Electronic Voting in the Netherlands: from early Adoption to early Abolishment*

Bart Jacobs[1] and Wolter Pieters[2]

[1] Digital Security group, Radboud University Nijmegen, bart@cs.ru.nl
[2] Centre for Telematics and Information Technology, University of Twente, w.pieters@utwente.nl

Abstract. This paper discusses how electronic voting was implemented in practice in the Netherlands, which choices were made and how electronic voting was finally abolished. This history is presented in the context of the requirements of the election process, as well as the technical options that are available to increase the reliability and security of electronic voting.

1 Introduction

In information security research, electronic voting is considered a particularly interesting topic. This may be due to a number of reasons. First of all, elections usually have high media coverage, especially if something goes wrong. This makes it easy to explain the societal relevance of the research. Furthermore, electronic voting seems to have a unique combination of security requirements: voters need to be authenticated, results need to be verifiable, but it should *not* be possible to link a vote to a voter.

The secret ballot requirement, in combination with the so-called Australian ballot, listing all candidates on a single sheet, was introduced in many countries in the 19th century (see *e.g.* [28, 35]). It is now seen as a cornerstone of election law and international treaties: without the secret ballot, voters could be subject to all kinds of bribery and coercion, for it would be possible to observe the choices they would make in the election. Combined with the demand that results be verifiable, this requires well-designed procedures. It turns out not to be easy to computerise the intuitive ballot box property that what goes in will also come out, unaltered and unlinkably, especially if it is not allowed to reveal the identity of the voter.

Many electronic voting systems that have been deployed worldwide were not especially designed to meet the demand of verifiability. Votes may indeed be stored such that they cannot be traced back to the voter, guaranteeing secrecy of the ballot, but at the same time it is not always possible to judge afterwards if a vote was cast by an eligible voter, or produced by software malfunction or malicious activities. Because they are generally newer and operate over an insecure

* Published in: Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures. Springer LNCS 5705, p. 121-144, 2009

infrastructure, it may be expected that Internet voting systems involve more efforts to meet verifiability requirements. Whether or not these efforts suffice is a topic of scientific and political debate. As often happens, computerisation of existing procedures leads to a critical reflection on these procedures. This is what we have witnessed over the last decade for voting. The discussion is particularly interesting for voting because of the combination of non-trivial scientific challenges and high societal relevance and interest.

In this paper, we focus on the practical issues involved in electronic voting, both in the context of voting machines at polling stations and in the context of Internet voting. We focus on the situation in the Netherlands because a radical change of position took place there. For electronic voting machines, the Dutch were both early adopters and early abolishers. The machines were introduced on a large scale in the 1990s, and their use was discontinued in 2008 after a short and effective campaign by a pressure group. Meanwhile, experiments with Internet voting had taken place using two completely different systems. While following these developments in a loosely chronological order, many of the issues involved in e-voting will be discussed.

In section 2, we discuss the emergence of electronic voting in the Netherlands, as well as the requirements that are thought to apply to the election process. We also give an overview of techniques that are available to increase the security of electronic voting. In section 3, we describe the controversy that was started by an activist group in 2006. We discuss the issues that were brought up and attempted solutions. In section 4, we describe the Internet voting experiments in the Netherlands. In section 5, we analyse the controversy on electronic voting in terms of trust.

2 Requirements and techniques

2.1 History of Dutch elections

The Netherlands are a constitutional monarchy, and have a system of proportional representation for local and national elections. Universal suffrage is in place since 1917 (male) and 1919 (female).

There is no registration procedure. Eligible people received a polling card by mail a couple of weeks before the elections, based on (local) citizen registrations. This polling card was handed in at the polling station. One could be asked to present identification, but the general feeling is that this hardly ever happened. Each polling station had a list of local residents who where expected to vote at that station. The residents names were marked on a list after handing in the polling card (and proceeding to cast a vote), in order to prevent multiple votes by one individual. When voting was limited to the local polling station, one could also vote with a passport instead of a polling card. Now that experiments are being run with voting in any polling station within the municipality, this is not possible anymore, because there is no central voter register for keeping track of who already voted. This has led to some complaints in recent elections by people who lost or forgot their polling cards.

Particularly noteworthy is the liberal policy in the Netherlands for voting by proxy. Since 1928, the option of "stemmen bij volmacht" (voting by proxy) exists: one can authorise other people to cast one's vote. It is meant to be used in case of illness or absence, but this option is not really appreciated elsewhere (see the critical remarks in [27], especially in relation to secrecy of the vote). The possibilities for authorisation have been restricted over time, because, especially in local elections, there had been cases of active vote gathering. By now, each individual is only allowed to have two authorisations. It is not necessary to register a proxy vote; one simply signs the polling card and hands it to the designated proxy.

Since 1983, Dutch citizens living abroad, or having job duties abroad during the elections, are allowed to vote by postal ballot. The postal ballot needs to be accompanied by a signed statement and sent to the election office in The Hague or a special office in the country of residence. Postal voting is not allowed within the country.[3]

The Netherlands were quick to introduce electronic voting. In 1965, a legal provision was put in place to allow the use of machines, including electronic ones, in voting. In the late 1980s, attempts were made to automatise the counting, and the first electronic voting machines appeared. From 1994, the government actively promoted the use of electronic voting machines in elections. Local governments were enthusiastic, mainly about the modern character and administrative efficiency and advantages of these machines: easy, push-button voting, reduction of the number of polling stations, fast delivery of results. Since then, voting machines have been used extensively during elections. Little attention was paid at the time to security and verification possibilities. The main concerns were related to the usability of the machines, especially for elderly people. How the votes were counted and how the result was calculated did not seem to be of much public interest. The introduction of these machines was uncontroversial.

In 1997, regulation on voting machines was established, including an extensive list of requirements that voting machines had to meet ("Regeling voorwaarden en goedkeuring stemmachines"). Demands on the verifiability of the counting, however, largely remained unspecified. Moreover, criteria for software that calculates the results from the totals of the individual machines had not been assessed at all. In 1999, local authorities were even reported to have used self-written software for this purpose [10].

Voting machines in the Netherlands had to be approved by an evaluation institute. Although multiple institutes could be designated in principle, only TNO has been involved in this procedure thus far. Only TNO (the department doing the evaluation now being called BrightSight) was given the source code of the software running on the machines, and the evaluation reports were not public either.

The full requirements specification, consisting of 14 sections, was found as an appendix to the regulation. We quote and translate the items from section

[3] Source: www.parlement.com, an excellent site on Dutch politics (in Dutch only, alas)

8: Reliability and security of the voting machine. The "normal environmental conditions" referred to are specified elsewhere in the requirements.

