Measures to Establish Trust in Internet Voting

Melanie Volkamer
Technische Universität Darmstadt
Mornewegstraße 32
64293 Darmstadt, Germany
+49 6151 16 5422
melanie.volkamer@cased.de

Oliver Spycher
Bern University of Applied Sciences
Höheweg 82
2501 Biel
+41 32 321 63 18
oliver.spycher@bfh.ch

Eric Dubuis
Bern University of Applied Sciences
Höheweg 82
2501 Biel
+41 32 321 64 74
eric.dubuis@bfh.ch

ABSTRACT

Technical research has achieved strong advances in addressing security concerns in internet voting, yet the solutions are complicated and difficult to explain to the public. Accordingly, internet voting commonly faces opposition despite the benefits voters and authorities may expect. It appears that security features are only one premise underlying a system's acceptance among the electorate. The other challenge is to exploit these features at establishing the required trust among the public. In this paper we introduce a number of measures meant to help at gaining trust. We hereby emphasize the importance of taking the exposition of a system's security features and the remaining risks as the foundation of any strategy. After describing the proposed measures and discussing both their advantages and pitfalls, we relate them to four commonly known applied internet voting systems.

Categories and Subject Descriptors

K.4.1 [**Public Policy Issues**]

General Terms

Management, Documentation, Design, Security, Human Factors, Standardization, Legal Aspects, Verification.

Keywords

e-voting, elections, trust, internet, privacy, verifiability, transparency, evaluation, standards, acceptance

1. INTRODUCTION

During the past decade, many governments have begun to debate on introducing modern technology into their voting procedures. In the United States different types of electronic voting devices have already been in use for many years. Estonians have gained the experience of internet voting at two parliamentary elections, and numerous Swiss referenda have been conducted using the internet. After several trials at non-binding referenda, also Norwegian citizens will vote from their home computers at the binding municipal and county elections in fall 2011. Internet voting projects in the United States and Armenia are currently being assessed. In Germany and other countries internet voting is also in use, however only in the non-political context, i.e. at companies, universities and non-profit organizations.

ICEGOV2011, September 26–28, 2011, Tallinn, Estonia.

Voting technology comes with many promises. While some see the potential of saving significant time and money, others will hope to increase voter turnout due to easy and flexible participation. Also, voters may expect mechanisms to validate their ballot to avoid an invalid vote, and the needs of disabled people can be addressed adequately. Although many stakeholders in voting are likely to benefit from such features in some way, voting technology still faces opposition and distrust. Correspondingly, they do not accept the technology. Along with privacy concerns, critics express their doubts regarding the integrity of the outcome of elections. Accordingly, distrust towards the Irish voting machines culminated in the cancellation of the respective project shortly before going live. For similar reasons Germany and the Netherlands have persistently banned their voting machines from use at political votes.

Trust in voting technology that lasts can only be established when operating a system that complies with high security standards. On the other hand, securing a system even to the maximum imaginable extent alone will hardly increase any trust among the public. In order to avoid the fate of the voting machines in Germany, the Netherlands and Ireland, we must not only ask ourselves how to make systems that are more secure. The focus should rather lie on the primary, superordinate question of how to establish trust itself and in particular trust that lasts.

We perceive a voting system as "trusted" if it attracts voters and if it leads to confidence regarding the integrity of the published results and the secrecy of the vote. Apparently, systems may be well-accepted despite being unworthy of trust. Such a situation may emerge from a combination of initial blind trust or indifference among the public and an exposition by the voting authorities that does not relate to the employed security features. However, it seems that such acceptance is fragile and may easily be disrupted in the event of even small irregularities. Due to its lacking persistence, we believe that "trust based on unawareness" holds much potential for the failure of systems that actually deserve to be trusted. In our framework we therefore define a class of measures focusing on establishing "justified" trust, i.e. trust that grounds on openly exposed security features and their assessment by experts. A second class of measures is meant to attract voters who have other personal reasons not to cast an electronic vote, for instance due to distrusting their own technical abilities.

