Transparency in Electronic Voting : the Great Challenge

Chantal Enguehard

IPSA International Political Science Association RC 10 on Electronic Democracy. Conference on "E-democracy - State of the art and future agenda", Stellenbosch University, South Africa, 22 – 24 January 2008.

Transparency in Electronic Voting : the Great Challenge

Chantal Enguehard
LINA - UMR CNRS 6241
2, rue de la Houssinière
BP 92208
44322 Nantes Cedex 03
France

Abstract:

Voting must respect several criteria to be democratic. In this paper we determine whether electronic voting can simultaneously protect secrecy, be transparent, accessible and resistant to intimidation and fraud.We consider different types of e-voting ranging from Direct Recording Electronic voting systems to remote internet voting. We show that there are major contradictions between the constraints of democratic elections and the possibilities offered by computers. In particular, electronic voting appears to make massive and invisible fraud possible to achieve by small groups of people with the necessary skills. At present, it is not a realistic possibilility to design an electronic application, remote or not, that could cope with the demands of democratic elections.

Keywords:

democratic elections, electronic voting, DRE, VVAT, fraud, accessibility, intimidation, vote selling, internet remote voting, remote voting.

Introduction

Counting votes is simple, it becomes a huge problem when there are millions of voters. Automation of the voting process has a long history. In the USA, where multiple polls are usual, there were early attempts to automate the casting and the counting process: automatic booth lever voting machines and punched card voting machines appeared in the beginning of the 20th century and rapidly spread through the urban centres of the country. Since 1960, several types of electronic optical mark sensing scanners have been adapted to count votes. The first electronic voting machine which allowed votes to be cast directly without any ballot paper appeared in 1974 (the Video Voter system). Lastly, computers were adapted for use in 1982 with the Microvote Electronic Voting Computer.

Electronic voting (or e-voting) is, therefore, a term which refers to various voting processes where computers are used to count votes and/or to cast votes. There are now many different models and types of electronic voting systems in use in a dozen countries. Some of these countries use them in a generalized way. We can cite: Brazil, India, Netherlands, Venezuela and United States of America. During this brief history, some countries have had to abruptly revise their decisions about the computerization of voting procedures because technical, sociological and ethical problems arose[1]. After twenty-five years of use we can now take stock of these different experiments.

In this article we will describe several features of e-voting: transparency, accessibility, and resistance to intimidation and fraud. After reiterating the definition of genuine elections as defined by international organizations, this paper will present a typology of e-voting. Then, it will analyse different electronic voting systems in order to evaluate their compatibility with several criteria which define democratic elections. Finally we will compare these different electronic systems with a traditional paper ballot system and demonstrate that electronic voting facilitates massive and invisible frauds.

1 Electronic voting, first introduced in the Netherlands in the early 1990s and used in 90% of the country, has been withdrawn in favor of traditionnal ballot paper and red pencils in October 2007.

1. Genuine elections

1.1 - Basic principles

The basic principles of genuine elections are defined in article 21 of The Universal Declaration of Human Rights (accepted by all the member states of the United Nations):

> « The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures. » [United Nations 1948]

This article 21 describes some characteristics of genuine elections: there should be no discrimination of any kind, such as that based on race, colour, sex, religion, etc. (universality) each voter may cast only one ballot which is counted as one vote (equality), voting should take place in privacy. Most importantly genuine elections should return an accurate result which fairly conveys the will of the people. The reliability of the election process must be proved and the election system must be observable and observed to give confidence and be regarded as trustworthy.

In this article we will not discuss all the conditions that have to be considered to meet fair elections, we will focus only on particular features: transparency, which allows confidence, accessibility, which is the right of every voter to vote and we will observe how the system is protected against fraud and how it protects voters against intimidation.

1.2 - Transparency for inspiring confidence and ensuring trustworthiness

Confidence in the election system is crucial because this will influence whether the election results are accepted.

The election system should provide sufficient evidence to convince the losing candidate that he or she actually lost. People who voted for the defeated candidate will only accept the winner if they believe the system is fair. In the case of low voter confidence, the elected person's legitimacy could be called into question which could potentially result in violent disturbances and political instability. If there is to be high confidence in the electoral process, genuine elections are vitally important because they enable a peaceful resolution of the struggle for political power and are therefore, central to the maintenance of peace and stability.

This confidence is based on the premise that all aspects of the elections process are directly observable, by the candidates, the official observers and the people themselves. Observations must cover all the stages of the voting process: the pre-election period (constitution of the election commission membership, registration of candidates, of voters, etc.), the election day, the vote count and the post-election period (announcement of the results, treatment of complaints, etc.) [ODIHR/OSCE 2005]. We will only focus here on a few stages that are affected by electronic voting.