1. The vote stored in the vote memory of the voting machine is the vote cast and confirmed by the voter;
2. A cast vote cannot be lost due to breakdown of the energy supply, failure of one component, "normal" environmental conditions (as specified), normal use, or mistakes in the operation of the voting machine;
3. The read-in lists of candidates are maintained completely in case of breakdown of the energy supply, normal environmental conditions, normal use, or mistakes in the operation of the voting machine;
4. The functions of the voting machine are maintained completely in case of breakdown of the energy supply, normal environmental conditions, normal use, or mistakes in the operation of the voting machine;
5. The storage of the cast votes is made redundant. The vote is stored in such a redundant way in the vote memory, that it can be proved that the failure rate is 10^{-6}. If there is a discrepancy in the redundant storage, the machine will report this to the voter and the voting station;
6. The voting machine is able to avoid or reduce the possibilities for accidental or intended incorrect use as much as is technically feasible in fairness;
7. The way of vote storage does not enable possibilities to derive the choice of individual voters;
8. The voting machine has features which help to avoid erroneous actions during repair, maintenance and checks, for example by mechanical features which preclude assembly in wrong positions or in wrong places;
9. The voting machine may have functions which are not described in the Election Law, the Election Decree, or this appendix, as long as they do not impair the required functionality of the voting machine and are related to the voting procedure.

Note that the possibility of recount or other forms of verification are not mentioned at all. Furthermore, most of the requirements above concern correctness under normal circumstances, and not protection against possible election fraud.

2.2 Nedap voting machines/computers

The most widely used voting machines were produced by the Dutch company Nedap, see Figure 1. These were so-called full-face direct recording electronic voting machines (DRE) with a button for each candidate. Such a Nedap machine contains a Motorola 68000 processor from the 1980s, together with EPROM (2×128KB for the software binary), EEPROM (8KB) and RAM (8KB) memory [13]. It has two simple screens, one for the voter, and one on the election officials' console for enabling the machine. The votes are stored in memory in a redundant manner, in arbitrary order. The system software determining the behaviour of these machines can easily be changed, simply by plugging in different EPROM chips. In this way one can make the machine store votes for one party

as votes for another party. One can build this software in such a way that it is practically impossible to detect, see [13] for details.

The verification possibility that these Nedap machines offered is the comparison of the votes per candidate to the votes per party, and to the total number of votes cast. This check, however, is based on votes that have already been processed by the machine. There was no paper trail.

It is interesting to note that this voting equipment has been referred to as a voting *machine*, since its introduction. The word "machine" suggests a single, unchangeable functionality. One of the important points raised by the pressure group against e-voting (see subsection 3.1) is that they should not be called "voting machines" but "voting computers": there is no single unchangeable functionality, because they are proper computers that can be made to do anything. To illustrate this point it was shown [13] that they could be adapted to play chess, or to count fraudulently. Since then it has become almost an ideological issue whether to speak of "voting machines" or of "voting computers" in the Netherlands. Even though we agree that the most appropriate word is "computer", we shall stick to the more common, historical way of referring to them as "machines".

More recently, touch-screen based systems marketed by the former state press Sdu were also used, notably in Amsterdam, see Figure 1.

Fig. 1. Voting machines from Nedap (left & middle) and Sdu (right)

2.3 Requirements

In 2007, an official Election Process Advisory Commission was formed, see subsection 3.2 below. It formulated the following requirements for elections, which we quote together with their explanation.

- **Transparency**
  The election process should be organised in such a way that the structure and organisation is clear, so that everyone in principle can

understand it. There must be no secrets in the election process: questions must be able to be answered, and the answers must be verifiable.

- **Verifiability**
  The election process should be objectively verifiable. The verification tools may differ, depending on the method of voting that is decided upon.
- **Fairness**
  The election process should operate in a proper manner, and the results must not be capable of being influenced other than by the casting of lawful votes.
- **Eligibility to vote**
  Only persons eligible to vote must be allowed to take part in the election.
- **Free suffrage**
  Every elector must be able to choose how to vote in complete freedom, free from influence.
- **Secret suffrage**
  It must be impossible to connect the identity of a person casting a vote to the vote cast. The process should be organised in such a way that it is impossible to make a voter indicate how he or she voted.
- **Equal suffrage**
  Each voter, given the Dutch election system, must be allowed to cast only one vote in each election, which must be counted precisely once.
- **Accessibility**
  Voters should be enabled as far as possible to participate directly in the election process. If this is impossible, there must be a way of taking part indirectly, i.e. by proxy.

It is widely acknowledged that not all requirements can be guaranteed absolutely, certainly not in combination with each other. For example, paper voting in polling stations is usually judged to provide high guarantees with respect to most of the requirements, but scores quite low on accessibility. Similarly, there are tensions between secrecy on the one hand and authentication and verifiability on the other.

2.4 Techniques

Several techniques are available to realise these requirements (to a certain degree) in electronic voting systems. Some of those have only been the subject of academic analysis, others have been used in real elections. In advanced systems from academia, a distinction can be made (see *e.g.* [16, 36]) between protocols based on mix-nets, protocols based on blind signatures and protocols based on homomorphic encryption. These systems have rarely been used in elections though. More practically oriented systems have been based on public key infrastructures, randomised ballots, and hashes. If we do not focus on the electronic possibilities

for securing information only, visual cryptography, voter verified paper audit trails and trusted parties can help in achieving security goals.

In order to give an impression of the field, each of these techniques will be described briefly in this subsection. We start with an explanation of the general use of cryptography in voting. For more information we refer to [36] and the references therein.

Cryptography Key to all secure electronic voting systems is the use of *cryptography*, often abbreviated to "crypto": technology developed in order to protect information by manipulating the information itself. Cryptography can be used to protect the *confidentiality* or *integrity and/or authenticity* of information. The former is realised by *encryption*, the latter by *signing*.

Encryption means scrambling data according to a certain procedure, such that they become unrecognisable. Typically, a (cryptographic) *key* is a parameter in a fixed scrambling method, such as DES or AES. The key is usually just a very big number. A key is also needed for decryption, the recovery of the original data. This key may be the same as or different from the encryption key. The science of designing and analysing encryption schemes is called *cryptology*.

If the same key is used for both encryption and decryption, one speaks about *symmetric* or *secret key* crypto. If different keys are required for encryption and decryption, one calls this *asymmetric* or *public key* crypto. The main advantage of public key crypto is that the problem of establishing a shared key before the transaction is reduced. Instead of having to define a shared secret key for each pair of users, a *certificate* ascribes a *public key* to a person or organisation. This public key can be used to send secret messages to that agent, which only the agent itself can decrypt using its *private key*.

The other way around, the agent can use its *private key* to *sign* messages. The signature can be checked by anyone in order to verify the integrity of the data, using the *public key* in the certificate. The certificate, in its turn, is signed by a higher authority to ensure its authenticity.

Secret-key crypto is generally much faster than public-key crypto. Security-enhanced websites typically use public-key crypto for authentication, based on the site's certificate, during which a *session key* is established. The session key is used in a secret-key scheme for the remainder of the transaction.

It is important to realise that most of these techniques provide *computational* security as opposed to *unconditional* security. This means that security is based on mathematical problems that are *hard* to solve, but not impossible. If one manages to solve the mathematical problem, one can break the confidentiality or integrity of the messages sent. It will take more than a reasonable amount of time to solve them with current computers. If computers get faster, we may start using longer keys to keep new data secure. However, if someone for some reason stored data encrypted using the *old, short* numbers, these may then be easily recovered. So-called 'forward security' is important in voting: even after a very long time it should not be possible to reveal encrypted votes, for instance by brute-force trying.