In the following section we start off by giving a first introduction to the measures that seem likely to have a positive impact on the public's view of a voting system. Section 3 shows related work that motivates the selection of our measures. Our further exposition will relate to the two prominent voting systems employed at parliamentary elections in Estonia and Norway, further to the voting system Polyas, which is mainly used for low

risk elections, and Helios, which emerged directly from security research. Section 4 briefly introduces each of these systems. Starting with section 5 we dedicate each section to one of the identified measures. In corresponding subsections we describe and discuss each measure and relate each one to its application within the different systems.

2. OVERVIEW OF MEASURES FOR TRUST ESTABLISHMENT

A literature review shows that there is only little work done on this topic. Although security in electronic voting is widely studied in the research community, the question of how to ideally benefit from security features at gaining the public's trust seems to be undiscussed. Certain measures may expose security features that solve one problem but introduce another. The prioritization of the two problems may be assessed variably among individuals and across societies. In our exposition we therefore discuss the measures in the light of both their benefits and pitfalls.

The list below introduces the measures in the scope of this paper. The comments after each point give a first intuition of how the measures are meant to be applied or explained in order establish trust. Note, that we do not aim at specifying an instructive hand-book on trust establishment, since it seems that the ideal selection and the concrete mode of application of the identified measures will vary over time, across societies, and in dependence of the type and character of the elections or referenda in question. We rather provide a starting point that should enable voting providers to estimate which ones they could employ in order to achieve a satisfying payoff in terms of trust.

1. **Transparency –** This is the key-measure for the successful application of the remaining ones. The more information is withheld, the less the public will appreciate the added value gained by applying the remaining measures.
2. **Evaluating the system according to international standards –** This is meant to confirm to voters that the developed system corresponds with the one that is documented in terms of security. It also suggests that accredited experts actually took advantage of the open documentation and performed a thorough analysis according to widely accepted security standards.
3. **Implementing separation of duty –** If all computations are performed at one site, secrecy and integrity can be violated there. By splitting up computational tasks among multiple organizations, the two security features will only be broken if the persons in charge at all sites illegally collude. Trust among the public is thus not only determined by the trust they bring forward to an individual party. It is rather defined due to the organizational independence of multiple parties.
4. **Enabling verifiability** – By accessing the data collected by the voting servers, voters can verify that their vote is counted as intended. They can even verify that all collected votes were cast by eligible voters and that all those votes are correctly counted. If all processed data can be verified as correct, it becomes obsolete to trust in any system players at preserving the integrity of the vote.
5. **Enabling vote updating –** If voters can re-cast and replace previous electronic votes, vote-buying can be rendered far more difficult. Further, voters must not fear any unease or confusion during or after the process of casting a vote.
6. **Test elections –** This measure allows voters to experience the full voting process beforehand. Thus, voters' doubts and concerns that emerge from the act of casting their vote itself can be addressed without requiring them to simultaneously question the success of a real election.
7. **Allowing independent implementations of voting client software** – Certain groups of voters may distrust the correct functioning of the officially provided voting client software (the program they use for casting votes). Other groups may fear that they will not be able to operate the product correctly. In both cases the possibility of using an alternative product could be appreciated.

Points 3-5 comprise measures that are directly derived from concrete technical system aspects. The technical system aspects in return imply security features. Unfortunately the perfect system, i.e. the one that solves all commonly quoted security concerns simultaneously, has not yet been invented. Accordingly, with contemporary systems the goal can never lie in suggesting to the public that every security gap is closed. Nevertheless, if the electorate gets an understanding of the security features, we believe that it will more likely assess certain security gaps as acceptable and gain trust towards a system in spite. The gained trust will be rather persistent since it is directly qualified by the system itself. In that spirit, measures 1-5 (our first class of measures) seem helpful as a starting point for explaining the strengths and limitations of those security features and thus aid voters at assessing the trustworthiness of the system as a whole. We point out that despite known security deficiencies the traditional paper-based model is also generally accepted. It seems reasonable to believe that the acceptance mostly relies on a common understanding of the remaining risks.