Observations should be consist of practical evidence that is directly related to the voting process and which anyone may gather. It must not be limited to a simple examination of the results of the voting process because these results may not reflect the voters' intents. Observing a representation of the voting process is also unsatisfactory because the representation of the voting process may be erroneous. A representation of an object is not the object itself[2].

The demonstration that the voting urn is empty at the beginning of polling day is a good example which illustrates this fundamental idea. This may be done in several ways. The first possibility would be to have a transparent empty urn people can see and touch. Alternatively there could be a wooden urn which people could see inside when open, but which they could not touch. A third method could consist of a wooden urn which is opened by an official who then confirms the urn’s

2 This idea is expressed is the well-known Magritte painting representing a pipe and illustrated with the words "Ceci n'est pas une pipe" (this is not a pipe).

emptiness. A fourth situation would be to have a voting computer print a ticket which announces that there are no vote in its memory. These four different situations illustrate a successive decline in observability from the first situation, which is a fully observable, to successively more unsatisfactory ones in which the non-emptiness of the urn could not be detected (in the second case the urn could have a false bottom that hides ballots, in the third case people have to trust the official, in the last case, people have to trust the computer program).

Thus, transparency which allows direct observation is a key-concept for genuine elections: it allows the detection of structural defects and of some threats to the election process or the voters themselves (frauds, intimidation), that could alter the results.

Transparency is a requirement in intergovernmental organizational guidelines for elections.

In its Election Observation Book, the Organization for Security and Co-operation in Europe defines

> « A genuine election is a political competition that takes place in an environment characterized by confidence, transparency, and accountability and that provides voters with an informed choice between distinct political alternatives. » [ODIHR/OSCE 2005]

The European Commission for Democracy through Law emphasizes the necessity for electronic voting systems to be transparent. This commission mentions explicitly that free suffrage can be achieved only if the right to act to combat electoral fraud is guaranteed and if the voting procedure is simple [ComVenice 2002].

In the Principles and Guidelines Governing Democratic Elections, the Southern African Development Community states

> « Ensure the transparency and integrity of the entire electoral process by facilitating the deployment of representatives of political parties and individual candidates at polling and counting stations and by accrediting national and/other observers/monitors; » [SADC]

In this last guideline we must note that voters themselves are not given the explicit authority to ensure the transparency and integrity of the electoral process yet these issues are major concerns of voters in their role as proprietors of sovereignty as is the case in all democracies[3]. In democracies people entrust their representatives, designated at elections, with many executive powers. The power to ensure the transparency and integrity of the electoral process is not given to representatives because if this was the case then these representatives would have all executive power and the electorate would no longer have any power at all which is contrary to the concept of democracy.

1.3 - Accessibility

The electoral process must allow the population to vote in privacy without any human assistance, including elderly or disabled people or any illiterate person.

1.4 - Resistance to intimidation and fraud

The electoral process must prevent bribery (“I’ll pay you 15 euros for your vote”) and coercion (“I’ll break your face if you don’t give me your vote”) at the level of individual voters.

2. Different types of e-voting

2.1 - Direct Recording Electronic - DRE[4]

Direct Recording Electronic systems are computers. They are placed in the polling stations where

3 Democracy literally means “rule by the people”. It is derived from the ancient Greek words demos (δημος), "people", and kratos (κρατος), “rule”.

4 In French: Ordinateurs de Vote avec Bulletin de vote Dématérialisé (OdV-BD)

the voters usually vote. They are not responsible for identity verification which is required to ensure the uniqueness of each vote. The entire process of voting takes place in booths: noting the different candidates, choosing, casting the vote. Votes are directly stored and counted by computers, there are no paper ballots. At the end of the poll, results can be presented in different formats, depending on models and laws. Printed papers could be issued from voting computers, or digital information could be transmitted to the centralization station. Some systems could send the results directly via the internet network.

2.2 - Optical scanning systems[5]

These systems are also placed in usual polling stations. The voters fill out their ballot paper as usual, in a booth. Optical scanning systems are simply used to count votes on ballot papers. This may take place throughout the voting day: voters directly cast their vote into the optical scanning system of their polling station and the optical scanning system delivers results after the close the poll. Alternatively the scanning systems may be used at a later stage: ballots are collected in a urn, optical scanning is then done by officials to count the votes after the poll has closed.

2.3 - Voter Verified Audit Trail - VVAT[6]

This second generation of voting computers appeared around 2002. They are referred to by several terms, all of which are equivalent : Voter Verified Audit Trail (VVAT), but also “Voter Verified Paper Audit Trail” (VVPAT) or Voter Verified Paper Records (VVPR).