Future developments, like in quantum computing, may pose more fundamental challenges to these assumptions. If we manage to build real quantum computers, the mathematically hard problems may not be hard for these new machines at all, for instance via Shor's algorithm for integer factorisation. However, new techniques are being developed that use quantum primitives to provide so-called "unconditional" security, which is not dependent on limits of computational power. If these developments are successful, they may have major consequences for e-voting systems (and many other systems as well).

PKI PKI stands for *Public Key Infrastructure*. Voting systems based on PKI, such as the Estonian system [22], typically use the system of public keys and certificates also applied to for example e-commerce websites. In the Estonian system, the voter encrypts the vote with the election's public key and then signs it with her own private key to prove authenticity. Such systems require each voter to have a certificate and a private key. The private key must be available to the voter in a way that is both secure and easy to use. In the Estonian case, the private key is embedded in a smartcard. Then, voters will need a smartcard plus an installed smartcard reader to be able to vote on their own computer. Due to the limited availability of smartcard readers among voters, PKI-based systems are currently not the best in terms of accessibility.

Blind signatures Normally, one signs a message that one knows the contents of. It would be possible to put a signature on a message on carbon paper within a sealed envelope. In this way, I could decide to sign *exactly one* message for each of my friends, after identifying them.

The electronic equivalent of this procedure is called a *blind signature* (see *e.g.* [4]). Blind signatures are useful if we wish to allow voters to choose their own election credentials, *e.g.* a key used to encrypt their vote. They can do this without having to reveal this information to the authorities, through the blinding procedure. They "blind" the information, have it signed, and "unblind" it again. By means of this method, a combination can be achieved of authenticity and anonymity of the vote. Still, the communication channel will need protection, since it is otherwise easy to see from which computer a vote originates.

Mix-nets When using a ballot box, votes come out in an order different from the order in which they went in. This ensures anonymity of the voters. How to do this electronically? In mix-nets (see *e.g.* [34, 1]), encrypted messages are passed on between different authorities, making sure that no-one can derive a relation between the messages going in and the messages coming out. Basically, this is done by having each authority change the order of the votes. The authorities have to prove that the *content* of the messages is still the same after they shuffled them. After the last step, the votes are decrypted. This technique can be used in voting, to make sure that no-one can gain any information from the *order* of the votes, unless *all* of the authorities cooperate. In this way, it is made sure that votes are kept anonymous.

Homomorphic encryption Another way to ensure anonymity is to count the votes *while encrypted*. In this way, one calculates a result from the individual votes without revealing the contents of each individual vote. This is exactly what homomorphic encryption achieves (see *e.g.* [7, 8, 16]). For example, we may *multiply* all the encrypted votes to ensure that if we decrypt the result, this represents the *addition* of the original votes.

Visual cryptography and randomised ballots Many systems employ a "take-one-destroy-one" principle to ensure security properties. In such a scheme, the vote consists of two parts, which are kept separated, and which do not reveal the vote individually. One example is the visual crypto scheme by [5]. Here, two visual patterns can be combined to a pattern revealing the vote. Prêt-à-Voter by [6] has a similar setup. Here, the voter takes a receipt, but the order of the candidates on the ballot will be destroyed. The order is different on each ballot. The particular order belonging to a ballot can only be recovered through processing by a mix-net, such that each individual vote is kept secret, by separating the vote and the order of the candidates on the ballot. Usability may be a weak factor in these schemes, since voters will have to perform more complicated tasks. Also, voters are prevented from "preparing" their vote at home by finding the name of the candidate on a pre-published candidate list. On the other hand, putting the candidates in different order on each ballot may improve the fairness of the election, because it avoids a possible bias of the voters towards the first-listed candidates [6].

One of the threats to online voting is the possibility of a virus on the voter's computer altering the vote. Randomised ballots may also help to prevent such attacks. Each candidate is then represented by a number, but these numbers are different on each ballot. If the ballot is sent to the voter via traditional mail, and the voter only has to enter a number on a website, it is nearly impossible for the virus to change the voter's choice into one for the party of the virus's choice. This technique was used in the Dutch KOA online voting experiments of 2004 (see Section 4).

Commitments Some voting systems allow anyone to calculate the result. This can be done by providing before the election a table which can be used to count each possible individual vote. Of course, one cannot put the possible votes themselves in this table, because that would allow people to copy them and send them in as fake votes. However, there are ways to identify some piece of information uniquely (at least with very high probability), without revealing the information itself. Such arrangements are called *commitments*. What can be put in the table instead is for instance a *fingerprint*, a *hash* of each vote.

A hash is a cryptographic operation that assigns to a possibly long document a relatively small sequence of bits. The operation should satisfy the following properties:

- a hash can be efficiently computed from a document;

– it is practically impossible to reconstruct the document from the hash;
– it is practically impossible to find two documents with the same hash.

These properties prevent the reconstruction of valid votes from the table, but when a vote is received it can easily be looked up and counted.

Trusted parties Not all security is technical. It is doubtful whether a technically perfect system can be built, and if so, whether it would be practical. Often, the security of the whole system is based on procedural as well as technical measures. The procedural measures should include a separation and division of responsibilities. In this way, the voter will not have to have full faith in one organisation, but she can be confident that problems can only occur if *all* of the involved organisations cooperate maliciously. The RIES system (section 4) suffers from limited separation of tasks [17].

Still, even in standard public key crypto, we need trusted organisations to sign the certificates that ascribe a public key to a person. Also, in some communication protocols it is assumed that one of the participants is fair. This participant is usually called a trusted third party (TTP). How much trust we should really place in such parties when it comes to voting is a legitimate question.

Voter verified paper audit trails A solution to improve the security of electronic voting that has become very popular in the US is the Voter Verified Paper Audit Trail (VVPAT), as proposed by Rebecca Mercuri [23]. This basically means that a voting machine not only stores the vote electronically but also produces a separate print of each vote, which can be used in case a recount is demanded. The print is verified by the voter and then deposited in a ballot box. More than half of the states in the US have now passed legislation making a paper trail mandatory.

Some people argue that a VVPAT does not help much in improving security, because people will have a hard time checking their vote, due to the large number of races on which they have to vote in a single election in the US. It has been suggested to use an audio trail instead [37]. Also, an important question is what to do if in the end the electronic trail and the paper trail differ. Which one has to be preferred? If this question is not properly addressed in advance, VVPAT does not make much sense.

None of these security measures were implemented in the electronic voting machines used in the Netherlands. In the end, this led to major criticism, as we will see in the next section. The Internet voting experiments, which we will address in section 4, did use some.

3 Controversy

3.1 "We don't trust voting computers"

There have been some isolated incidents and accusations during the history of electronic voting in the Netherlands before 2006. In 1998, it was found that the

machines led to a competitive advantage for the numbers 31 of the candidate lists of the parties. Due to space restrictions, these were placed at the top of a second column, next to the candidates heading the lists. Also in 1998, Hans Janmaat, a right-wing maverick, accused the voting machines of deliberately reducing his number of seats.

