OPENEVOTING: PUBLIC OBSERVATION AND QUALIFIED BALLOTS FOR MORE TRANSPARENCY IN E-VOTING[1]

Robert Kofler[2]) Christian Buchta[3])

Abstract

According to DeJong et al. [5], the perception of e-voting is a trade-off between anonymity, ease of use and correctness of process. In this paper we propose quality criteria for a completely new level of transparency for online elections to avoid such a trade-off, while presenting a detailed description of a powerful protocol which is able to fulfill all these criteria. Finally we outline a new type of digital ballot which enables everyone to become an election observer – using only the final result as primary data source. This approach can be qualified as 'open source e-voting' where the term 'open source' reflects the trust in the algorithms and data reviewed by the general public. The suggested protocol does not require trust in election authorities nor trust in a small group of election observers – instead the general public replaces such traditional election observers.

Keywords: online elections, e-voting, observer, qualified ballot, trust, e-voting 3.0, absentee ballots, public observation.

1. Introduction

1.1 Anonymity versus correctness of process?

DeJong et al. [5] compared paper ballot to voting machines. According to their findings the voter's perception of voting technology is a (mandatory) trade-off between anonymity, ease of use and correctness of process. Considering these results we assume that the perception of online-voting is even worse: there is a reduced trust in anonymity and reduced trust in correctness of process – both caused by a lack of transparency. McGaley and McCarthy [11] describe the situation as: "The Nature of computers is that their inner workings are secret" and "Once the vote is cast, the voter 'loses sight' of it."

We believe that only a system which makes the digital ballots 'tangible' can make the difference in perception. An e-voting system should be able to provide even more trust in *correct processing* and more *confidence in anonymity* and *integrity*. New criteria focusing on transparency and result checking need to be defined for e-voting. This can be easily realized with existing instruments out

[1] This work was co-funded by Openevoting.org, an initiative for fully transparent evoting systems, Vienna, Austria.

[2] Institute for Production Management / Vienna University of Econimics and Business, Augasse 2-6; A-1090 Vienna, Austria (robert.kofler@wu.ac.at | robert.kofler@openevoting.org)

[3] Institute for Tourism and Leisure Studies / Vienna University of Econimics and Business, Augasse 2-6; A-1090 Vienna, Austria. (christian.buchta@wu.ac.at)

of the cryptographic toolbox. In the following section we define some of these new criteria required by e-voting and the proof of concept.

2. Quality criteria for a public review of an election result

It is said that only what is supervised by the general public can be considered safe and trustworthy as nobody else has the manpower for sufficient code review (e.g. in [8] Karhumäki and Meskanen estimate a thorough checking of the entire code could require several man-years). We have extended this 'Linux' way of thinking from algorithms to data – in this case to election results. In addition to existing e-voting recommendations and guidelines, like [3] made by the Council of Europe, we suggest that more emphasis be placed on guaranteed anonymity and transparency. We do not expect, that the voter trusts in the authorities or in a group of voting observers[4].

The following list of criteria is not complete, e.g. items like "the secrecy of the ballot must be preserved" are missing because this is supposed to be trivial.

2.1 Voting protocol must be published

To provide full transparency and to allow everyone to observe an election, it is essential that the voting protocol is published, in order for us to be able to understand all data fields of the result set.

2.2 Encryption function of ballots must be published

To verify the quality of an e-voting system all encryption functions used must be published. In contrast to security by obscurity a public review results in more trust in an e-voting system. This can be compared to the well known SSL/TLS [6] protocol which can be considered very secure although everybody can read its underlying source code.

2.3 Votes/ballots must be anonymous

In any case it must not be possible for the authority or for any system administration to compromise voter's anonymity. This requirement addresses failures caused by malfunction of software, wrong system design or unfair election authorities.

2.4 Each vote/ballot must be verifiable

Each ballot must contain additional information which enables anyone who does not belong to the election committee to prove the following points:

- The ballot was authorized for usage.
- It was filled by an eligible voter.
- The ballot was not moved to another constituency.
- The voters' choice was not changed.
- It was not inserted by a system administrator or man in the middle.

[4] In Austria it is good practice to have election observers from each political party in each constituency. They are physically present when the ballot box is opened and also during counting of ballots.

When we talk about ballots, we mean absentee ballots. We stress that it is useless for any digital post audit process (e.g. over the internet) to review just the publication of a voting result – commonly used in paper-based but also in online elections.

2.5 Votes/ballots must be system independent

Election results are worthless without the underlying data. In this context an e-voting result must be reproducible from the ballots without having the system available which collected them – this is self-evident for paper ballots but a big obstacle for online voting results. This requirement gives us the freedom to choose a counting and verification tool in which we trust.