The main idea is to attach a printer to each DRE system. When a voter chooses a candidate the system generates a ballot which the voter can read in order to verify that what is printed is really the choice he made. When he confirms his choice the ballot is then collected in an urn [Mercuri 2002b].

2.4 - Voting Kiosk[7]

Voters can vote in any polling stations. The voting computers are linked to a remote server. Votes are registered in the server's memory.

2.5 - Internet Remote Voting[8]

Voters can vote from any computer connected to the internet. They will have been previously provided with authentication keys: login and password. Votes are registered by the voting application server.

2.6 - Non Internet Remote Voting

Experiments have been done with other remote voting systems such as short message service (SMS) or digital phone calls.

3. Analysis

3.1 - Transparency

The nature of computers is that their inner workings are secret. Since transactions and calculations happen at an electronic level, it is not physically possible for humans to observe exactly what a computer is doing [McGaley 2004].

Voting computers are often presented as straightforward computers such as those we are familiar

5 In French: Ordinateurs de Vote avec Bulletin de vote Matérialisé et Numérisé (OdV-BMN)
6 In French: Ordinateurs de Vote avec Bulletin de vote Matérialisé Vérifié par chaque Électeur (OdV-BMVÉ)
7 In French: Kiosque à Voter
8 In French: Vote à distance par internet

with from everyday use, for example when we withdraw money from a bank automat or when we buy a train ticket. In fact there are two very important differences. Firstly, when a withdrawal is made from a bank automat the result of this operation is clear – the relevant bank balance will have been reduced by a verifiable amount. The results of an election, however, are not known in advance, so it is impossible to deduce from the election result whether a voting machine has worked properly. Second, when purchasing a train ticket, or buying things over the internet, a purchaser will know exactly what would happen (goods will be received, and the correct amount of money will be debited from client's bank account). We observe that the secrecy of the vote forbids observation of the system during the voting period while, in commercial transactions, the identity of buyer and seller are known and registered, allowing verifications.

The impossible prediction of the results and the respect of anonymity are special characteristics of voting processes that do not appear with common computerized application.

3.1.1 - Direct Recording Electronic Voting Computers (DRE)

It is impossible to directly verify that the computer registers the votes exactly as they are cast by voters. Neither the voters, the officials organizing the votes nor the purchasers really know if a voting machine properly registers each vote.

Tests, whether they are done by experts before or after the vote, are not appropriate procedures with which to ensure that the software delivers accurate results and that the computers run smoothly: a computer can function properly during tests but may not do so during the real election because of bugs or errors. Even in the more reliable industries, such as aerospace, there is no completely reliable method known which enables software to be designed and implemented so that computers do exactly what they are supposed to [Schneier 1999].

> « It's entirely possible that a DRE voter could vote for one candidate, which would be displayed on screen, while an entirely different candidate could be recorded internally as having received that vote. » [Wallach 2005]

These types of error, which occur in opaque environments, are completely undetectable because there is no way to notice them. In addition any failure that affects the recording of the vote or the integrity of vote data can cause unrecoverable errors..

DRE voting machines are used by many states like Belgium, France or United States of America. In these states a certification procedure is supposed to give the assurance that the voting machines conform to standards, ignoring that today's certification and "logic and accuracy testing" are completely insufficient to detect such problems. Many scientists claim that the defined standards present serious problems and that such certification procedures do not catch the majority of security or usability problems [Alexander 2004], [Mulligan 2004], [McGaley 2006], [Barr 2007].

Because these machines are not observable, nor auditable, they can not be used with confidence. This inherent lack of transparency makes the DRE voting machines inappropriate for democratic elections.

3.1.2 - Optical scan systems and Voter Verified Audit Trail (VVAT)

With these two voting systems, the production and storage of paper ballots allows ballots to be recounted in order to verify the results given by the machines. The ability to perform such a recount provides a critical defence against the risk of failures.

We must evaluate whether electronic voting systems which enable the possibility of a recount may be considered to be transparent voting systems.

Firstly it should be noted that while the accuracy of these voting systems may be verifiable this does not necessarily mean that they will effectively be verified. The major flaw is that they could return a result which will instantly become official, even if there is no verification at all or if the verification is not properly done.

Secondly, performing a meaningful verification is a complicated task because it involves many tricky questions that deal with scientific, legislative and social subjects. All of these aspects could have a strong influence on the verification procedure.