While an appropriate application of measures 1 and 2 supports the payoff of measures 3-5, measures 6 and 7 do not directly imply enhanced security features of the overall system. Nevertheless, they address personal concerns that may keep voters from casting their vote. Concerns may include distrust towards their own technical abilities or personal reservations towards the organizations who provide and operate the system. Measures 6 and 7 form the second class.

Due to space constraints the list of measures is incomplete. We leave further possibilities such as “voting by personalized codes” to address secrecy and integrity on the voters’ computers, or “employ cryptographic smartcards” to address sound remote authentication to future work.

3. RELATED WORK

Some of the measures listed in the previous section relate to the following three existing documents: 'Guidelines on transparency of e-enabled elections' published by the Council of Europe in [1], the discussion in [2] on advantages and disadvantages of two concrete measures, i.e. security evaluation versus verifiability, and the computation of a k-resilience value in [3] and [4] to clarify which entities (including persons, hardware and software) voters need to trust in terms of not maliciously collaborating in order to violate one of the security requirements. Further, [5] proposes a list of information that should be published in the context of an electronic voting project.

In order to ensure that our list of measures is more comprehensive than in existing literature and that the paper contains an objective analysis of these methods, we integrate the measures proposed in [1] and extend them. Further, our exposition of the verifiability and the evaluation measure takes into account corresponding discussions from [2]. Furthermore, the k-resilience approach from [3] and [4] is integrated in the separation of duty measure. Our statements on the transparency measure also include propositions from [5] regarding what kind of information should be published about an electronic voting system.

4. VOTING SYSTEMS

In this section we shortly introduce the internet voting systems and corresponding projects that we discuss in the light of the measures enlisted in section 2. We have selected the systems and projects that provide enough publicly available information.

4.1 Estonian System

The Estonian system was used at the national governmental level in the 2007 and 2011 parliamentary elections [6]. Estonians wanted to be the first nation to implement internet voting nationwide. They succeeded due to beneficial preconditions. First of all the widely distributed national electronic identification document (ID card), secondly the huge amount of other e-governmental applications enabled over the internet and last but not least the confidence in the young government.

In 2007 30,275 voters used internet voting, representing 3.4% of the eligible voters and 5.4% of the votes cast. In 2011 140,846 voters used internet voting, representing 15,4% of the eligible voters, and 24,3% of the votes cast [7].

There are a couple of available sources which were used as input for the analysis below: The Election Assessment Mission Report of the OSCE "Office for Democratic Institutions and Human Rights" (ODIHR) [8], the Report for the Council of Europe by the European Union Democracy Observatory [9], and the web pages of the National Electoral Committee (NEC) [6],[7].

4.2 Norwegian System

The Norwegian internet voting project has recently been started and is the one that is currently discussed most. The government's motivation is to increase the availability of the voting system and to reduce costs in the long term. The internet voting channel is available for everyone in advance to the Election Day. After registering, voters authenticate based on a well-established service called MinID, which has already been employed for other governmental purposes. Trials are planned in ten municipalities for the 2011 county and municipal elections in fall. Afterwards, the parliament will decide whether to continue the project and enable remote electronic voting for federal elections in future.

The employed system is provided by Scytl, a renowned provider of internet voting solutions. Of all internet voting systems that are currently in use for political votes, the Norwegian one is by far the most documented. Documents describing the administrative context, including project guidelines, responsibilities and milestones, but also the technical system features themselves including the source code can be accessed publicly through the project web-site [10],[11],[12].

4.3 Helios System for academic elections

Based on preexisting cryptographic and web development technologies, the Helios system was designed to provide an accessible End-to-End verifiable remote electronic voting solution. Helios was first presented and mainly implemented by Ben Adida [13],[14][15]. However, Helios is far from being just a research project and an experimental prototype of a remote electronic voting system. There exist first user guidelines [16] and videos explaining the ballot casting process [17]. Different custom deployments of Helios were successfully used in actual legally binding elections, namely for the university's presidential election in March 2009 at the Université Catholique de Louvain [18], 2010 for the election of student associations at Princeton University, and the election for the International Association of Cryptographic Research (IACR). In this paper, we refer to the last deployment at IACR.

