Verifiability in Electronic Voting
An Interdisciplinary View

Sonja Weddeling / Melanie Volkamer / Christian Paulsen / Katarzyna Młyńczak / Anastasia Meletiadou / Nils Meissner / Robert Krimmer / Jörg Helbach

T-Systems Enterprise Services GmbH
Hannoversche Straße 6–8, 49084 D-Osnabrück
sonja.weddeling@t-systems.com; volkamer@uni-passau.de; paulsen@dfn-cert.de; kmlynczak@gmail.com; nancy@uni-koblenz.de; r.krimmer@e-voting.cc; joerg@helbach.info

Keywords: electronic voting, verifiability, transparency, online voting, security, usability, client security

Abstract: Verifiability as a basic component of elections is related to many different aspects including trust in the correctness of the election results, transparency of the election processes and preparation for a possible contestation of the election. In the majority of cases the problem of designing appropriate verifiability methods is approached only from one point of view (i.e. technical). Therefore, this paper describes and points out the interdisciplinarity of this topic to improve upcoming scientific and practical work.

1. Introduction

Verification or Verifiability means the proof that a stated fact is true. In conjunction with information technology, it can be specified as the act of reviewing to establish that a product, service or system conforms to the standard or specification requirements. In respect of electronic voting the definitions are more complex and heterogeneous, because verifiability is of crucial importance in legally regulated elections. In this context, verifiability means that voting systems must be designed correspondingly and must generate appropriate data during the voting process, so that after determination of the election result the correctness can be made evident.

There are already some approaches to deal with verifiability in the way described above. For example Fujioka, Okamoto and Ohta [FOO92] define a

voting scheme as having the property of verifiability if no one can falsify the result of the voting.

As described in the abstract, the goal of this paper is to show that verifiability should be seen from many different scientific viewpoints (e.g. political, social and juridical) which pose varied research questions.

2. Verifiability Forms and Requirements

From a juridical point of view it has to be declared that several documents defining requirements and in particular security requirements can be found in literature. The most popular are the Recommendations of the Council of Europe [CoE04], but they address verifiability only on the sidelines. Verifiability is addressed in few election laws, like in Germany, where the voter has the right to observe the whole voting process in the polling station.

Three different classes of verifiability can be distinguished:

- Individual Verifiability:
  a) Without open objections to the tally: Allows the voter to verify whether his vote has been counted but forces him to reveal his vote in order to file a complaint. Thus, individual verifiability guarantees that it can be detected if votes of individual voters are deleted or changed.
  b) With open objections to the tally: Allows the voter to verify whether his vote has been counted and files a sound complaint without revealing the content.
- Universal Verifiability: Anyone can verify the correctness of the tally from a set of (encrypted) votes. Thus, universal verifiability guarantees that it can be detected if votes are changed, added or removed in the counting process.
- Deniability: The voter can bring to proof that his vote was not counted or not counted correctly.

3. Verifiability and Society

3.1 Distinction of Voting Machines and Remote Voting

First of all we need to distinguish the two electronic voting forms: electronic voting machines (in polling stations) on the one hand and on the other hand remote electronic voting.

3.1.1 Electronic Voting Machines

For computer science purposes the use of verifiability with electronic voting machines can be described as follows: on the Election Day the voter goes as usual to a polling station and casts an electronic vote. In order to ensure individual verifiability, the voter needs to get some kind of receipt. Now we can distinguish at least three forms:

- The device prints the vote and the voter can verify the correctness and has to put this piece of paper in a traditional ballot box. Individual verifiability is only given under the strong assumption that this device is trustworthy and stores the vote as it was printed.
- The voter gets an electronic receipt, on e.g. a smart card or memory stick. Then he has to use this at a second device, which displays his vote. If this corresponds to the voter's decision, the vote is also stored in an electronic ballot box of this second device.
- The voter can take the receipt (not saying anything about the content of the vote) home in order to check the correctness later over public channels such as the Internet, newspapers or blackboards.

In general, none of these solutions provides satisfying trust models.

3.1.2 Remote Electronic Voting

For remote electronic voting similar statements can be made: the individual verifiability is strongly connected to the trustworthiness of the voter's device used to cast a vote, e.g. if the vote is changed before sending to a voting server, the received receipt might be correct but belongs to the "wrong" vote. Moreover, in order to check at the end of the election whether his vote is counted or not, the voter needs to store the receipt in a secure way.

3.2 Verifiability and Usability

In examining the different methods of verifiability of electronic voting systems, also the sociological view regarding usability of verifiability is of crucial importance. In order to analyze the usability properly, it is essential first to characterise the user groups, which have a very heterogeneous formation. The Electoral Board or public institutions constitute one part of the users of the verifiability programs. The other component of the user group is the voter, whose main concern is the accuracy of the voting procedure. It needs to be emphasized that the technical affinity of these two user groups may vary. Among voters a distinction needs to be made between those who are well or even very well acquainted with the technology and those who do not have extensive knowledge in this area.

Generally, verifiability methods should correspond to the following minimum ergonomic requirements:

- clear and simple usability
- fast usability
- universal availability
- simple installation
- technological knowledge should not be a pre-requisite
- comprehensible program sequence
- universal adaptability of the verification program
- accessibility for disabled persons

Scientific investigations have further proven that a simple pro forma verifiability, which gives the user on-screen proof that his vote has been accurately registered, is sufficient to instil user confidence in remote electronic voting. Apparently, voter confidence is based on personal perception rather than facts. The simpler, more efficient and faster verifiability is, the higher the trust in verifiability and in the voting system in general [OB04].