From a scientific point of view, we must note than even if one machine was shown to function correctly, it does not prove that another machine did so too. The idea of verification of a small number of the machines to prove that the entire machines are then verified is a non sense. The verification method itself is also crucial. The National Institute of Standards and Technology recommended that only "software independent" voting systems be certified. "Software independent" systems can be audited without relying on any software for the reliability of the audit [NIST 2006]. This recommendation clearly points out that the recount should be done manually, without any software.

Although it is senseless, a random choice of the machines to be tested is made in many countries that use VVAT systems. In such a case, the law must say how the machines to be tested are chosen because this procedure should be carefully examined to ensure that the choice really is random. This procedure should be transparent, and candidates and voters should have the right to ask for the testing of additionnal voting computers without being subject to costs. The law must also take in account a large amount of details in case of a dispute several days after the poll, for instance, voting machines must be kept in secured place forbidden anyone to modify them.

Finally, it will be socially difficult to organize large-scale verification because people will not be prepared to repeat a task that had been previously performed by a computer. There is a huge risk that people and officials will fail to organize verification after a few successfull polling days show test results that indicate no problems occurred. In addition, the commercial arguments will convince them that any verification is finally costly and useless.

The worst fault of optical scan and voter verified audit trail systems is that they can deliver results even when there is no verification at all. Finally it appears that the addition of ballot printers to DRE machines, instead of enhancing transparency, will lead to opacity.

3.1.3 - Remote Voting

Remote voting may be done using different devices (personal computers, phones) that can not be fully transparent. Voters can not verify if their vote is correctly stored and counted.

3.2 - Accessibility

It is extremely difficult to design a simple computer-human interface which is widely understandable and which can be used without any assistance. In the overall voter population there are elderly, illiterate and disabled people (blind people)[9] who may have problems when using voting machines. Many of these people may vote with assistance from a third party. This has implications regarding privacy and therefore their votes cannot be considered to have been cast freely.

Any voting system should be designed to be ergonomic (user friendly). It would appear that current systems were developed without following common guidelines for usability when designing ballot forms, did not prevent the appearance of system messages which may cause alarm [Laskowski 2004] and did not properly take into account the possible use of the system by the disabled [Fields 2003].

Accessibility studies are rare because they are costly and difficult to organize for political reasons[10]. Nevertheless some research has shown that e-voting can affect election results by excluding a

9 In western countries, around a quarter of the voters are more than 65 years old, in numbers of economically poor countries, many voters, sometimes the majority, are illiterate. The consequences of these situations are rarely evaluated.

10 Accessibilty (and security, costs) have been widely used as commercial arguments. When officials decide to use e-voting they ususally tend to use the same ideas to convince the people about the new voting system they choose, even if there had been no real study on these questions.
Funding accessibility studies would be recognizing that voting machines do not fulfil their promises.

significant part of the population [Michel 1999]. Some people may not manage to vote for the candidate they intended to. They make mistakes because they are unfamiliar with the screens and may misunderstand the actions (like 'validate') they are required to perform. Observations during simulations showed that some people failed to vote as they intended and did not notice their error. The importance of this phenomenon has not been quantified.

3.3 - Resistance to intimidation and vote selling

3.3.1 - DRE and Voter Verified Audit Trail

Since the vote takes place entirely in a booth, a voter could film himself in one continuous shot (for instance with a mobile phone) from the moment he chooses his candidate until the vote is cast, bringing with him a proof of vote. This vote proof can then be exhibited to sell the vote, or may be forcibly exhibited in the case of intimidation.

3.3.2 - Optical scanning systems

The process described above would be inappropriate when using an optical scanning systems because people cast their votes publicly, outside of the booths: it would be difficult to make a one shot film without being noticed. Special equipment like cameras concealed in spectacles would allow this kind of film, but it is unusual, rare and may cost several hundred euros.

3.3.3 - Remote Voting

Remote voting, with or without electronics, offers no protection against intimidation or vote selling because people vote in an uncontrolled environment. The basic requirements for confidentiality are not guaranteed. Offering a possibility to re-vote ([Maaten 2004], [Van Acker 2004]) is not an appropriate solution to this problem.

3.4 - Resistance to fraud or errors

Changing the software of a computer changes the behaviour of the computer. So, changing the voting software of a voting machine is enough to change how votes will be stored and counted. It is easy to conceive of a program that would appear to behave as intended by voters and poll workers but that would divert some votes in the favour of a preferred candidate. Voting trends might remain unaffected but the preferred candidate would obtain more votes than really were cast by voters, which might be enough to win the race. This kind of fraud could be launched by a signal and kept dormant the rest of the time.

