






Secret Voting: Knowledge vs Trust

Ildar M. Khamitov¹(✉) , Victor Dostov² , and Pavel Shoust² 

¹ Saint-Petersburg State University,
7-9 Universitetskaya Emb., St Petersburg 199034, Russia
CryptoVoter@gmail.com

² Russian Electronic Money and Remittance Association,
5/2 Orlikov per, Moscow 107078, Russia
{dostov, shoust}@npaed.ru

Abstract. In this paper we discuss on the general level the issue of trust the voters put in the secret voting system used in political elections. We promote the point of view that the voters' recognition and acceptance of a particular voting system should be based not on trust, but on knowledge—on the knowledge of what is really happening during the voting, not presumed. The starting point of knowledge is mistrust. We formulate a postulate of mistrust (of an election commission) and keeping it in mind look closely at several deployed voting systems including the Estonian one. We find all of them unacceptable. Then we formulate three criteria for an Internet voting system to be acceptable to the voters (civil society). These are (1) openness, (2) acceptance of the system by an uncertain and broad set of qualified examiners and (3) a verifiable access of unsophisticated voters to the voter's software approved by the aforementioned set of examiners. Finally, we explain only the modest role of the official (government) certification of the voting system in its recognition by the voters (civil society).

Keywords: Secret voting · Internet voting · Mistrust · Estonian Internet voting system · Civil society

1 Introduction

When discussing the practical use of a secret voting system in political elections, the issue of trust the voters put in the system under discussion inevitably arises. The issue of trust is particularly acute with regard to technically equipped voting systems, in particular Internet voting systems (which we are most interested in). Usually it is not very clear why the voting system inspires trust in the electorate, what extent this trust should reach to make the voting system acceptable, and so on. And these are not idle questions, because, although it may not be so yet, in the end it is the civil society that has to accept or reject a particular voting system. In this article, we advocate the following view: Russian citizens' recognition and acceptance of a particular voting system should be based not on trust, but on knowledge—on the knowledge of what is really happening during the voting, not presumed. Part of that knowledge is mistrust. In this case, the word “mistrust” doesn't mean having vague doubts, but a certain approach to the analysis/development of the voting system, as well as knowledge on

the basis of which a bad voting system is rejected. The role of trust (whose trust, trust in what and to whom) we will discuss in one of the following sections.

There has been extensive literature on electronic voting. For example, Gritzalis formulated the basic principles and requirements towards secure e-voting [1]. Cloud computing has been proposed in this domain as well [2]. The importance of transparency and audit were underlined in the work by Samra, Hafez, Assassa and Mursi [3]. However, methodological assumptions about the trust issues are still beyond the academic purview.

We will begin by clarifying an approach based on mistrust that forces us to assume the worst. We will formulate the worst in the form of a postulate.

2 The Basic Postulate of Mistrust

The concept of trust is a matter of concern in election systems since the time of Ancient Greeks [4]. Here we look at general trust issues and start with formulating the postulate of mistrust.

Postulate of Mistrust

The main goal of the election commission is to solve the following two tasks:

1. *the election commission shall imperceptibly and unprovably falsify the results of voting,*
2. *the election commission shall imperceptibly and unprovably violate the secrecy of each voter's choice.*

Certainly, there are many villains who pursue the same goal, but the election commission (hereinafter EC) is obviously in the favorable position in terms of achieving this goal, as it is less limited in actions than other villains, as it has access to and influence on data in the process of preparation and voting.

It should be noted that in the context of this essay, the EC is composed not only of those who are formally members of the commission's staff, but also of those who can influence the EC during the preparation, voting and result compilation processes, without being its employees. For example, voting system developers, programmers, contractors, equipment suppliers, system administrators of the EC servers, etc. are among the suspects.

Not all threats to the integrity of the vote are formulated in this postulate, but this is enough for our purposes. We will note only that the secrecy of voting (secrecy of voter's choice) means the right of the voter to keep his/her vote in secret from all and availability of technical means to exercise this right.

Thus, we adhere to a paranoid approach to the analysis of various voting systems.

3 Conventional System of Secret Voting

The secret voting system that uses tangible (usually paper) impersonal ballots, which are collected in ballot boxes at polling stations, we will call a conventional system of secret voting.

The ways to falsify the voting results of the conventional secret voting are too diverse to be discussed here. We will only mention the modern version of falsification by means of abusing new absentee ballots, introduced in 2018 and called “Voting at the place of stay” or “Mobile voter” [5].