4.4 Polyas System for the GI election

The Polyas Internet voting system has been developed by Micromata Objects GmbH, a company headquartered in Kassel, Germany. Polyas has been in use since 1996 in various national and international elections in the private sector including those for the DFG - Deutsche Forschungsgesellschaft (German Science Foundation) -, the Initiative D21 Association, the Swiss Life Group (an insurance company), and both Finnish and German youth elections. Recently, it was used to enable remote electronic voting for the first legally binding university election at the Friedrich-Schiller-University in Jena, Germany. The most popular example has been the annual elections of the GI – Gesellschaft für Informatik (German Society for Computer Scientists) -, where it has been used in parallel with postal voting since 2004 (for example in 2010, 3193 members cast an electronic vote and only 51 cast a mail vote). Therefore, in this paper we refer to the annual GI's elections. Information can be found in [19] and [20] and on the Polyas web page [21].

Polyas has so far successfully handled all these elections. It is estimated that as of 2010, about one million legally binding votes have been cast using this voting system [20]. However, we note that these elections, similarly as the one run with Helios, bear a low public profile and a low security risk.

5. TRANSPARENCY

Transparency is the key element for establishing trust among the public. In the absence of a thorough documentation, the public would not be able to assess and appreciate the qualities of a system. Instead, trust would solely rely on vague assertions provided by the election organizers and their contractors. Notably, if authorities fail to inform the electorate on the applied security precautions, significant efforts may be wasted that hold much potential of increasing trust.

5.1 Description

Relevant information includes the following[1]:

- Full technical documentation of how the system is designed functionally and technically (user interface, employed protocols, all levels of software documentation, source code) and of the technical and organizational environments where the system is hosted. The exposition should relate to a security goal that is clearly defined. This should allow

[1] Note that we exclude information which is already relevant for traditional paper based elections like the notification of elections and the nomination of candidates.

independent experts to understand and appreciate the security features, and establish their individual assessment.

- A simplified documentation of how the system works under the application of the chosen measures to establish trust. They can be explained easily on a high level and allow the broad public to assess the trustworthiness of a system. In the exposition limitations of security should also be pointed out in terms of those measures. Independent technical experts should confirm to the public that the simplified documentation has been correctly derived from the full technical documentation and that the exposition of the limitations in security is complete.
- A public platform for collecting and answering questions and doubts among the electorate.
- Administrative project information including a project plan, the call for tender and minutes of meetings. All involved parties and their responsibilities should be clearly declared.
- Full documentation of all conducted evaluations, also assessments provided by independent experts. It should relate to the system documentation (full and simplified) and most importantly to concerns expressed by the public.

The published documents should clearly refer to each other and need to be available early enough for everyone to read and analyze. Thus, doubts can be ruled out early enough before going live.

5.2 Discussion

In order to be able to provide all this information, the transparency policy should be explained and discussed with the vendor before the tender. Generally, companies will not likely be thrilled about sharing too many details on their technology with the market.

By consistently following the transparency guideline, the project will become more expensive for various reasons: First of all, the vendor will most likely ask for an extra compensation. Also a lot of documents have to be produced and managed. Further it is required to hire extra staff to answer general and specific questions on the documentation and the system.

The following issues related to changes in the system during the preparation phase should be discussed and corresponding guidelines set before starting the project:

- When is information ready to be published? (Not too early, because items may change, but not too late to allow analysis.)
- How should changes in the full system documentation be managed?
- How should change recommendations be handled after costly and time-consuming evaluations have been successfully performed? (Implement change and re-evaluate, or go ahead as planned.)

Further, publishing all this information bears the risk that someone exposes vulnerabilities that give the project bad press. The risk of people losing blind trust just due to the mere fact the system's security aspects are debated seems real. However, if security problems can be solved due to transparency, the election authorities can gain much credibility when explaining their system.