To be effective, a fraudulent program must be installed before polling day. Therefore, computers must be stored in secure places, secured by several locks whose keys are held by officals and people from different organisations in order to prevent any collusion to install a fraudulent program. Officials without any special skills in computers sciences may find this requirement difficult to understand because they may tend to believe that computers are inherently incorruptible[11]. In addition to this kind of storage being unusual, there is a lack of experience.

Many demonstrations of fraud have shown that less than five minutes are generally enough to replace correctly functioning software with a program that would give fraudulent results [CEV], [Kohno 2004].

The main problem is that a fraud which attacks firmware could have huge consequences by affecting a large number of machines. Achieving this type of fraud demands technical skill and it is out of reach of the general population, but could easily be done by well organized people. A few people with the necessary skill-set and the opportunity of access to the machines would suffice. For example technical staff working for the voting machine’s manufacturer or people with access to the machines during transportation or maintenance could install fraudulent software. We must note that

11 This argument is widely used by the vendors of voting machines.

there would no risk for the fraudsters because their illegal activities would take place before polling day.

These security flaws could be used by terrorists or foreign countries to destabilize a nation.

3.4.1 - DRE

With DRE, since there is no physical ballot, it is completely impossible to verify the results of the voting computer independently of the computer itself. By consequence detecting a fraud is impossible.

Some parallel tests could be organized. Several computers will be chosen to be tested during the whole polling day and will be in use in addition to those actually used for the election. The results from the test machines cannot be counted for the election because these tests' methodology implies cast votes are noted down and cannot be secret. At the end of the polling day the results directly issued by the tested machine are compared with the votes that had been manually recorded, any divergence will be detected, showing whether the tested machines were accurate or not.

The main problem is that these type of tests are easy to subvert. It is possible to automatically analyse the voting sequence to detect if it is a real vote sequence or a test. The computer could then choose to commit the fraud or not. In addition, parellel testing is completely inefficient in the case of a dormant fraudulent program that is activated by an accomplice[12] (for instance, it could be a voter who knows the secret combination of buttons of the voting machines needed to activate the fraudulent program).

Usually these kind of parallel tests are never organised because officials think that this is useless to test voting machines that they purchased because they were told that they had already been tested. In addition testing a voting machine during several hours, noting each vote, is complicated and prone to error. If there is a small difference between the results of the machine and what has been noted by hand, it would be possible to conclude with good faith that human errors occur when recording the votes.

3.4.2 - Optical scan systems and Voter Verified Audit Trail

It is comforting to have a printed paper ballot. Fraud seems more difficult to organize. In reality it just takes another form.

A recent study shows that, on DRE voting machines, most of the voters do not review screens at the end of the voting process and that they fail to detect malicious changes [Everett 2007]. This behaviour should be borne in mind when reviewing printed ballot paper. A machine which would sometimes present a ballot paper with malicious changes would be difficult to detect: most of the people would not notice the changes or, if they notice it, may think that they have made an error due to inattentiveness rather than conceive that the machine has made an error, and will cast their vote again, the machine would not attempt to cheat the same voter twice, so the rare voters who does notice an attempt to falsify the vote will probably not be believed

Discrepancies and fraud in counting can be detected only by the verification of the ballot boxes. Thus, the storage of the ballot boxes is crucial: any ballot tampering would be a major security flaw because it will raise the possibility that the ballot boxes have been altered to make them fit with the official results (coming directly from machines).The European Commission for Democracy through Law recommends explicitly that «Mobile ballot boxes should only be allowed under strict conditions, avoiding all risks of fraud.» [ComVenice 2002].

The identity of the particular computers which will be used as controls must be kept secret before and during the poll in order to avoid "easter egg" fraud.

12 This kind of functionality of a program, realeased by a secret sequence of interactions between the computer and a user is known as an “easter egg”.

There must be no legal limits placed upon the processes which are involved in counting ballots contained in ballot boxes. This ensures the election organizer cannot prevent votes in particular ballot boxes from being counted. The best place to organize an election fraud would be from within the body responsible for organizing the election.

3.4.3 - Kiosk and remote voting

There are many security flaws with remote voting or kiosk voting because they use devices that can not be fully controlled: personal computers can be affected by viruses or worms, different attacks can affect the server (e.g. denial-of-service attacks) or the connection spoofing (man-in-the-middle) [Jefferson 2004].

Parallel testing is impossible because votes coming from many kiosks or personal computers are stored by a very small numbers of servers.

4. Facts

Many studies did confirm the analysis which is presented below. Currently, the real situation is worse than the analysis suggests.