2.6 Filled (encrypted) ballots and their history must be provided online within suitable intervals[5]:

Even the most sophisticated security arrangement as described in the work of Cansell and Gibson[4] cannot prevent somebody from physically destroying the write-once data PROM or from just destroying the ballot box with its collected ballots. This refers to paper ballots as well as digital absentee ballots from an online election.

Here we want to stress one of the major advantages of online voting: publishing snapshots of the encrypted intermediary results guarantees that they cannot be removed or destroyed after being published. The latest published dataset covers all ballots from the previous dataset plus new ballots. The time interval or the publication threshold must be set according to the size of the constituency to prevent attacks against anonymity such as publishing only the latest inserted ballot. After election close the authority publishes its private keys[6] so that anyone who is interested can download the keys and can decrypt and count the history of (previously downloaded) snapshots of ballots. Previous snapshots must be a subset of the next snapshot so we can understand how the final result materializes.

2.7 E-voting systems must be made as simple as possible:

More complex systems are difficult to review, especially in terms of cryptography.

2.8 E-voting system and operating system must be based on open source libraries:

To be really sure what's going on and what happens to the votes between input and output a continuous public review of the functions and libraries is needed. As encryption libraries cannot work without an operating system, we propose also the underlying operating system should be open source. This enables the greatest possible review – a community review.

3. Only qualified ballots can be observed

In the following section we outline a protocol based on qualified ballots which are a precondition for public observation and audit. Then we describe our implementation of such a protocol as a web service.

---

[5] This publication interval can be a time interval e.g. every 15 minutes or after another 100 votes or we just randomly sort the ballots before publishing.

[6] We assume that ballots are encrypted with the authority's public key to keep the result secret.

3.1 Suggestions for a new protocol

We suggest the use of a two-stage protocol as presented by Kofler et al. in [9] and tested during the Austrian presidential elections 2004 [12]. The protocol is based on David Chaum's blind signature [2] and on the work of Fujioka et al. [1] and Nurmi et al. [7] with some minor modifications to increase resilience against election fraud. The usage of blind signatures offers a mathematical proof for anonymity which can be seen as unbreakable and is therefore more trustworthy than organizational guarantees as discussed in [10] or commonly used in current e-voting systems e.g. Scytl [13].

We combine the registration and voting phase into one step. When an anonymous absentee ballot is inserted it will contain the vote and the blind signature of the registration server. Both items are cryptographically joined together. We call this combination of a vote and the blind signature a *qualified ballot*.

In a post audit process these *qualified ballots* will show their functional capabilities:

- Qualified ballots can directly be published – there is no need to remove any identifying attributes like voters' signatures[7].
- We can easily check whether it comes from a valid voter or was inserted by somebody unauthorized.
- We need not care about the issue of non-empty ballot boxes before the voting phase because we will recognize illegal ballots.
- Because we can publish votes 'as-is' we do not have to rely on any authorities to keep the anonymity or to count the votes correctly.

To protect against attacks such as deletion of ballots – an issue also for paper ballots – we suggest the distribution of the filled qualified ballots directly from the voting clients. The filled ballots can be sent to national as well as international observers, e.g. servers run by trustworthy NGOs. In that case, it does not matter that the 'inner workings[8] of computers are secret'.

3.2 The Observer – A do-it-yourself audit in three steps

Observation based on usage of *qualified ballots* is easy – even during the election. All we need is a published snapshot of qualified ballots and the encryption algorithms used (note that at this stage, the result is still encrypted).

3.2.1 First Step – download a snapshot of published qualified ballots from some publishing web service:

We download a snapshot of qualified ballots from one of the distributed ballot boxes e.g. from https://www.evotingobserver.org which offers a WADL[9]-based web service. The following screenshot shows a small observer program written in Java but checking of snapshots can be done with any other tool, e.g. using the statistical software R[10].

---

7 See footnote 6: to hide the result before the end of the election qualified ballots can be encrypted with the public key of the authority.

8 Here: the 'inner workings' of the ballot box.

9 Web Application Description Language, https://wadl.dev.java.net

10 R Development Core Team (2009). R: A language and environment for statistical computing. R Foundation for Statistical Computing, Vienna, Austria. ISBN 3-900051-07-0, URL http://www.R-project.org.

The result shown in figure 1 is based on an election with two voting districts and two authorities, quite similar to the elections to the Austrian University Council in 2009.