The idea is that the EC’s accomplice first registers via the Internet as a voter at several polling stations (with a little help from the malicious EC according to our “postulate of mistrust”). At the day of voting this accomplice can cast more than one vote visiting all the polling stations with which he or she has registered.

The protocol of the conventional secret voting was designed to meet the aforementioned requirement of the secrecy of voter’s choice. However, this protocol is vulnerable. Taking into account a significant progress in printing and other technologies, the conventional voting system should be considered as the open (non-secret) one for the EC. Any operations with tangible objects during personal voting at the polling station makes it impossible to preserve the secrecy of the voter’s choice. Firstly, a paper (more generally tangible) ballot is a very complex physical object. The voter cannot check whether the ballot he received is impersonal and does not carry individualizing marks in the form of microtext, micro-punctures, small distortions of the security marks and ornaments, certain displacements of the design elements, invisible chemical marks, RFIDs, etc. Secondly, the EC can install a lot of hidden video cameras at the polling station to reliably record each and every movement of the voter from all view angles.

Conventional voting systems have another significant fault in ensuring the secrecy of choice, associated exclusively with their organizational form. After the end of voting time the votes cast are counted separately at each polling station. In Russia, around 750 people vote at each polling station on average. If all the voters voted unanimously at a given polling station, then, for obvious reasons, there is no secrecy of choice at this polling station. In case of the Internet voting, the “Internet polling station” includes millions of voters—ideally all 110 million Russian voters. A unanimous vote at such a large “polling station” is much less likely than at a small physical one.

4 Voting Using “Black Boxes”

If technical devices (scanners) are used to process and count the tangible (paper) ballots cast at polling stations, we will call such a system a conventional automated system of secret voting. In the terminology of the Central Election Commission of the Russian Federation (CECRF) automated voting is implemented through the Ballot Processing Devices (BPD) [5] with optical scanners. After filling out a paper ballot, the voter inserts it into the BPD’s scanner, which draws the ballot into the inside and stores it there.

If voters vote without tangible ballots by pressing buttons or touching touch screens of terminals installed at polling stations, we will call such a system a conventional electronic system of secret voting. Again, in the terminology of the CECRF electronic voting is implemented through the Electronic Voting Devices (EVD). The EVD includes a touch screen, so that the voter makes his choice by touching virtual buttons. In addition to the image on the screen, the voter’s choice is printed on a control paper tape and shown to the voter through a small window.

From the point of view of civil society both BPDs and EVDs are “black boxes”, that is, devices, which construction and operation algorithm are unknown. The “black box” receives the real choice of the voters as input, and outputs some “result”. The way this “result” relates to the choice of voters is unknown to the civil society, but not because its representatives are lazy to examine the construction and software of the “black boxes”. Of course, one can study the technical documentation of the “black box”, and a small group of experts (certification body) can dig into a couple of “black boxes”. What will that prove? On the one hand, there is a need to trust a small group of experts exposed to harmful influences, which is unacceptable in our paranoid approach. On the other hand, the voter will never be able to establish what relation this “black box” at this polling station has to the publicly available technical documentation of the “black box”, as well as to those “black boxes” that were presented to the experts. Unfortunately, the copy of a “black box” cannot be digitally signed! Due to the inherent closeness of the “black boxes”, voting with their help provides the EC with ample opportunities for falsifying the results of such voting.

BPDs add new methods of fraud in the conventional voting. The voter cannot know what the BPD does with the ballot. A voter sees how the BPD is drawing the ballot into the inside so that the ballot disappears from the sight for some time. So the voter cannot understand what then falls into the translucent receiving ballot box. For example, if the voter’s ballot contains a “wrong” choice, the BPD may place it in its secret compartment and drop a pre-prepared ballot with the “right” choice into the receiving ballot box. In this way, the BPD can replace several hundred ballots. Another way of the falsification lies in the fact that the BPD can make the “unwanted” ballot invalid by marking an extra field in the ballot in the process of drawing it into the inside.

Falsification of voting results with the help of the EVDs does not have borders at all. One should not have illusions about the control tape, which is supposedly printed by the EVD. At the end of the voting, a tape bearing the falsified results will be extracted from the EVD, while during the voting, a fragment of a completely different piece of tape with a short list of all options could be shown to the voter via the EVD’s window.

In the conventional electronic system of secret voting, when voters vote with the help of EVDs, there is no secrecy of choice at all. In this case, the EC has to exert even less effort than in the case of the conventional voting system to get the name, fingerprints, photograph and the choice of the voter as soon as he or her finishes the voting procedure. In the case of the conventional automated system of secret voting, where voters insert ballots into the BPD’s scanner, the only thing the EC will not be able to easily obtain are the voters’ fingerprints.