Criticism of the obscurity of the election procedure when using voting machines has risen after 2000. Main reasons were the secrecy of the source code and the evaluation reports, and the lack of verifiability. Attempts to retrieve the source code of the machines via the Freedom of Information Act failed, because the source code is intellectual property of the producer. But after Ireland judged the Nedap machines they bought unfit for use in the elections,[4] Dutch citizens and politicians started asking questions about the safety and verifiability of such machines. At first, the government responded that everything was OK and not much happened.

In Fall 2006, a chain of events completely changed the e-voting battleground in the Netherlands. A pressure group called "Wij vertrouwen stemcomputers niet" ("We don't trust voting computers") was founded around June by Rop Gonggrijp, who was soon joined by Maurice Wessling. Gonggrijp managed to get hold of a couple of Nedap voting machines, took them apart and reverse-engineered the source code [13]. The results of the analysis were made public in a national television programme on October 4, with the general elections scheduled for November 22 [13]. The first main problem that was illustrated was the easy replacement of the program chips, allowing the attacker to have the machine count incorrectly, or execute any other desired task. Due to the lack of verifiability features, such attacks could go unnoticed: the machine would be able to perform according to its own will. The second main problem shown was the possibility to eavesdrop on the voting machine via a tempest[5] attack. Tempest involves listening to so-called "compromising emanations", *i.e.* radio emission from the device, in this particular case the display. Also, problems were found with the (physical) security of the storage facilities where the machines are kept in between elections.

The tempest attack was particularly successful because there is a special (diacritical) character in the full name of one of the parties. This required the display to switch to a different mode with a different refresh frequency, which could easily be detected.[6] The responsible minister responded to the findings of the activists by having all the EPROM chips containing the software binaries replaced with non-reprogrammable ones (a questionable solution, but the public bought it), seals on all the machines, and having the intelligence agency look into the tempest problem. Tempest expertise is scarce, but typically exists in those circles.

---

[4] `http://www.cev.ie/htm/report/first_report.htm`, consulted May 28, 2009.

[5] Also written TEMPEST, supposedly being an acronym for Telecommunications Electronics Material Protected from Emanating Spurious Transmission or something similar. For more information, see Chapter 15 of [3].

[6] See the video at `http://www.youtube.com/watch?v=B05wPomCjEY`.

The fix for the diacritical character problem was easy (don't use special characters). With that implemented, the signal emitted from the Nedaps was fairly limited. However, the intelligence agency also looked into the other type of voting machine, the touch-screen based system produced by the former state press Sdu. They found that the tempest issue was much worse there, and someone outside the polling station might be able to reconstruct the whole screen from the signal.

The technical requirements only stated that voting machines should maintain the secrecy of the vote *in storing the vote*, not in casting (see page 4). Nonetheless, the minister suspended the certification for the Sdu machines three weeks before the elections, because the Election Law requires that machines are certified only if the secrecy of the ballot is guaranteed. In the background legal threats from the pressure group played a mayor role. The suspension affected about 10% of the voter population, including Amsterdam. Some districts got spare Nedaps, but others had to use paper ballots, especially because the certification of one of the older Nedap types was suspended later.

There was some discussion about whether eavesdropping on election day was such a realistic scenario that it would justify the suspension. In any case, the pressure group was very happy to have a major event that backed their concerns, even though the focus had shifted from verifiability to secrecy. And the minister was happy to have created an image of a decisive government.

In the beginning of 2007, there was an attempt to re-certify the Sdu machines for the elections for the provinces. However, machines with reduced radio-emission turned out to be unreadable for the colourblind, and Sdu had apparently made mistakes in the machines delivered to the testing agency. In the end, the minister extended the suspension. Sdu demanded a new test in a court case, but the machines failed the test again.

The Ministry of the Interior and Kingdom Relations explained their point of view on the controversy on their website. They stated that apart from the secrecy problem due to the tempest attacks, the security of the machines is acceptable. They argued that in the Dutch proportional system, as opposed to the Anglo-Saxon district-based system, small numbers of votes will not have any major influence on the result. Besides, existing guarantees were thought to be sufficient in order to prevent fraud.[7]

3.2 Two committees

Another concession of the minister was the initiation of two commissions of independent experts, who would look into, respectively, the past and future of e-voting. The former was the Commission Decision Process Voting Machines[8], the second the Election Process Advisory Commission[9].

[7] `http://www.minbzk.nl/onderwerpen/grondwet_en/verkiezingen_en/stemmachines`, consulted February 13, 2007, not online anymore.

[8] Members: drs. L.M.L.H.A. Hermans and prof. dr. M.J.W. van Twist.

[9] Members: mr. F. Korthals Altes (chairman), prof. mr. J.M. Barendrecht, prof. dr. B.P.F. Jacobs, C. Meesters and M.J.C. van der Wel MBA.

In March 2007, the Organization for Security and Co-operation in Europe (OSCE) reported on the Dutch elections [27]. On April 16, the Commission Decision Process Voting Machines published its report [15]. Both reports argued for increased verifiability, by means of a paper trail or equivalent procedure. It was not made clear what kind of (technical) procedures, discussed in the previous section, would count as equivalent.

The report of the Commission Decision Process Voting Machines was quite critical about the role of the government in the electronic voting problems. There was too little expertise with the government, and it was too dependent on external parties for the running of elections. The role of TNO as both designer and tester of the machines was questioned. The legal requirements came too late, contained too little security, and did not address the counting software. Also, the government had ignored earlier signals of concern. The government humbly accepted the conclusions, and moved the election process to a more technology-oriented department. There was also an attempt to redraft the requirements.

On September 27, the Election Process Advisory Commission reported on the future of the electoral process in the Netherlands [2]. The report stated that the primary form of voting should be voting in a polling station. Internet voting for the whole population would not be able to guarantee transparency, secrecy and freedom of the vote sufficiently—for the foreseeable future. It was advised to equip polling stations with "ballot printers" and "vote counters" instead of electronic voting machines, providing a paper vote in between the two stages. Ballot printers would only print the voter's choice, which would then be verified by the voter and put in a ballot box. After the close of the polls, the vote counter would scan the votes and calculate the totals.

The American solution of a paper trail was not advised. It was argued that registering the vote twice, electronically and on paper, could lead to different outcomes, depending on which registration would have priority in case of a dispute. Significantly, systems without a paper copy of the vote were not considered as alternatives, for reasons of transparency.

On October 21, 2007, the existing regulation allowing voting machines was withdrawn. A technical expert group was formed to investigate the practical issues involved in the commission's proposal for the new method of voting.

After further research into the tempest issue [20], the option of a ballot printer was judged not to be feasible. A tempest-protected prototype vote printer was built (see Figure 2), with a thick metal shield, but turned out to be too heavy for practical use (almost 100kg). Most importantly, however, the procedures for testing thousands of machines individually for tempest compliance were thought to be way too complicated. Additional measures that are used for tempest protection, like forbidding mobile phones and restricting access to *e.g.* adjacent rooms, turned out to be incompatible with the open nature of elections: you don't want to run them as a high-security military style operation.