AId Id of authority (here: 1 or 2)
BId Id of ballot (here: 1 or 2)
PId Id of the candidate (position) on the ballot; here PId is negative (-1) because the election is still ongoing and we have not yet received the private keys to open the ballot box.
Position the encrypted position chosen
VKey the verification key
ASig the signature of the authority
Psig the signature of the encrypted position

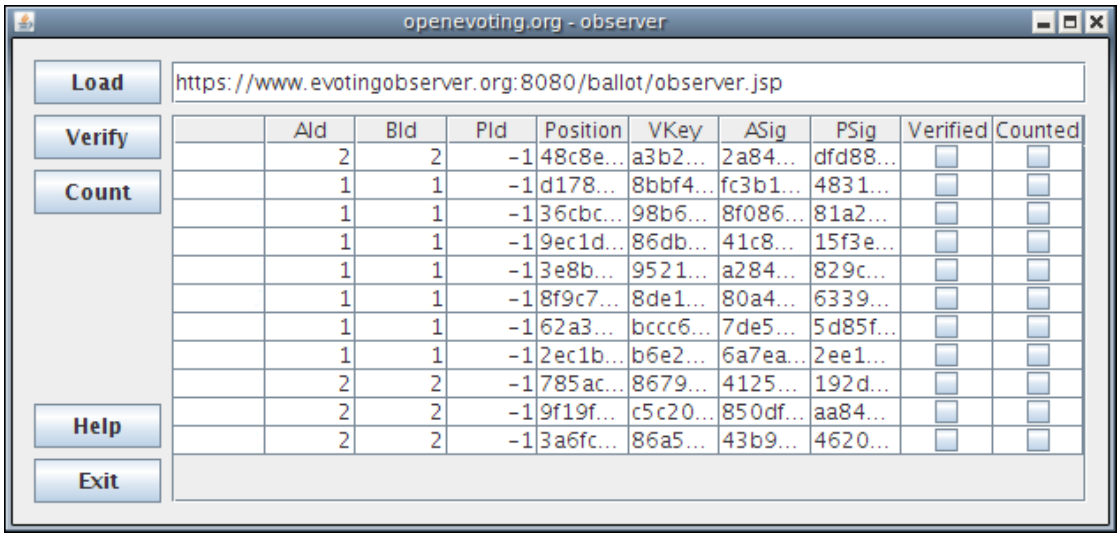

Figure 1

3.2.2 Second Step – Verification of a snapshot of published qualified ballots:

After verification we see that one ballot could not be verified due to incorrect authority signature or position signature (e.g. the vote was tampered with).

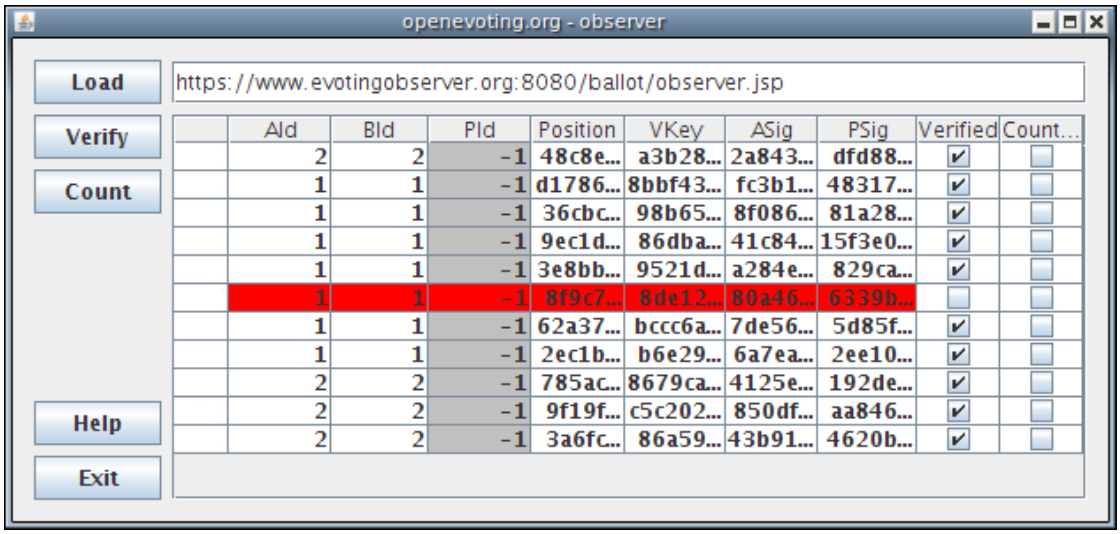

Figure 2

We can repeat this step for each snapshot which is published.

3.2.3 Third Step – Counting of choices:

After the election is closed and the authority has published their private keys we will make a final verification of the ballots, decrypt the choices (PId) and count them. Zero means intentionally invalid vote, 1/2/3/4 is the position of a valid vote on the ballot, and -1 is a vote which was tampered with.