A few examples:

USA: The analysis of the DRE Diebold Touch Screen Voting Machine proved that these machines can be fraudulently modified without leaving any trace. A few minutes are enough to change the memory where the voting software is stored. [Open Voting Foundation 2006]

USA: Harri Hursti showed how to change the program of the Diebold optical scan system in a few minutes. His fraudulent program behaves as a virus: it is propagated from machine to machine [Hursti 2005].

USA: In November 2003 in Boone County, Indiana over 144,000 votes were cast using DRE voting computers even though Boone County contains fewer than 19,000 registered voters. And, of those, only 5,532 actually voted [Simons 2004].

South Korea: The Interior Ministry designed a VVAT system. In this system voters can verify whether the names that are written on its ballot are the ones of the candidates he chose, but it can not check this information in the encrypted image that figures also on its ballot. However, the verification procedure will count information stored in this encrypted image which has not been checked. The VVAT concept is here completely misunderstood, and the South Korean system should be seen as a DRE system.

Venezuela: The choice of the VVAT voting computers that have been verified in 2004, and then in 2006, has not been transparent. Although supposed to be randomly chosen, statistical studies demonstrated that verified machines were not representative of the whole [Delfino 2006]. For the last elections, 54% of the ballots boxes had been verified but even if the decision procedure has been transparent to the European Union Election Observation Mission, its random character has not been questioned by the members of this mission [EU EOM 2006].

USA: In November 2007, in Cuyahoga County, when it had been decided to recount ten races that were very close, officials discovered that 20% of the ballot papers were unreadable. They decided to make the voting machines generate a replacement copy that can be counted, even if these replacements had not been verified by electors.

Venezuela: During the 2006 presidential elections, the European Union observation mission noticed that voters encounter some problems when using voting machines in half of all the observed polling stations, especially amongst older people and in rural areas.

Australia: The Australian Capital Territory estimates in an observation conducted on the 2004 election, that 86% of voters found the electronic voting system easy to use [Green 2005]. Thus, 14% did not find it easy to use. This proportion is high. A significant part of these people had to

vote with assistance, or did not vote successfully as they intended. In researching a high-tech solution the ACT considered the replacement of a keypad with a touch-screen, forgetting that keypads are accessible to blind, while touch-screens are not.

USA: the Usability Professionals' Association highlighted several usability problems with electronic voting including cases of miscounts by optical scans, and various other technical difficulties [UPA 2004].

Estonia: Since 2003, people had been able to remote vote via Internet. During the 2006 elections in Estonia some vote-buying incidents became public [Maaten 2006].

This list is far from being complete.

5. Assessment

We must make a comparison between electronic voting systems and traditional voting systems.

5.1 - Transparency and fraud

Transparency still remains a problem for electronic voting.

DRE systems are completely opaque. These electronic systems are vulnerable to large-scale fraud which may be undetected due to their characteristics. Of course, some fraud occurs in traditional voting systems using paper ballots, but it is unlikely to be both massive and invisible. In traditional voting systems large-scale fraud is difficult to organize because too many people would be required and it could be more easily reported by witnesses who would be more likely to be aware of the fraud's existence and extent.

The transformation of DRE to VVAT by adding a printer is an attempt to enhance electronic voting system transparency, but our analysis shows that even when a system is fully verifiable, this does not necessarily mean that the verification process has taken place or will take place.This solution results in a voting system that may give results even when the verification process is neglected. A massive fraud could then be organized as with DRE.

The transparency of traditional systems with paper ballots can be enhanced by the systematic use of transparent urns, and the wider involvement of voters. Voters must have the right to observe or participate in counting votes in poll stations (avoiding the ballot move is a major safeguard against fraud), and to control the centralization procedure.

5.2 - Accessibility

Voting systems' accessibility is poor and could certainly be improved. Traditional system accessibility should be evaluated in specific studies, but we note that many people who are not confident with computers, have no problems with paper, envelopes and pens because these objects are encountered in every day life. Ballot design should be enhanced to reduce invalid votes.

By comparison electronic voting can not be comfortably used by numbers of voters, especially elderly people, blind people, or people who are not confident with computers.

5.3 - Resistance to intimidation

It is crucial to ensure the personal security of voters by avoiding any possibility that a voter may leave the poll station with a proof of vote upon which the selection the voter made is registered. This protection is assured by the traditional voting system where people must choose in booths, and publicly cast their vote. This manner of proceeding should have been kept with electronic voting.