Machine counting of manually cast paper votes was not seriously considered: the huge ballots used in the Netherlands are impossible to feed automatically into a machine. Besides, problems in the United Kingdom with this type of e-

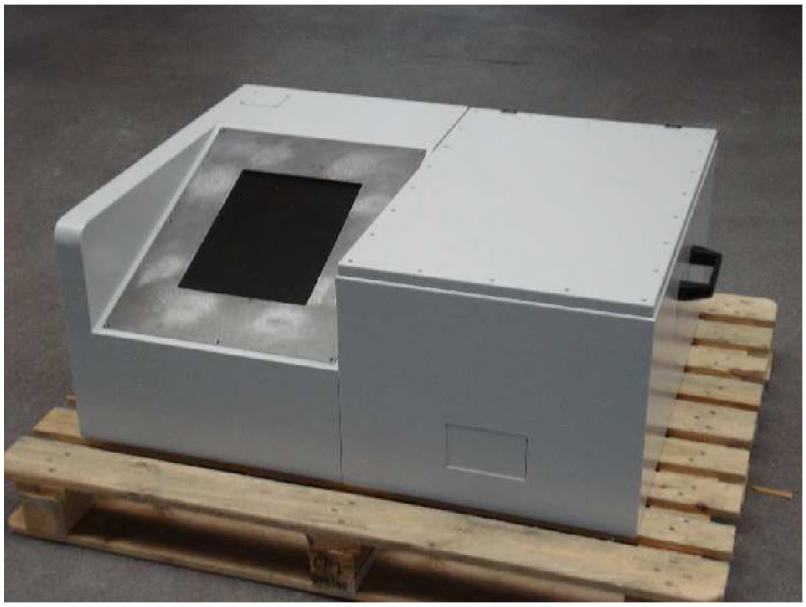

Fig. 2. A prototype tempest-shielded voteprinter, with touch screen and protected tray for the printed vote.

counting were a reason for the Election Process Advisory Commission not to recommend this option.

On May 16, 2008, the government decided that voting would be on paper for the near future. An experiment with machines similar to the Nedaps for counting by the poll workers only was still proposed. They would then enter the paper votes manually into the machine. Because of the separation between the voter and the entering of the vote in the machine, this would resolve the tempest issue. However, parliament could not be convinced that this would reduce the other security problems involved in electronic voting, and rejected the option.

Thus, in the summer of 2008, the discussion was closed and the Netherlands returned to paper voting, with manual counting of the ballots. Inevitably this will lead to delays in partial results and prognoses on election night—and possibly to a restart of the discussion.

Looking back one must acknowledge that the pressure group has been incredibly effective and has reached its goals in a remarkably short time. It relied on a clear vision, technical skills, bravery, effective use of freedom of information rights, professional communication via their own newsletter and a very informative webpage, frequent and convincing media appearances, and, in the end, threats of legal actions. No politician (or civil servant) likes to have such an adversary.

3.3 The German constitutional court

Nedap voting machines were also used in parts of Germany and France. The German Constitutional Court (*Bundesverfassungsgericht*) was asked for a verdict by the Chaos Computer Club (CCC)[10]. On March 3, 2009, the Court ruled that the use of these machines in elections in Germany was unconstitutional because of lack of transparency and verifiability by ordinary citizens. This verdict came too late to have any impact in the Netherlands, but it was received as a confirmation of the decision to abolish voting machines earlier on.

4 Internet voting

In the Netherlands, several experiments have been performed with voting via the Internet. During the European elections 2004, Dutch citizens living abroad could vote online for the first time. Moreover, elections for two water boards have combined postal ballots with Internet voting in fall 2004, with a total of 120,000 actual online voters. Hence these elections were among the larger ones, worldwide.

Kiezen op Afstand (KOA) The first of the two experiments in the Netherlands was initiated by the Ministry of the Interior and Kingdom Relations. The experiment took place during the European elections in 2004. Participation was intended for expatriates, who only had the option to vote by mail before. This possibility is typically used by 20,000 - 30,000 people, of the about 600,000 potential expat participants. They were given the opportunity to vote via Internet or phone. For this purpose, the KOA system was developed in 2003–2004,[11] and a law regulating the experiment was passed through parliament.

The main setup of the system is as follows [11]. Voters register by ordinary mail, and choose their own access code as password. In return they receive a vote code as "login", together with a list of candidates, each with her own candidate code. There were 1000 different lists in the experiment. Combining login and candidate code, one could then cast a vote.

The system was designed by Logica CMG. However, the government demanded the transfer of the intellectual property rights of the source code with the system. This made it possible to publish the source code after the elections. The source code zip file, published on the website www.ososs.nl, contained all Java code written specifically for the online voting system. Code that was part of general Logica CMG technology was not open source. This meant that it was only possible to inspect the (partial) source, not to compile and run it. A fully open-source version of the system has been developed later by Joe Kiniry and colleagues from Trinity College Dublin [19].

[10] There was mutual inspiration, communication and exchange between the German and Dutch campaigns.

[11] [24], see also `http://www.minbzk.nl/persoonsgegeven_en/kiezen_op_afstand`, consulted October 11, 2005, not online anymore.

A follow-up trial was conducted in the national elections in 2006. However, the system used was different.

Rijnland Internet Election System A somewhat more sophisticated system, called RIES, was developed with far less money by the water board of Rijnland[12] together with two companies cooperating under the name TTPI[13], based on earlier work by Robers [33]. A water board (Dutch: hoogheemraadschap or waterschap) is a regional government body for water management. Because the water boards are not bound by the Dutch election law, they are relatively free in their means of voting. Its officials are usually elected via ordinary mail, but voter participation for these elections is typically fairly low. An experiment with election via the Internet has been conducted in the regions Rijnland and Dommel in 2004, with 1 million eligible voters. 120,000 people voted online, but turnout did not increase, against expectation and hope. RIES was also used in the second KOA remote voting experiment during the national elections in 2006, instead of the KOA system from 2004.

The RIES system uses cryptographic operations to protect votes and at the same time offer good transparency, at least in principle. It is possible for voters to verify their vote after the elections, and for independent institutions to do a full recount of the results. The Radboud University Nijmegen did such a recount for all elections in which the system was used, and confirmed the official results [17].

The RIES system uses hashes to publish a pre-election table, see [17, 18]. Once the votes have been published, anyone can calculate the result of the election from the pre-election table and the table of received votes. Because of the use of hash functions, the system is relatively simple, offers protection of votes and allows scrutiny of the results. Whereas the hashes of all possible votes are public, it is (or should be) computationally infeasible to deduce valid votes from them without the required voter key.

The system works as follows. First of all, a reference table (see figure 3) is published before the elections, including (anonymously) for each voter the hashes of all possible votes, linking those to the candidates. The original votes are only derivable from a secret key handed to the voter. The confidentiality of these keys is achieved via organisational security measures, in the same way that identification codes for bank cards are handed out. It is possible to compare the number of voters in this table with the number of registered voters.

In the voting phase, voters use their secret to derive a valid vote for their desired candidate. This vote is then submitted to the server via an encrypted connection.

After the elections a document with all received votes is published. This allows for two important verifications: a voter can verify his/her own vote, in-

[12] `http://www.rijnland.net` and `http://www.rijnlandkiest.nl`, consulted May 28, 2009.