4. Verifiability and Client Security

Regarding the information technology there are several doubts about the client security and their influences on verification systems. Unlike on electronic voting machines, regarding remote online voting systems, a canvasser has no influence on the voting client. In particular, he or she cannot check if the voting client, i.e. the personal computer of the voter, is in a proper state.

According to Vinton Cerf, co-developer of TCP/IP and architect of the Internet, "of the 600 million computers currently on the Internet, between 100 and 150 million were already part of these botnets." [Web07]. In 2002 Ronald Rivest introduced the term "secure platform problem" with reference to electronic voting systems. In his article Rivest shows that "in reality, the current generation of personal computers running Windows or Unix are not sufficiently secure to act as trusted voting agents" [Riv02].

One possibility to solve this problem is to split the communication process, i.e. to transfer the vote with the different candidates on the one hand and the voter's decision on the other hand on different communication channels. One according approach is to use code voting as proposed by David Chaum in 2001 [Cha01].

In the future, election processes and voting systems could be advanced by means of trusted computing (TC). TC is an approach to improve the security of computer systems, even if nowadays this technology is not fully developed.

5. Verifiability Methods

In the literature on remote voting protocols, different tools to achieve verifiability are described.

- **Bulletin Board and Published Lists**
  A Bulletin Board (see [CGS97]) is "a public broadcast channel with memory. All communication through the bulletin board is public and can be read by any party." It is not possible to delete information and each participant writes messages only in his designated section, which is usually controlled by digital signatures. Because of its public nature, it is a very powerful tool for verification purposes.
- **Digital Signatures**
  Digital signatures are used in electronic voting, as they are in other applications, to assure the authenticity and integrity of a message. With regard to verifiability, digital signatures are attached to verification data to guarantee that they are sent by the right entity and are not changed in between transport to publication.
- **Zero-Knowledge Proofs**
  A Zero-Knowledge Proof is a cryptographic protocol executed by two mutually mistrusting parties. In electronic voting these proofs are used

to verify the correct shuffling and decryption of votes or the correct decryption of the election result.

- **Secret Sharing**
  As the name implies the idea behind secret sharing is that a secret will be distributed to a group of participants (voters). However, each of them will only receive a share of the secret. One share on its own is of no use, but the secret can be reconstructed when all shares are combined. Particularly for e-voting this means that each voter communicates his vote to all other participants (or authorities).
- **Mix method**
  The idea behind the mix method is that all votes will be posted in random order to other participants. This order is unknown to the participants, so anonymity is protected. The first proposal of a mix scheme was developed in 1981 by Chaum [Cha81], with encrypted rounds and mix-net operations.

6. Conclusions

We have seen in the analysis above that verifiability methods are not practicable in every case. Verification systems must be comprehensible for every vote. They can lead, regarding the necessary cryptography, to huge performance problems. In addition to this, they cause a loss of usability and cost-effectiveness. Even though verifiability is a highly sensible aspect concerning remote electronic voting, no viable solution has been found. Certainly, the existing verifiability possibilities for every voter, irrespectively of his or her level of computer literacy, need further improvements, but the way to verifiable e-voting is already paved.

7. Literature

[CoE04] Council of Europe (2004): Legal, operational and technical standards for e-voting. Recommendation Rec (2004)11, Strasbourg.

[CGM85] Chor, B., Goldwasser, S., Micali, S., Awerbuch, B. (1985): "Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults", FOCS85, pp. 383–395.

[CGS97] Cramer, R., Gennaro, R., Schoenmakers, B. (1997): "A Secure and Optimally Efficient Multi-Authority Election Scheme", *Advances in Cryptology – Eurocrypt'97*, LNCS 1233, pp. 103–118.

[Cha01] Chaum, D. (2001): "Sure Vote: Technical Overview", Proceedings of the workshop on trustworthy elections (WOTE 01), presentation slides.

[Cha81] Chaum, D. (1981): "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communication of the ACM, Vol. 24, No. 2.

[FOO92] Fujioka, A., Okamoto, T., Ohta, K. (1992): "A practical secret voting scheme for large scale elections", *Advances in Cryptology – Auscrypt'92*, LNCS 718, pp. 244–260.

[Krim04] Krimmer, R. (2004): Die Dimensionen der Elektronischen Demokratie, in: Schweighofer, E., Liebwald, D., Kreuzbauer, G., and Menzel, T. (eds.), Informationstechnik in der juristischen Realität, Verlag Österreich, Vienna, pp. 217–222.

[OB04] Oostveen, A.-M., Besselaar, van den, P. (2004): "Security as belief. User's perceptions on the security of electronic voting systems", Electronic Voting in Europe – Technology, Law, Politics and Society, GI LNI Series P-47.

[Opp02] Oppliger, R. (2002): "How to address the secure platform problem for remote internet voting", Proceedings of the 5th Conference on "Sicherheit in Informationssystemen" (SIS 2002), Hochschulverlag, pp. 153–173.

[Riv02] Rivest, R. L. (2002): "Electronic voting", Financial Cryptography '01, pp. 243–268. http://citeseer.ist.psu.edu/rivest02electronic.html.

[Web07] Weber, T.: "Criminals 'may overwhelm the web'". http://news.bbc.co.uk/1/hi/business/6298641.stm. Version: 2007.