In addition, ballots must be carefully designed, especially if Australian ballots[13] are used. The ballots must not display too many choices in order to avoid a common fraud: if there are many possible combinations of choices, each voter can be forced to select a particular, unique

13 This ballot type is named after its country of origin. On Australian ballots, the names of all-competing parties and candidates are grouped on a single sheet of paper, to be marked by the voter.

combination. If the voter decides to disobey the chances may be minimal that the selection which he was forced to make, will be made by chance by another voter, so his disobedience would be easily noticed.

6. Conclusion

After presenting some features of genuine elections, we described various types of electronic voting systems. We exposed the qualities and defaults of these different electronic voting systems with regard to transparency, accessibility, resistance to intimidation and resistance to frauds.

Our analysis demonstrates that traditional voting systems which use no electronic counting systems compare favourably to electronic voting systems when transparency is taken into account, transparency being a crucial factor in creating voter confidence in the voting system, and in consequence, in that of the elected representative's legitimacy.

Traditional voting systems are designed to be transparent and can be made extremely resistant to attempts to perpetrate large-scale fraud. Because there is no electronic counting aid, a guarantee can be given that every ballot will be manually counted, which, according to the National Institute of Standards and Technology, is the best procedure.

In contrast, all existing electronic voting systems appear to be designed with the capacity to hide large fraud which may they take place before polling day and which may be undetected. Errors could also remain undetected. Even the VVAT systems can not guarantee that each ballot paper be effectively counted.

In addition electronic voting systems would appear to deny the right to vote in privacy to an important proportion of the electorate. It has also been shown that they facilitate intimidation and bribery, and fail to protect individuals.

As long as these major defects are not be repaired, electronic voting should not be used for democratic elections. It would be conceivable to take advantage of the computer's great potential (accuracy, speed) after research has led to some major improvements with regard to the following difficult questions which have not yet been adequately answered: Is it possible to conceive of a computer-human interface usable by everybody without any assistance? Could an electronic voting system be devised which enabled observation of the computer's operation and yet allowed the principle of the secret ballot to be maintained? It is time now to fund major research in these exciting fields.

The use of electronic tools, and especially internet communication, has a great potential to enhance participation when considering information processing, communication and transaction. But it must be understood that voting cannot be considered as a common communication process because of special constraints: secrecy, anonymity, transparency, the need to check results and attempted fraud constitute a new paradigm that do not exist in any other activity. Quite apart from computers in a polling station, democratic voting is clearly incompatible with the internet for the moment (in addition, security problem are far from being solved [Schryen 2004], [Madise 2006]). Here again, new research projects which encompass scientific, ethical and sociological aspects are essential.

References

[Alexander 2004] Kim Alexander. The Need for Transparent, Accountable and Verifiable U.S. Elections. *A Framework for Understanding Electronic Voting*, 2004.

[Barr 2007] Earl Barr, Matt Bishop, and Mark Gondree. Fixing Federal E-Voting Standards. *Communications of the ACM.* vol.50, N°3, March 2007.

[ComVenice 2002] European Commission for Democracy through Law (Venice Commission). Guidelines on Elections. July 2002.

[Delfino 2006] Gustavo Delfino, Guillermo Salas. Analysis of the venezuelan presidential recall referendum of 2004 and the relationship between the official results and the signatures requesting it in computerized centers. August 22, 2006.

[Fields 2003] Manhattan Borough President C. Virginia Fields and The Center for Independence of the Disabled in New York, Inc. Voting Technology For People With Disabilities. March 2003.

[Fischer 2003] Eric A. Fischer. Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues. *Congressional Research Service, The Library of Congress*. November 4, 2003.

[EU EOM 2006] European Union Election Observation Mission. Presidential Elections Venezuela 2006 Final Report. 2006.

[CEV] Commission on Electronic Voting. Secrecy, Accuracy and Testing of the Chosen Electronic System, First and second Report. December 2004 and July 2006.

[Everett 2007] Sarah P. Everett. The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection. Rice University PhD., Houston, Texas, May 2007.

[Green 2005] Phillip Green. Electronic voting and counting for elections for the Australian Capital Territory. *E-Voting and Electronic Democracy: Present and the Future - An International Conference*, Seoul, Korea, March 17-18, 2005.

[Hursti 2005] Harri Hursti. Critical Security Issues with Diebold Optical Scan Design. *The Black Box Report*, July 2005.

[Jefferson 2004] David R. Jefferson, Aviel D. Rubin, Barbara Simon, David Wagner. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE). January 2004.

[Kohno 2004] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach. Analysis of an Electronic Voting System. *IEEE Symposium on Security and Privacy*, Oakland, CA, May, 2004.

[Laskowski 2004] Sharon J. Laskowski, Whitney Quesenbery. Putting People First: The Importance of User-Centered Design and Universal Usability to Voting Systems. *National Institute of Standards and Technology; and Whitney Interactive Design LLC*, 2004.