[13] `http://www.ttpi.nl`, consulted May 28, 2009.

cluding the correspondence to the chosen candidate, and anyone can do an independent calculation of the result of the elections, based on this document and the reference table published before the elections. If your vote has been registered wrongly, or not at all, you can detect it. And if the result is incorrect given the received votes, you can detect it as well.[14]

```
Archive:  01010204.zip
  Length      Date    Time    Name
 --------  ----------  -----  ----
     2172  08-25-04 09:32   01010204/RT_0.zip
     4017  08-25-04 09:32   01010204/RT_1.zip
     2173  08-25-04 09:32   01010204/RT_2.zip
     1865  08-25-04 09:32   01010204/RT_3.zip
     2789  08-25-04 09:32   01010204/RT_4.zip
     3097  08-25-04 09:32   01010204/RT_5.zip
     2787  08-25-04 09:32   01010204/RT_6.zip
     1559  08-25-04 09:32   01010204/RT_7.zip
     1559  08-25-04 09:32   01010204/RT_8.zip
     2480  08-25-04 09:32   01010204/RT_9.zip
     2784  08-25-04 09:32   01010204/RT_A.zip
     3405  08-25-04 09:32   01010204/RT_B.zip
     2785  08-25-04 09:32   01010204/RT_C.zip
     1867  08-25-04 09:32   01010204/RT_D.zip
     1559  08-25-04 09:32   01010204/RT_E.zip
     3403  08-25-04 09:32   01010204/RT_F.zip
        0  08-25-04 08:51   01010204/
 --------                   -------
    40301                   17 files

Archive:  RT_0.zip
  Length      Date    Time    Name
 --------  ----------  -----  ----
      220  08-25-04 09:31   008AB1E98AEDFBA450A1813DDC153553
      220  08-25-04 09:31   08677B73378E1D59153DE30263A3C47C
      220  08-25-04 09:31   06CAC042AF7D6940DD8A51814E68DFF8
      220  08-25-04 09:31   00FEA51461FBF7B406554EEF2E23554D
      220  08-25-04 09:31   05C02BD8E3863DB24D6C332A17B78EFB
      220  08-25-04 09:32   070C60BFFC06B7355425E6FFADBBED30
      220  08-25-04 09:32   034C37BA687E21477D38A110954207B8
 --------                   -------
     1540                   7 files

008AB1E98AEDFBA450A1813DDC153553:

vervangend=0
verstrekt=1
vervallen=0
AC94983743058334B25452E0F63A9C20=0101020401
B0015EAC8ECF766DB67825592DC10957=0101020402
ACE42133255CA8184D18E0293FEF7EE8=0101020403
358AAB0C934757ACCF071A1CD732EDEA=0101020499
```

Fig. 3. Reference table format. The reference table in the figure has been split into 16 parts, which reside in different archive files. Each archive file (*e.g.* `RT_0.zip`) contains files for different voters, indicated by the hash of the voter's identity. In these files, hashes of possible votes of such a voter are mapped to the corresponding candidates (*e.g.* candidate `0101020401`).

The fundamental problem in the RIES system lies in the responsibility of the key generator to destroy the keys immediately after sending them to the voters. Failing to do this may compromise both the secrecy and the authenticity of votes.

[14] Of course, procedures need to be put in place to decide what will happen in case of such a claim.

This allows the organisers, in principle, to vote on behalf of participants[15]. One may wish to improve on this issue by having the voters generate their keys themselves. Here, blind signatures may be useful: the voter can have exactly one key signed by the authorities, without making it public.

Another problem is that the verification procedure might be used to sell votes. If I let someone else verify my vote, he or she could pay me for making the right choice. If I would need a smartcard to verify a vote, this would already be less easy, but this would limit the accessibility and usability of the system.

The water boards intended to use RIES for their combined elections in Fall 2008. This was not a particularly lucky time for the attempt, as the deputy minister had just abolished the electronic voting machines in polling stations. Parliament demanded an independent evaluation, which was performed by the IT-security company Fox-IT. Internet voting for the water board elections was cancelled after this independent investigation reported additional security problems, such as brute force key search [14] and the possibility of SQL injection attacks [12]. Electronic counting of postal ballots for the water boards was continued, though.

As a result, Internet voting developments in the Netherlands have also come to a halt.

5 Trust in technology

Trust is a major, but confusing, issue in the discussion on electronic voting [29]. In the following, we briefly investigate the role it played in the controversy in the Netherlands.

Papers discussing trust in electronic voting often seem to be unsure about their definition of trust. In [9], in a section named "*Increasing* trust" [emphasis added], the following sentence is found: "One way to *decrease* the trust voters must place in voting machine software is to let voters physically verify that their intent is recorded correctly." [emphasis added] But was the intent not to *increase* trust? Do we wish to increase and decrease trust at the same time? What is happening here?

Apparently, computing scientists stem from a tradition in which minimising trust is the standard. "In computer security literature in general, the term is used to denote that something must be trusted [...]. That is, something trusted is something that the users are necessarily dependent on." [25] Because we *must* trust certain parts of the system for the whole system to be verifiably correct according to the computing science models, we want to minimise the size of the parts we have to trust, thus minimising trust itself. This desire to minimise is clearly visible in efforts to reduced the so-called Trusted Computing Base (TCB). However, from a psychological perspective, or even a marketing perspective, it is desirable that users trust the *whole* system. Maximising trust seems to lead

[15] Analogously, bank employees can, in principle, withdraw cash on behalf of clients because also possess PINs.

to more fluent interaction between the user and the system, and is therefore desirable.

To explain these two different types of trust, we consult the German sociologist Niklas Luhmann. Luhmann [21] draws a distinction between *trust* and *confidence*. Both confidence and trust involve the formation of expectations with respect to contingent future events. But there is a difference.

According to Luhmann, trust is always based on assessment of risks, and a decision whether or not to accept those. Confidence differs from trust in the sense that it does not presuppose a situation of risk. Confidence, instead, neglects the possibility of disappointment, not only because this case is rare, but also because there is not really a choice.[16] Examples of confidence that Luhmann gives are expectations about politicians trying to avoid war, and of cars not suddenly breaking down and hitting you. In these cases, you cannot decide for yourself whether or not to take the risk.

When there *is* a choice, trust takes over the function of confidence. Here, the risky situation is evaluated, and a decision is made about whether or not to take the risk: "If you do not consider alternatives [...] you are in a situation of confidence. If you choose one action in preference to others [...], you define the situation as one of trust." [21] If you choose to drive a car by evaluating the risks and accepting them, this is a form of trust. The essential feature of trust as opposed to confidence is the *comparison of alternatives*.

Computing scientists generally try to replace confidence with trust, *i.e.* exchange unconscious dependence on a system for explicit evaluation of the risks, and minimising the parts in which we still have to have confidence. Thus, they wish to minimise confidence and maximise trust (in the terminology of Luhmann). But they do not always state it this way. Philosophers (and social scientists), instead, recognise the positive aspects of confidence, and may evaluate positively people having a relation of assurance with the system without exactly knowing its risks (*i.e.* confidence). This is not meant as a conclusion that holds universally, but rather as an indication of the role of the scientific subcultures in the debates.