Despite the obvious defectiveness of conventional automated and conventional electronic voting, politicians and officials, as well as some human rights activists, support the deployment of these systems and they are trying to form a positive image of the “black boxes”. Often this is done under the slogan of increasing transparency (!?) of the voting process, as well as under the guise of caring for the employees of the EC.

If we reject with indignation the understandable desire to control the voting results, it is difficult to rationally explain why a part of civil society supports the introduction of “black boxes” into the practice of voting. Apparently, the magic words “computerization”, “information technology”, “high-tech”, “innovation” outweigh the arguments

of reason. Moreover, many people consider computers and other hardware as independent and impartial creatures who can be entrusted with the sensitive things like an objective vote count. Of course, hardware is devoid of passions, but it is also devoid of mind and conscience so that it thoughtlessly executes the program installed in it. Therefore, the “black box” will falsify the results of the vote, with no remorse, if it is designed and programmed to do so.

5 Estonian Internet Voting System

Early voting via the Internet is allowed in Estonia¹. The Estonian Internet voting system uses cryptography to imitate the voting by the snail mail with the help of two envelopes.

Leaving the technical and bureaucratic details aside, one of the procedures for the two-envelopes voting goes as follows. The voter receives, either in person, by mail or any other way, the following:

1. paper ballot,
2. impersonal (blank) and non-transparent envelope,
3. personalized (that is, bearing identifying data of the voter) envelope addressed to the EC.

At the appropriate time, the voter fills in the ballot and seals it in the first, impersonal, envelope. Then the voter seals the sealed impersonal envelope in the second, personalized envelope and sends this nested letter to the destination (to the EC). At the post office the voter can further identify himself/herself by presenting his/her passport. It is assumed that the EC has two employees (or departments): Verifier and Teller (Ballot Box Keeper). The nested letter from the voter first gets to the Verifier, which according to the information specified on the outer envelope, checks that the sender is on the list of voters, that is, has the right to vote, and notes the fact of voting in this list. Then the Verifier extracts the impersonal envelope from the outer envelope and passes it to the Teller. The Teller extracts the ballot from the impersonal envelope and unorderly drops it into the ballot box.

The Verifier knows who took part in the vote but doesn't know the voter's choice. The Teller doesn't know who took part in the vote but knows the voter's choice. Communication between the Verifier and the Teller is prohibited. Therefore, the link between the voter's identification data and his or her vote in the current voting is severed.

It is easy to transform this scheme from the mail voting to the Internet voting. The asymmetric encryption with the Teller's public key is used as an impersonal envelope, the voter's digital signature and asymmetric encryption with the Verifier's public key are used as a personalized envelope.

¹ The Internet voting has been used in Estonia nine times since 2005. For example, during parliamentary elections in 2007, 2011 and 2015 share of voters who voted over the Internet was 5.5%, 24.3% and 30.5% [6].

However, voting by mail and its Internet counterpart are as bad as possible. These systems are much worse than the conventional voting system. The voter cannot know and cannot check whether the EC follows the declared procedure of processing the nested letter sent by the voter. That's why according to our basic postulate of mistrust, the Verifier and the Teller can (should) collude and find out the choice of the voter. In addition, the joint Verifier-Teller may replace the voter's ballot with any other ballot at their discretion. Moreover, this can be done by the Verifier alone. Thus, in the Estonian Internet voting system, the EC can imperceptibly and unprovable falsify the results of voting, as well as violate the secrecy of each voter's choice.

6 Requirement of Openness

The example of Estonia shows that a simple system of secret Internet voting can be absolutely unacceptable to civil society. At the same time correct system of the secret Internet voting will be technically complex, since it, for example, inevitably has to make abundant use of sophisticated cryptography. For this reason, it seems that civil society will not be able to come to a consensus on any complex voting system, since it does not consist only of doctors of mathematics, cryptography, electronics and IT sciences who understand the issue. Moreover, such professionals form a smaller part of the civil society. Nevertheless, the situation is not hopeless.

For convenience, let's call the mentioned doctor of science a qualified examiner. Thus, the examiner can professionally analyze, if not the entire voting system, but at least its part or level (protocol, software implementation, etc.). The examiner may have nothing to do with voting and even be, for example, a foreigner. If the examiner himself/herself takes part in the voting, in this case we will call him a qualified voter. The voter who is not a qualified one will be called an unsophisticated voter.

It is impossible to have an opinion about the voting system based on knowledge without the full and continuous openness of the system. Thus, we will put forward the requirement of openness.