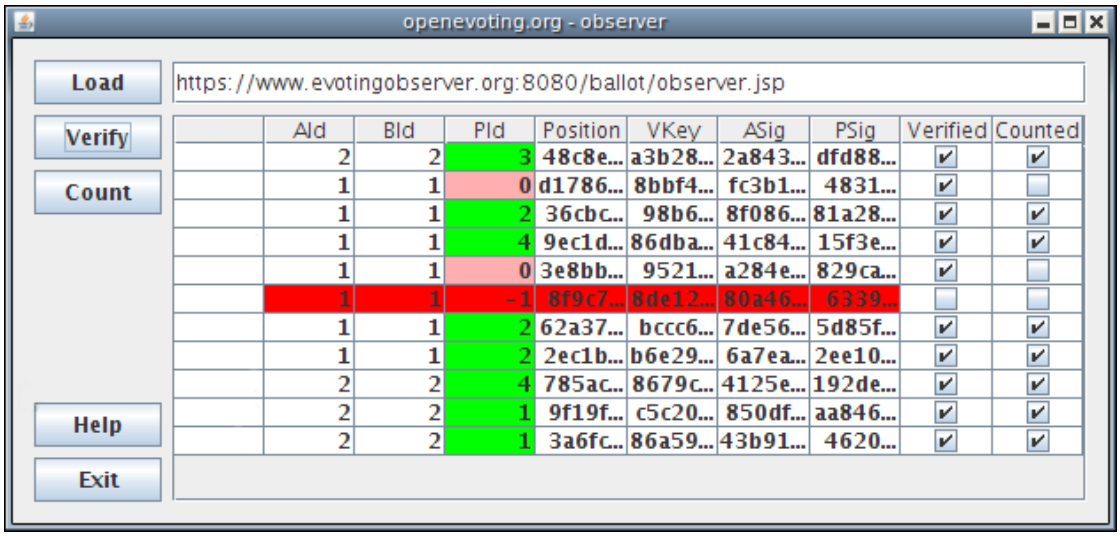

Figure 3

4. Conclusions

We have shown that more transparency will result in more confidence. We have outlined a new protocol which gives everybody the ability to become an election observer. In times of web 3.0 – also known as semantic web – we believe we should strive to improve one of the basic democratic processes, the election process. We have shown that compared with paper-based elections e-voting can outperform the traditional voting process with respect to transparency and reliability. We envisage this protocol to have a number of practical new applications to the existing voting infrastructures.

5. References

[1] A. FUJIOKA, T. OKAMOTO, AND K. OHTA. A Practical Secret Voting Scheme for Large Scale Elections, in Lecture Notes In Computer Science; Vol. 718. 1992.

[2] CHAUM. Blind signatures for untraceable payments, in: Advances in Cryptology: Proceedings of Crypto, 1983

[3] COUNCIL OF EUROPE, Recommendation Rec (2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting

[4] D. CANSELL, J. P. GIBSON. Formal verification of tamper-evident storage for e-voting, in: Fifth IEEE International Conference on Software Engineering and Formal Methods. 2007. DOI 10.1109/SEFM.2007.26

[5] DEJONG ET ALL., Voter's Perceptions of Voting Technology, in: Social Science Computer Review, Vol. 26, No. 4, 2008 p.399-410.

[6] DIERKS, ALLEN. The TLS Protocol Version 1.0, IETF RFC 2246, January 1999. http://www.ietf.org/rfc/rfc2246.txt

[7] H. NURMI, A. SALOMAA, L.SANTEAN. Secret ballot elections in computer networks, in: Computers & Security Volume 10, Issue 6, October 1991, Pages 553-560

[8] JUHANI KARHUMÄKI AND TOMMI MESKANEN. Audit report on pilot electronic voting in municipal elections, June 2008. http://www.vaalit.fi/uploads/5bq7gb9t01z.pdf (Elections website of the Finnish Ministry of Justice, query date: 2010-02-26)

[9] KOFLER, KRIMMER, PROSSER. Electronic Voting: Algorithmic and Implementation Issues, in: Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03) – Track 5, 2003.

[10] LANGER, SCHMIDT, VOLKAMER, BUCHSBAUM. Ein PKI-Basiertes Protokoll für sichere und praktikable Onlinewahlen, in: Proceedings of EDEM 2009 – Conference on Electronic Democracy, Vienna, 2009.

[11] M. MCGALEY AND J. MCCARTHY. Transparency and e-Voting: Democratic vs. Commercial Interests. In Electronic Voting in Europe - Technology, Law, Politics and Society, pages 153– 163. European Science Foundation, July 2004

[12] PROSSER, A., KOFLER, R., KRIMMER, R., UNGER, M. 2004. E-Voting Election Test to the Austrian Federal Presidency Election 2004. Working Paper 02/2004 des Institut für Informationsverarbeitung und -wirtschaft der Wirtschaftsuniversität Wien.

[13] SCYTL Pnyx.Core, E-voting Core Security Technology, http://www.scytl.com/_a_productos/Pnyx.Core.pdf (query date: 2001-02-27)