adopted by the Council of Europe (Council of Europe, 2004). Later the semi-formal method of the Common Criteria (CC) (Common Criteria, 2006) was used to specify a basic set of security requirements for online voting products (Volkamer & Vogt, 2008). Furthermore, the method KORA (Konkretisierung rechtlicher Anforderungen/Concretisation of Legal Requirements) (Hammer, Pordesch, & Roßnagel, 1993) was used to derive security objectives for electronic voting from legal specifications (Bräunlich, Grimm, Richter, & Roßnagel, 2013).

DOI: 10.4018/jisp.2013040101
Besides their differences, there is common agreement that the following security objectives have to be granted by an electronic voting system:

- **Fairness**: Each voter can cast exactly one vote and no voter loses his voting right without having cast a vote.
- **Eligibility**: Only eligible voters who are unmistakeably identified and authenticated are allowed to cast a vote that is stored in the ballot box.
- **Protection Against Precipitation**: The voter can abort his voting process at any time prior to the final casting of the vote without losing his right to vote and there is no limit on the number of corrections a voter can make to his vote until the final casting of the vote.
- **Secrecy and Receipt-Freeness**: The voter’s voting decision must be kept secret (ballot secrecy) and must be enforced even against the voter himself (receipt-freeness). I.e. the voter does not gain any information that enables him to prove his voting decision to others. By hiding a voter’s voting decision, the voter is protected against unlawful influence.

In the context of electronic voting, it is necessary that the voters have trust in the system security of the electronic voting system. One way to strengthen the trust of the voters in the electronic voting system is the assurance of system security by means of verifiability.

- **Verifiability**: To grant traceability of the whole voting procedure, so called end-to-end-verifiability (Adida & Neff, 2006), the essential steps of an election must be open for examination by the voter. The essential steps are the marking and encryption of the vote (=ballot) and the counting of the ballots from the ballot box, or more precisely:
  - **Cast-As-Intended**: The voter can ascertain himself that the ballot is correctly encrypted and represents his voting decision correctly. In order to protect ballot secrecy, cast-as-intended can only be verified by the voter himself. It can be verified by the voter only before the ballot has been cast into the ballot box. Because otherwise, this verification functionality could be used by an attacker to reveal the voter’s voting decision.
  - **Recorded-as-Cast**: The voter can retrace that his ballot is correctly transmitted and stored in the ballot box. In order to protect receipt-freeness, recorded-as-cast has to be implemented such that the voter cannot prove his voting decision (to others). The verification of recorded-as-cast can take place directly after the ballot casting or after the voting phase.
  - **Counted-as-Recorded**: The voter as well as the broad public can verify the election result. I.e. it has to be verifiable that all ballots from the ballot box are counted-as-recorded.

Verifiability as described above is one way to assure system security and thus, to strengthen the trust of the voters in the electronic voting system. Another way is the certification of the electronic voting system. As discussed in Volkmer, Schryen, Langer, Schmidt, and Buchmann (2009), these approaches are not exclusive but should be combined in order to obtain the best possible result. Note that verifiability is a specific security function, which is subject to certification itself.

The **Common Criteria for Information Technology Security Evaluation** (CC) (Common Criteria, 2006) are a common standard for the evaluation and certification of IT-systems while the **Common Evaluation Methodology (CEM)** (Common Criteria, 2006) specifies the framework for the evaluation of such systems. An advantage of the CC is the structured and systematic specification of security requirements for an IT system in terms of Protection Profiles or Security Targets.
Exploring a Risk Adjusted Return on Capital Model for the Performance and Persistence of the Indian Equity Mutual Funds

Secure and Optimized Mobile Based Merchant Payment Protocol using Signcryption
www.igi-global.com/article/secure-optimized-mobile-based-merchant/68822?camid=4v1a