Requirement of Openness

1. *The protocol of the secret Internet voting,*
 2. *the specifications of the protocol,*
 3. *the source code of the software (in the voter's computing device), which, interacting with the EC server, executes the protocol in behalf of the voter,*
 4. *the executable code of this software, and*
 5. *some data (specified by the protocol)*
- must be public, that is, they must be published and available without restriction to all interested persons for study and critical analysis and must be certified and protected from changes by the digital signature of an authorized agency. The fact that the executable code of the voter's software is derived from the presented source code should allow simple verification.*

The authorized agency mentioned here may be the EC, but there is no need for the EC to be the publisher of protocols, specifications, etc. This agency cannot be trusted and such trust is not required. The signature is necessary to prevent the authorized agency from disavowing the voting system published, or using something unpublished and not agreed upon with civil society. This signature protects the protocol and the rest of the voting system from unauthorized changes.

Generally speaking, the source code of the voter's software (hereinafter referred to as VSW) can be used to restore both the specifications and the protocol of the voting system, that is, there is no need to publish them. However, the openness of the Protocol expands the range of potential examiners, adding to them, for example, mathematicians and cryptographers who are not engaged in programming. For the convenience of analysis, the description of the protocol is usually made minimal (cleared of details), but complete. The latter means that further detailing of the protocol does not add anything significant to it in terms of the way in which the stated result is achieved. Moreover, the protocol is the starting point for constructing the voting system.

By analyzing the source code, the examiners can make sure that the executable code fully and accurately implements the declared protocol of secret voting, and that it does not contain anything superfluous and harmful to the voter.

In general, the executable code is obtained from the source code by a compilation process, which is carried out by a special compiler program. Unfortunately, depending on the manufacturer, version, and compiler settings, many different versions of executable code can be obtained from the same source code, which executables will be the same in terms of their functionality. This means that looking at the executable code, it is not easy to understand that it corresponds to the given source code, and this is critical for the voters and examiners, because only the source code is analyzed for compliance with the protocol. This explains why the above-mentioned requirement includes the simplicity of verification that the executable code is actually derived from the source code.

The requirement of openness has a couple of side effects. First, the development of the voting system can be entrusted to anyone: it's only important that he had the right talents and was skillful enough in coding. Secondly, a large number of voluntary reviewers makes it possible to find errors and vulnerabilities in the system more quickly and, accordingly, to correct them faster, as well as to improve the system without connection with errors.

It's not necessary to require the openness of the source code of the EC's software, since all the properties of the voting system must be ensured by the protocol.

7 Conditions for the Acceptability of the Voting System

The developers of the system of secret Internet voting try to meet the pre-formulated requirements for such a system. We will not go into the discussion of a possible set of requirements for the voting system and its variations here. Instead, we will formulate the general conditions for the voting system to be acceptable both to qualified examiners and separately to unsophisticated voters.

Conditions of Recognition by the Qualified Examiners

The system of secret Internet voting shall be deemed acceptable if

1. *qualified examiners confirm that the declared properties of the voting system reflect the views of civil society about the correct voting system,*
2. *qualified examiners confirm that the declared properties of the voting system are actually implemented in the VSW, and*
3. *no one (yet) can show such a scenario of the voting participants' behavior, which leads to a significant violation of any important declared property of the voting system (for example, the secrecy of choice).*

Tens of millions of Russian citizens can understand the requirements for the correct secret Internet voting system. Millions of citizens are able to understand the protocol of the correct voting system (subject to the acceptance of the properties of certain cryptographic operations), and tens of thousands will be able to professionally analyze it, as well as to influence its development. Hundreds of thousands of Russian citizens, if not more, can also scrutinize the source code of the VSW and make sure that the VSW fully and accurately implements the declared protocol of secret Internet voting, and does not contain anything superfluous and harmful to the voter². They can also influence the creation of the source code of the VSW at the development stage, and can also check that the EC distributes the version of the executable code of the VSW, which was verified and accepted by civil society and bears the signature of the authorized agency. Numerous tech-savvy foreigners can participate as well.

Such a multi-million team of independent examiners, which team has no formal membership, cannot be bribed, intimidated or misled by various paid certificates. A huge number of people who understand why it is impossible to falsify the result of voting and violate the secrecy of choice, will help an unsophisticated voter (and hence the society as a whole) to develop the trust in the system through developing the trust in independent examiners, some of whom such a voter may know even personally.

