Election verifiability in electronic voting protocols

Ben Smyth, Mark Ryan and Steve Kremer School of Computer Science, University of Birmingham

1. Introduction

Electronic voting systems are being introduced, or trialled, in several countries to provide more efficient voting procedures with an increased level of security. However, current deployment has resulted in catastrophic failure due to unrealistic trust assumptions. In particular, the trustworthiness of hardware/software and election officials has been assumed. In practice, it is very difficult to establish this level of trust and thus systems are vulnerable. This research paves the way for dependable electronic voting systems.

2. Problem statement

A difference between electronic and traditional paper-based elections is *lack of transparency*. The current election process can be observed, and we rely upon physical characteristics of the world, e.g., the impossibility of altering ballots inside a locked ballot box. By comparison, it is not possible to observe electronic operations.

3. Solution

***Election verifiability* ensures votes have been recorded, tallied and declared correctly.**

- ***Individual verifiability (IV).* A voter can check that her ballot is included in the outcome.**
- ***Universal verifiability (UV).* Anyone can check the outcome corresponds to the ballots cast.**

These definitions are captured by boolean tests Φ^{IV} and Φ^{UV} which satisfy several conditions. The test Φ^{IV} is used by the voter in conjunction with private data, whereas the test Φ^{UV} can be checked by an observer using only public data.

4. Formal definition

The tests Φ^{IV}, Φ^{UV} are built from conjunctions and disjunctions of *atomic tests* of the form $M = N$. A protocol satisfies election verifiability if there exists tests

$$\Phi^{IV}(\mathit{my\_vote}, \mathit{my\_secrets}, \mathit{public\_data}, \mathit{ballot})$$

$$\Phi^{UV}(\mathit{election\_outcome}, \mathit{public\_data}, \mathit{ballots})$$

where *my_secrets*, *public_data* and *ballots* are defined by the electronic voting protocol, such that the following conditions are satisfied

- **Φ^{IV} holds for at most one ballot:**

$$\Phi^{IV}(v, s, d, b) \wedge \Phi^{IV}(v', s', d, b) \rightarrow v = v' \wedge s = s'$$

- **Φ^{UV} holds for at most one outcome:**

$$\Phi^{UV}(o, d, b) \wedge \Phi^{UV}(o', d, b) \rightarrow o = o'$$

- **Φ^{IV} and Φ^{UV} agree upon the outcome:**

$$\bigwedge_{1 \le i \le n} \Phi^{IV}(v_i, s_i, d, b_i) \wedge \Phi^{UV}(o, d, (b_1, \ldots, b_n)) \rightarrow (v_1, \ldots, v_n) = o$$

- **For all votes $v_1,\ldots,v_n$, there exists a protocol execution producing secrets $s_1,\ldots,s_n$, data d and ballots $b_1,\ldots,b_n$ such that tests Φ^{IV}, Φ^{UV} hold:**

$$\bigwedge_{1 \le i \le n} \Phi^{IV}(v_i, s_i, d, b_i) \wedge \Phi^{UV}((v_1, \ldots, v_n), d, (b_1, \ldots, b_n))$$

Intuitively these conditions ensure that: if the tests succeed, then the election is indeed valid (*soundness*); and there is a behaviour of the election system which produces data to satisfy the tests (*effectiveness*).

5. Results, further work & conclusion

A symbolic definition of election verifiability has been presented. This permits evaluation of electronic voting protocols and facilitates comparison on the basis of trust assumptions. The work has been successfully trialled with respect to two electronic voting protocols which have been implemented and deployed. In particular, the Helios 2.0 protocol was evaluated. This protocol was used in March 2009 to elect the president of the Catholic University of Louvain, Belgium, in an election that had 25,000 eligible voters. This demonstrates the suitability of the framework for analysing real world election systems. Finally, this research forms a foundation for the development of electronic voting systems which provide an assurance of integral elections.

research@bensmyth.com www.bensmyth.com