Verifiability in Electronic Voting – Open Issues

Johannes Buchmann and Melanie Volkamer
CASED at Technical University Darmstadt
{johannes.buchmann, Melanie.volkame}@cased.de

1. Introduction

In the past, evaluation and certification were the only precondition to use electronic voting computers in governmental contexts while it was accepted that these computers are black box systems and, thus, do not provide verifiability. This situation is currently changing in many countries - like the US. As more and more people are aware of arising problems during elections and know the results of system analyses from security researchers, they raise their voice against these black box approaches and make demands on verifiable systems. In Germany, since March, there is no debate on black box systems anymore because the Federal Constitutional Court judged in their decision that black box voting systems are unconstitutional as they do not "meet the constitutional requirements of the principle of the public nature of elections" [FCC09]. This principle of the public nature of elections "prescribes that all essential steps of an election are subject to the possibility of public scrutiny" [FCC09].

With this decision, there is a clear prohibition of black box voting systems (without paper audit trails) while the decision leaves open a lot of research questions for implementing verifiable electronic voting systems. These open issues are addressed in this position paper.

2. Addressed Principles

The court's decision focuses on the principle of the public nature of elections which is very often linked to correctness (eg, "votes cast are recorded in an unadulterated manner" [FCC09]) and thus indirectly attached to the principles of universal and equal elections. The main message is that the voter should not need to trust the integrity of the (evaluated) system but he has to be able to check whether his vote is recorded correctly and whether all votes are tallied correctly.

The court's decision does not take other election principle into account and in particular not the election secrecy principle. Therefore, it is an open research question whether the voter should also be able to verify that the electronic voting system ensures this principle, ie., the voter can check that the system does not store any information leaking the order of the cast votes and does not emit any information on the currently cast vote. Probably, for this election principle holds the same as for the integrity of the election result: the voter should not need to trust the integrity of the system. Otherwise, you have to explain why the voter should trust the evaluated system regarding the election secrecy while additional mechanisms are implemented for the integrity of the election result.

But how can this type of verifiability be implemented? One obvious possibility is that the voting systems in the polling station does not know the plaintext vote but only the encrypted one (like with Prêt à Voté [PR06]). This would strongly limit possible electronic voting systems. Another solution might be the possibility of vote-updating. Are there others?

3. Required Verifiability Class

There exist two classes of voting systems implementing verifiability:

- Either with a plaintext receipt (on paper) which the voter can check but which has to be put into the traditional ballot box in the polling station.
- Or with an encrypted receipt (probably also on paper) which the voter takes with him and which he uses to later check on the bulletin board whether his vote was not altered and counted.

While the second one provides stronger verifiability the first one is easier to explain to voters. Therefore, one further open question is which class complies with the election laws and the court's decision. The decision demands eg. that "the result can be examined reliably and without any specialist knowledge of the subject” [FCC09]. Here, the question is whether the voter can be supported with verifiability tools which he can use without any specialist knowledge or whether he needs to understand the techniques behind this verifiability tool.

The following issues focus on encrypted receipts. However, for the plaintext receipts, there exist also a couple of open issues like: how many polling stations count the paper votes? Which one is the legal vote – paper or electronic one? How to handle differences between electronic and manual counting?

4. Required Strength of Verifiability

[LSSVB09] presents different strength of individual and universal verifiability (while both together define different strength of E2E verifiability). E.g. regarding individual verification it is distinguished whether – in case the voter wants to file a complaint - the voter is able to do an open objection with or without scarifying election secrecy. Regarding universal verifiability it is e.g. distinguished whether eligibility requirements are included or not (meaning it can be verified that no ineligible votes have been added). The court’s decision does not provide such a definition. Thus, it is an open research question to deduce from legal requirements a corresponding definition for E2E verifiability.

In addition, implementing individual verifiability causes two further open issues: First of all, denial of service attacks in terms of voters wrongly stating that their vote has been modified. Secondly, the possible strength of election secrecy might be restricted, eg. in terms of receipt-freeness, coercion resistance or long-term confidentiality.

5. Usability and Didactics

Implementing verifiability based on an encrypted receipt, usability and didactic research questions appear: How to communicate that the system is evaluated but additional security mechanisms in terms of verifiability are implemented? How to communicate that additional steps are required and this needs to be done later on and using the Internet/bulletin board? How to communicate that not all voters need to apply the verifiability in order to arise the security? Verifiability gets even harder to explain if individual verification is applied prior to the actual vote casting. How to explain that the voter cannot directly verify that his vote is recorded correctly but only indirectly because of the possibility to pre-verifiability?

It needs to be ensured that the verifiability process is user-friendly, ie, not too long strings are to be compared and it does not cause too much extra steps. This also holds for the complaining process.

6. Flexibility of Election Law

Existing electronic voting schemes providing verifiability are not compatible with current election laws as they propose eg to randomize the candidate order per ballot or to allow vote-updating. Here it needs to be checked whether corresponding modifications of the laws are possible.

In addition, it needs to discuss how to integrate verifiability mechanisms in the law and in particular how to handle the arising new types of claims.

7. Impact on the Evaluation

There are already evaluation standards for black box voting systems [VSS]. It needs to be analyzed whether some of the contained requirements can be removed because they are covered by verifiability mechanisms or whether the standard needs to be extended and thus gets more complex.

8. Conclusion

We (at least in Germany) are currently in a timeframe between the era of black box electronic voting systems and the era of more advanced electronic voting systems implementing verifiability in a way that the principle of the public nature of elections is ensured. Due to the huge amount of open research questions, it is not possible to develop and deploy new electronic voting systems for the parliamentary elections in September. Thus, all voters are going to cast their vote with pen and paper. The goal is to switch back to electronic voting for the parliamentary elections in four years and thus start to answer the above questions, soon.

9. References

[FCC09] Bundesverfassungsgericht: BVerfG, 2 BvC 3/07 vom 03.03.2009, Absatz-Nr.(1-136); English Press Release: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-019en.html (2009)

[PR06] Ryan, P.Y.A., Schneider, S.A.: Prêt á Voter with Re-encryption Mixes. In: Gollmann, D., Meier, J., Sabelfeld, A. (eds.) ESORICS 2006. LNCS, vol. 4189,pp. 313–326. Springer, Heidelberg (2006)

[LSSVB09] Langer, L., Schmidt, A., Stolfik, A., Volkamer, M., Buchmann, J.: Towards a Framework on the Security Requirements for Electronic Voting Protocols; accepted for RE-Vote09. (2009)

[VSS] Federal Election Commission: Voting System Standard. Agenda Documents 01-62 and 01-62a, http://www.fec.gov/agenda/agendas2001/mtgdoc01-62/mtgdoc01-62.html (2001)