Condition of Protection of an Unsophisticated Voter

The voter should be able to obtain the VSW for their computing device and make sure that he or her has at their disposal exactly the version of the VSW approved by the qualified examiners, that is, by the civil society.

The meaning of this condition is that an unsophisticated voter must reliably merge with the crowd and be indistinguishable from a qualified voter. From behind the “wall” of the approved VSW, all voters look as qualified ones. It is therefore important that no villains can deceive the unsophisticated voter into obtaining a malicious VSW. To get the VSW, the voter must follow the approved instructions and, in particular, make sure that he or she has obtained the version of the VSW approved by the civil society. The digital signature of the authorized agency and the publication of this signature on the

² According to Microsoft, there were 350 thousand professional software developers at the end of 2010, and this figure grows by 20 thousand annually. This estimation is based on the number of licenses for developer's software sold in Russia. Microsoft also estimated number of non-professional software developers at 850 thousand people [7].

websites of parties and public organizations will help him in this. Fortunately for unsophisticated voters, using the right system of secret Internet voting is not much more difficult than, for example, Estonian system, because all the complexity is hidden inside the VSW.

8 Certification, Attestation, Audit and All That

A certificate is a document confirming the compliance of a certain object, such as a voting system, with certain requirements, standards, regulatory documents, etc. Such certificates are issued by an authorized certification organization, by the process of certification.

The main problem with certification is that the group of experts conducting the certification is fixed and small. And a fixed and small group of people (among whom can be stupid, and greedy, and cowardly, and “their own” members) is prone to various outside influences (deception, bribery, intimidation, instruction, etc.). As the result it is not possible to trust such certificates.

In fact, due to the openness, the correct protocol of the secret Internet voting, its specifications and implementation on the voter’s side do not require any certification or other approval from the state bodies. More precisely, for the civil society, any official certificate does not provide a decisive reason for accepting a given voting system, and the absence of a certificate does not provide a decisive reason for rejecting the system. A certificate represents only one view in the public debate within the civil society on the acceptability of a particular system of secret Internet voting. If the authorities want someone (some entity) to be engaged in analysis and participate in public discussion of a given system of secret Internet voting on duty, and not only on their own, then they can entrust this care to any of their controlled structures or suitable external organizations. If desired, these structures or organizations can be called the authorized certification organizations.

From the voter’s (civil society) perspective, certification, attestation, audit and other similar activities on the side of the EC are of no interest, since they do not play any role in ensuring the integrity of voting and the secrecy of choice. In addition, the results of these activities cannot be verified and determined as to what they relate, as there is no way for all civil society to monitor day and night every action of the staff of the certification organization.

From the government point of view certification, attestation, audit and other similar activities on the side of the EC are still needed, but for other purpose. The purpose is simple. Voting should take place under any conditions, that is, it should be provided with appropriate technical support. This means that the EC staff must be qualified, the equipment must be productive and reliable, the software must be tested, the data must be backed up remotely in real time, the power supply must be uninterrupted, access to the server must be limited, fire safety must be in good condition, etc., etc. All this should be confirmed by certifications, attestations, audits and other similar activities on the side of the EC.

9 Conclusions

Using a paranoid approach to the analysis of several deployed voting systems including the Estonian one, we found all of them unacceptable. So we put forward three criteria for an Internet voting system to be acceptable to the voters (civil society). These are (1) openness, (2) acceptance of the system by an uncertain and broad set of qualified examiners and (3) a verifiable access of unsophisticated voters to the voter's software approved by the aforementioned set of examiners. We believe that the recognition and acceptance of a particular voting system should be based not on trust, but on knowledge—on the knowledge of what is really happening during the voting, not presumed.

References

1. Gritzalis, D.A.: Principles and requirements for a secure e-voting. *Comput. Secur.* **21**(6), 539–556 (2002)
2. Zissis, D., Lekkas, D.: Securing e-Government and e-Voting with an open cloud computing architecture. *Gov. Inf. Quarterly* **28**(2), 239–251 (2011)
3. Samra, K.M., Hafez, A.A., Assassa, G.M., Mursi, M.F.: A practical, secure, and auditable e-voting system. *J. Inf. Secur. Appl.* **36**, 69–89 (2017)
4. Randell, B., Ryan, P.Y.: Voting technologies and trust. *IEEE Secur. Priv.* **4**, 50–56 (2006)
5. <http://cikrf.ru/eng/activity/relevant/detail/39450/>. Accessed 31 Mar 2019
6. <https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia>. Accessed 31 Mar 2019
7. <http://cloud.cnews.ru/news/top/index.shtml?2010/04/12/386342>. Accessed 31 Mar 2019