5.3 Systems in Use

In the past, electronic voting projects generally published only scarce information about their systems. The public documentation was incomplete and kept on a very high level of exposition. Notably it did not allow to analyze and understand the system and its security in depth. Generally only the average voter is addressed and given a high level understanding of the system, mostly focused on why the secrecy of the vote will not be at stake. In some cases it is possible to get more information and also the source code after signing a very restrictive NDA. The two systems on which finally more public information is made available are the Norwegian and the Helios system.

Specifically, the following transparency levels in terms of published information are reached in the different systems:

The source code of the Estonian system and log files after an election can only be reviewed after signing a restrictive NDA. Interested people have to visit an office where the information is provided on some machine. Thus, it is not possible to use own equipment for the review. However, information about the Estonian system is available for average voters and distributed to the public explaining them how the system operates on a very high level and in particular that the internet voting system exactly mimics the mail voting system. This is explained in such an approachable way that people believe to understand the voting system and that it is secure.

The Norwegian project has chosen transparency as one of their main guidelines. The available documentation shows high quality and is presented in a logical, accessible structure on their web-site [10]. The protocol underlying the system is presented in [11]. The same document provides an analysis of its security features. The security objectives are defined in [12]. Furthermore, the source code is publicly available and Common Criteria Security Targets. Since the project is still at an early stage, one may expect to find detailed information on the implementation of their system soon.

Documentation about the Polyas system as well as the source code is made available after signing an NDA. Some people from the GI signed this NDA and reviewed the source code and some documents. For non-experts there exists a high level explanation of the system as well as a FAQ and screen shots showing the vote casting process.

As the Helios system is an open source project and papers on the protocol have been published on several conferences, detailed information is available including a security concept. However, as it is an academic project the specification of the source code is hard to understand due to missing or inconsistent documentation. For the average voter, there exist videos accessible on youtube.com, showing how to cast and how to verify the correct casting of a vote. However, background information on verifiability and its inherent benefits and pitfalls is not included.

6. EVALUATION

People are used to the approach of having accredited companies or agencies evaluate products (devices, food, but also software). Accordingly, the evaluation of a voting system according to standardized and internationally recognized procedures is critical at establishing trust.

6.1 Description

Some may argue that an evaluation of the remote electronic voting system is not necessary for systems that implement E2E

verifiability. According to [2] this is not the case because verifiability only covers the integrity of the election outcome but not privacy and many other requirements. In addition, people who are not familiar with verifiability and the related cryptography, will gain more trust if they know that qualified experts checked the system according some standard evaluation approaches. Notably, publishing the detailed system documentation alone does not automatically imply that experts will thoroughly look into them, as this costs time and money.

Such a standardized evaluation approach should contain formal logical and mathematical methods to prove that the system ensures the security requirements. Correspondingly, most of the evaluation techniques address security. However, also the usability should be evaluated.

Regardless of the item under evaluation, it is important to base the evaluation on international standards (in general ISO) or recognized research methods. Thus, it is ensured that the evaluation methods, depth and processes are transparent.

Ideally, such an evaluation would envelope the following approaches:

- Formal protocol analysis and proofs including the identification of underlying assumptions fitting to the published security concept (see Section 4)
- Common Criteria evaluation [28] for software components of the voting system e.g. according to or based on the existing Protection Profile [29]
- ISO 27001 [30] or similar standards to evaluate the security of the infrastructure (servers, backup systems, organizational measures, etc.) in which the internet voting software is used; again including the identification of underlying assumptions fitting to the published security concept
- Observation of security critical processes during preparation and election; as due to our knowledge there exists no standard; at least a concept should be developed in the preparation phase of the project

Whatever path is taken, it should be explained and its choice justified to the public.

6.2 Discussion

All of these evaluations are costly and time-consuming. Thus, evaluations have to be started early enough (probably between 9 and 12 month before the day the certificate is required). Notably special knowledge to produce corresponding documents is required. In addition, the Protection Profile proposed in [29] only covers basic requirements and in particular does not address verifiability. Correspondingly, this Protection Profile needs to be extended for broader application.