Electronic voting systems *may* be seen as alternatives to the existing system. Whether this is indeed the case depends on the situation. If the new technologies are not seen as an alternative, but as an improvement of existing procedures, electronic devices are more attractive, because they are more reliable and thus more easily acquire confidence. In the Netherlands, the pressure group created in their arguments a clear distinction between paper voting on the one hand and electronic voting on the other: they were said to be fundamentally different. If electronic voting is seen as a really different alternative to paper voting, which the pressure group encouraged, people suddenly get the option to decide on a

[16] Some native English speakers have noted that this distinction seems to be counter-intuitive. They would rather use the word "trust" for a situation which one has not analysed, and confidence for a more rational form of assurance. In order to avoid confusion in comparison with Luhmann's original text, I will still follow the terminology as introduced there.

voting system. This invites actively revealing the risks of the different systems, and basing the decision on an analysis of these risks. This means that trust now becomes the dominant form of assurance, as opposed to confidence. This has as a consequence that voting systems are required to be trustworthy rather than reliable only.

By making the distinction between paper voting and e-voting, the pressure group thus created a set of alternatives, requiring a decision, and changing the expectations from reliability to trustworthiness. For now, it seems that no existing voting technology can meet the high demands associated with a comparison with paper voting. Still, the Dutch government indicates that they will follow the technical developments, and most people involved seem to think that the discussion on electronic voting will re-emerge in the next decade. One interesting question is if socio-technical developments will have made it possible for electronic voting to acquire trust by then. This is especially interesting for Internet voting, since it changes some existing assumptions about the election process.

If it were possible for a technology like Internet voting to acquire trust, this is not merely a technical achievement. New information technologies, like mobile phones, do not merely solve a communication problem. They may profoundly change the experiences and behaviour of citizens [38], and we have indeed seen this in the mobile phone case. With Internet voting, the character of voting as a public ritual is abandoned. Instead, people vote in a private place, with no incentive to abandon their private interests and vote for the "greater good" [32, 26]. Even if it is generally not considered acceptable now, future developments may make it possible to link the voting site directly to the sites of political parties, voting advice websites, or discussion fora. It may even become possible to follow the advice of a private organisation and cast this vote directly from their website. This fundamentally changes the place of voting in the democratic process. Also, the fact that the government no longer takes responsibility for the secrecy of the vote may change the importance of the secret ballot. People may vote with their families or friends, and new ways have to be found to prevent undesirable social influence. What, then, is autonomy in voting really? Or in general?

Also, the idea of multi-channel elections, where people can choose the communication medium that most suits them, changes the way we think about equal access in elections. If there is a single channel, like a polling station, some people may live closer than others, but it is generally accepted that this does not constitute an unfair advantage. If people with Internet access can vote from home while others cannot, the acceptability of this inequality is not so trivial. Moreover, the whole system will then be as secure as the least secure channel. Even if fair voters choose the most secure one, unfair voters may take advantage of weaknesses in other channels.

If and when the discussion on electronic voting gets back on the agenda, these issues should be subject to public debate. Otherwise, we may end up in the same situation as with the Dutch voting machines: we did have confidence,

but in the end, we had to acknowledge that we failed to address all the issues involved, so that the technology did not deserve our trust.

6 Conclusions

The Netherlands were both an early adopter and an early abolisher of electronic voting. When electronic voting machines were introduced, verifiability was not an issue, and the machines did not include advanced means for verification of votes or results. Questions about the machines were put on the political agenda by a pressure group from 2006. This group also pointed to tempest problems, next to security issues with the integrity of the machines. An alternative voting method was devised by the Election Process Advisory Commission, which consisted of a ballot printer and a vote counter, where only a paper printout of the vote would form the connection between the two stages. However, because of the tempest issue, designing and testing a sufficiently protected ballot printer was judged to be infeasible in any practical election process. Practical issues thus were a major feature in the Dutch electronic voting history.

The experiments with Internet voting showed that fundamental design issues as well as practical details can contribute to the success or failure of Internet voting experiments. The environment may be crucial as well; the demise of the voting machines was not a particularly encouraging event for risking the large-scale elections the water boards had planned.

The success of the pressure group in the Netherlands can be explained in terms of confidence and trust. Whereas the Dutch machines were reliable enough to have confidence, they were not trustworthy enough to survive a critical comparison to the alternative of paper voting.

The big questions, although partially addressed in the Dutch debate, still remain largely unanswered:

1. What are essential requirements in e-voting, and what do they mean?
2. What are the threats?
3. Which techniques should be used to counter them?

Epilogue about the authors and their involvement

Given the broad descriptive character of this article it is appropriate to make the authors' roles and involvement explicit. The second author (WP) has done his PhD work [31] from 2003 to 2007 within the computer security research group at the Radboud University of Nijmegen, where the first author (BJ) holds a professorship. The group has been involved in several evaluation activities with respect to e-voting (KOA, RIES), often together with colleague Engelbert Hubbers, and sometimes on a commercial basis. This resulted in several publications, such as [17, 30, 18]. Also, the group played a public role in some of the societal discussions around voting in the Netherlands.

The first author was a member of the Commission Decision Process Voting Machines, and was chair of the subsequent more technical commission that studied the tempest issue (see section 3). The second author worked for the Ministry of the Interior from September 2007 until July 2008, on electronic voting and travel documents. Currently he is researching information security at the University of Twente. This text is not based on any non-public information obtained from the authors' work in these commissions or at the Ministry.

References

1. M. Abe. Universally verifiable mix-net with verification work independent of the number of mix-servers. In K. Nyberg, editor, *EUROCRYPT 98*, number 1403 in Lect. Notes Comp. Sci., pages 437–447. Springer, 1998.
2. Adviesommissie Inrichting Verkiezingsproces. Stemmen met vertrouwen, September 2007. Available online: `http://www.minbzk.nl/contents/pages/89927/advies.pdf`, consulted May 28, 2009.
3. R. Anderson. *Security Engineering*. John Wiley & Sons, 2001. Available at `www.cl.cam.ac.uk/~rja14/book.html`.
4. D. Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology: Proceedings of Crypto 82*, pages 199–203. Plenum Press, 1983.
5. D. Chaum. Secret-ballot receipts: true voter-verifiable elections. *IEEE Security & Privacy*, 2(1):38–47, 2004.
6. D. Chaum, P.Y.A. Ryan, and S. Schneider. A practical voter-verifiable election scheme. In S. de Capitani di Vimercati, P.F. Syverson, and D. Gollmann, editors, *ESORICS 2005, Proceedings*, number 3679 in Lect. Notes Comp. Sci., pages 118–139. Springer, 2005.
7. R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung. Multi-authority secret-ballot elections with linear work. In *Advances in Cryptology - EUROCRYPT'96*, volume 1070 of *LNCS*, pages 72–83. Springer-Verlag, 1996.
8. R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. In *Advances in Cryptology - EUROCRYPT'97*, volume 1233 of *LNCS*, pages 103–118. Springer-Verlag, 1997.
9. D. Evans and N. Paul. Election security: perception and reality. *IEEE Security & Privacy*, 2(1):24–31, January/February 2004.
10. Het Expertise Centrum, consultants voor overheidsinformatisering. Stand van zaken automatisering rond verkiezingsproces, 28 May 1999.
11. Het Expertise Centrum, consultants voor overheidsinformatisering. Definitierapport kiezen op afstand, 15 September 2000.
12. B. Gedrojc, M. Hueck, H. Hoogstraten, M. Koek, and S. Resink. Rapportage advisering toelaatbaarheid internetstemvoorziening waterschappen. Fox-IT, `http://www.verkeerenwaterstaat.nl/Images/20081302%20Bijlage%201%20Rapport_tcm195-228336.pdf`, 12 August 2008.
13. R. Gonggrijp, W.-J. Hengeveld, A. Bogk, D. Engling, H. Mehnert, F. Rieger, P. Scheffers, and B. Wels. Nedap/Groenendaal ES3B voting computer: a security analysis, October 6 2006. Availabe online: `http://www.wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf`, consulted May 28, 2009.