[Maaten 2004] Epp Maaten, Towards remote e-voting: Estonian case, *2nd International Workshop, "Electronic Voting in Europe* – Technology, Law, Politics and Society", *GI-Edition, Lecture Notes in Informatics*, Robert Krimmer (Ed.), pp.83-90, Bregenz, Austria, July, 7th-9th, 2004.

[Madise 2006] Ülle Madise, Tarvi Martens, "E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world", Electronic Voting 2006, *2nd International Workshop, "Electronic Voting in Europe* – Technology, Law, Politics and Society", GI-Edition, Lecture Notes in Informatics, Robert Krimmer (Ed.), pp.15-26, Bregenz, Austria, August, 2nd-4th, 2006.

[McGaley 2004] Margaret McGaley, Joe McCarthy, Transparency and e-Voting Democratic vs. commercial interests, *Electronic Voting 2006, Workshop "Electronic Voting in Europe – Technology, Law, Politics and Society", Lecture Notes in Informatics*, Robert Krimmer (Ed.), pp.153-163, Bregenz, Austria, July, 7th-9th, 2004.

[McGaley 2006] Margaret McGaley, J. Paul Gibson. A Critical Analysis of the Council of Europe Recommandations on e-voting. *Electronic Voting Technology Workshop*, Vancouver B.C., Canada, August 1, 2006.

[Mercuri 2002b] Rebecca Mercuri. A Better Ballot Box? *IEEE Spectrum Online*, October 2002.

[Michel 1999] Gabriel Michel, Walter Cybis De Abreu. Vers une exclusion technologique : expérience de l'évaluation ergonomique du vote électronique au Brésil. *IHM 99*, 8 pages, 1999.

[Mulligan 2004] Deirdre Mulligan, Joseph Lorenzo Hal. Preliminary Analysis of E-voting Problems Highlights Need for Heightened Standards and Testing. *Electronic Voting Best Practices A Summary*. based on the Symposium on Voting, Vote Capture & Vote Counting, Kennedy School of Government Harvard University, June 2004.

[NIST 2006] National Institute of Standards and Technology. Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC. November 2006

[Open Voting Foundation 2006] Open Voting Foundation. Worst Flaw Ever in Diebold Touch Screen Voting Machine. July, 31, 2006

[ODIHR/OSCE 2005] Office for Democratic Institutions and Human Rights / Organisation for Security and Co-operation in Europe. Election Observation Book. fifth edition, ISBN 83-60190-00-3, 2005.

[SADC] Southern African Development Community. Principles and Guidelines Governing Democratic Elections.

[Schneier 1999] Bruce Schneier. Security in the Real World: How to Evaluate Security. *Computer Security Journal*. v 15, n 4, 1999, pp. 1-14

[Schryen 2004] Guido Schryen, "How Security Problems Can Compromise Remote Internet Voting Systems", Electronic Voting 2006, *Workshop "Electronic Voting in Europe* – Technology, Law, Politics and Society", GI-Edition, Lecture Notes in Informatics, Robert Krimmer (Ed.), pp.121-131, Bregenz, Austria, July, 7th-9th, 2004.

[Simons 2004] Barbara Simons. Electronic Voting Systems: the Good, the Bad, and the Stupid. *ACM Queue* vol. 2, no. 7 - October 2004 .

[Thürer 2005] Daniel Thürer. Periodic, fair and free elections: important elements for the promotion and protection of human rights. *Second expert seminar "Democracy and the rule of law"*, United Nations, Commission on Human rights, Geneva, 28 February-2 March 2005.

[United Nations 1948] United Nations. Universal Declaration of Human Rights. 1948.

[United Nations 2005] United Nations. Declaration of Principles for International Election Observation. New York, October 27, 2005.

[UPA 2004] Usability Professionals' Association. Usability Problems Reported in the Media. 2004.

http://www.upassoc.org/upa_projects/voting_and_usability/voting_usability_problems.html

[Van Acker 2004] Bernard Van Acker, "Remote e-Voting and Coercion : a Risk-Assessment Model and Solutions", *Electronic Voting 2006, Workshop "Electronic Voting in Europe – Technology, Law, Politics and Society", GI-Edition, Lecture Notes in Informatics*, Robert Krimmer (Ed.), p.53-62, Bregenz, Austria, July, 7th-9th, 2004.

[Wallach 2005] Dan S. Wallach. Electronic Voting: Accuracy, Accessibility, and Fraud. *Democracy at Risk: The 2004 Election in Ohio*, 2005.