14. R. Gonggrijp, W.-J. Hengeveld, E. Hotting, S. Schmidt, and F. Weidemann. Ries — Rijnland Internet Election System. very quick scan of published source code and documentation, July 2008. Availabe online: `http://www.wijvertrouwenstemcomputersniet.nl/images/7/7f/RIES.pdf`, consulted May 28, 2009.
15. L.M.L.H.A. Hermans and M.J.W. van Twist. Stemmachines: een verweesd dossier. rapport van de commissie besluitvorming stemmachines, April 2007. Available online: `http://www.minbzk.nl/contents/pages/86914/rapportstemmachineseenverweesddossier.pdf`, consulted May 28, 2009.
16. M. Hirt and K. Sako. Efficient receipt-free voting based on homomorphic encryption. In B Preneel, editor, *Proc. EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 539–556, 2000.
17. E. Hubbers, B. Jacobs, and W. Pieters. RIES – Internet voting in action. In R. Bilof, editor, *Proc. 29th Annual International Computer Software and Applications Conference, COMPSAC'05*, pages 417–424. IEEE Computer Society, July 2005.
18. E. Hubbers, B. Jacobs, B. Schoenmakers, H. van Tilborg, and B. de Weger. Description and analysis of the RIES internet voting system, June 24 2008. Version 1.0, available online: `http://www.win.tue.nl/eipsi/images/RIES_descr_anal_v1.0_June_24.pdf`.
19. J.R. Kiniry, A.E. Morkan, F. Fairmichael, D. Cochran, P. Chalin, M. Oostdijk, and E. Hubbers. The koa remote voting system: A summary of work to date. In *Proceedings of Trustworthy Global Computing (TGC) 2006*, Lucca, Italy, 2006.
20. M. Kuhn, G. Friedrichs, A. Aksoy, E. Koch, and L. Friedrichs. Tempest specificaties en testmethoden voor elektronische stemapparatuur. Appendix BLG15766 of Kamerstuk 2007-2008, 31200 VII, nr. 64, Tweede Kamer, 21 May 2008.
21. N. Luhmann. Familiarity, confidence, trust: problems and alternatives. In D. Gambetta, editor, *Trust: Making and breaking of cooperative relations*. Basil Blackwell, Oxford, 1988.
22. Ü. Madise, P. Vinkel, and E. Maaten. Internet voting at the elections of local government councils on October 2005, 2006. `http://www.vvk.ee/english/report2006.pdf`, consulted November 9, 2007, not online anymore.
23. R.T. Mercuri. A better ballot box? *IEEE Spectrum*, 39(10):26–50, 2002.
24. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Project kiezen op afstand. report BPR2004/U79957, November 11 2004. Available online: `http://www.minbzk.nl/onderwerpen/grondwet-en/verkiezingen-en/kiezen-op-afstand/kamerstukken?ActItmIdt=12800`, consulted May 29, 2009.
25. P. Nikander and K. Karvonen. Users and trust in cyberspace. In B. Christianson, B. Crispo, J.A. Malcolm, and M. Roe, editors, *Security Protocols: 8th International Workshop, Cambridge, UK, April 3-5, 2000, Revised Papers*, number 2133 in Lecture Notes in Computer Science, pages 24–35. Springer, 2001.
26. A.M. Oostveen and P. Van den Besselaar. The effects of voting technologies on voting behaviour: Issues of trust and social identity. *Social Science Computer Review*, 23(3):304–311, 2005.
27. OSCE Office for Democratic Institutions and Human Rights. The Netherlands parliamentary elections 22 November 2006: OSCE/ODIHR election assessment mission report, March 12 2007. Available online: `http://www.osce.org/item/23602.html`, consulted May 28, 2009.
28. J.H. Park. England's controversy over the secret ballot. *Political Science Quarterly*, 46(1):51–86, March 1931.

29. W. Pieters. Acceptance of voting technology: between confidence and trust. In K. Stølen, W.H. Winsborough, F. Martinelli, and F. Massacci, editors, *Trust Management: 4th International Conference (iTrust 2006), Proceedings*, volume 3986 of *Lect. Notes Comp. Sci.*, pages 283–297. Springer, 2006.
30. W. Pieters. What proof do we prefer? variants of verifiability in voting. In P. Ryan, S. Anderson, T. Storer, I. Duncan, and J. Bryans, editors, *Workshop on e-Voting and e-Government in the UK*, pages 33–39, Edinburgh, February 27-28 2006. e-Science Institute, University of St. Andrews.
31. W. Pieters. *La volonté machinale: understanding the electronic voting controversy.* PhD thesis, Radboud University Nijmegen, January 2008.
32. W. Pieters and M. Becker. Ethics of e-voting: An essay on requirements and values in Internet elections. In P. Brey, F. Grodzinsky, and L. Introna, editors, *Ethics of New Information Technology: Proc. Sixth International Conference on Computer Ethics: Philosophical Enquiry (CEPE'05)*, pages 307–318, Enschede, 2005. Center for Telematics and Information Technology.
33. H. Robers. Electronic elections employing DES smartcards. Master's thesis, December 1998. `http://www.surfnet.nl/bijeenkomsten/ries/robers_scriptie_election.pdf`, consulted November 9, 2007, not online anymore.
34. K. Sako and J. Kilian. Receipt-free mix-type voting scheme – a practical solution to the implementation of a voting booth. In L.C. Guillou and J.-J. Quisquater, editors, *EUROCRYPT'95*, volume 921 of *LNCS*, pages 393–403. Springer, 1995.
35. R.G. Saltman. *The History and Politics of Voting Technology.* Palgrave Macmillan, New York, 2006.
36. B. Schoenmakers. Voting schemes. In M. Atallah and M. Blanton, editors, *Tools and algorithms for the contruction and analysis of systems.* CRC-Press, 2009, to appear.
37. T. Selker and J. Goler. Security vulnerabilities and problems with VVPT. Caltech / MIT Voting Technology Project, Working Paper #16, 2004. Available online: `http://www.vote.caltech.edu/drupal/files/working_paper/vtp_wp16.pdf`, consulted May 28, 2009.
38. P.P.C.C. Verbeek. *What things do: Philosophical Reflections on Technology, Agency, and Design.* Pennsylvania State University Press, 2005.