Such security evaluations are very static and the certificate is only valid for one particular implementation of a system. A re-evaluation after modifications is required. Thus, changes shortly before the election would mean that a non-certified system is used for the election (compare to section 5.2).

6.3 Systems in Use

In many projects, the security of the voting protocol and/or the voting software and/or the infrastructure has been analyzed by internal experts. However, it remains unclear who and how many people with which background and expertise, using which methods have participated and how deep the evaluation went. This intransparency results in mistrust.

The Polyas system is currently undergoing a Common Criteria evaluation according to the Protection Profile proposed in [29]. Also the Norwegian project announced that they will go for a Common Criteria evaluation and even a more thorough one than demanded in [29] before using the voting system for further elections after the local elections this year in September. In addition, they announce to run the voting software only in data processing centers that are certified according to ISO 27001 [30].

The only system that – due to our knowledge – has been analyzed scientifically regarding its usability is the Helios system [32]. The user study identifies a few flaws in the interface design.

A formal voting protocol analysis has only been done on the Norwegian one. The analysis shows many beneficial security features. However, it lies in the nature of protocol definitions that they do not specify all technical particularities it takes for defining a full system. The protocol analysis thus simply assumes beneficial security features of some of the components. Once the detailed technical specification documents are made available, trust would benefit from an analysis on whether the system succeeds in complying with the initial assumptions on the security features.

The Estonian project applies a different approach. They have auditors who have a booklet describing all steps administrators have to take during the election set up, the election phase and the tallying. They are present together with the administrators to take care that the administrators take only these steps and log this manually. As it is unclear what is described in the booklet and who produced and checked it, this measures seems to be weak at establishing trust.

7. SEPARATION OF DUTY

If a process is designed to output data, appropriate verification mechanisms might allow acknowledging its correct execution.[2] However, it is much harder to verify that all copies of critical data have been deleted, when they are supposed to, or that computations have not been performed, when they are not supposed to.

7.1 Description

Particularly, no system entity should compute the information showing how voters voted (privacy) and no partial result of the ballot should be available prior to the closing of the polls (fairness). Although the Council of Europe recommendations [1] do not explicitly enlist these requirements, it seems reasonable to believe that they underlie the public acceptance within any electorate. In [22] the effect of doubts regarding privacy on internet consumer behaviour has been observed. Similarly, establishing trust in secrecy is bound to have a positive effect on the acceptance of a voting system.

By distributing secrecy-critical duties, one can exclude the event of a single entity being able to break the voters' privacy or fairness. Under separation of duty, secrecy is only broken if a

[2] The question of how to verify the integrity of an election is discussed in the next section. Separation of duty with regard to integrity is also discussed there, i.e. as a weaker replacement of verifiability. Other requirements in this context like robustness are left for future work.

whole group of entities fail in following their respective procedures correctly.

Responsibilities can be separated on various levels, i.e. organizational (enforcing restricted access to information within an organization), architectural (physically and logically separating information) and evolutionary (having the organizations in charge use their own equipment, particularly use self-developed or well-established 3rd party software). The degree of the gained trust heavily relies on the selection of the responsible parties, their ability to perform their duties independently and to confirm to the public that they have done so truthfully.

Trust in secrecy will certainly benefit from the good reputation of a vote organizer in combination with experts who confirm the implementation of sophisticated measures to guarantee for secrecy. However "real" trust as specified in the introduction grounds on an explanation on how secrecy is ensured. Identifying a number of independent organizations and stating that privacy will only be broken if all organizations collude can be easily understood. Finally, instead of requiring all voters to trust in the same organization, it is sufficient for each voter to trust in merely one out of all participating ones. In a society where individuals tend to confide in the party they vote for, it may seem reasonable to distribute duties evenly across the political spectrum.

7.2 Discussion

Separation of duty has the potential of drastically reducing the probability that secrecy properties are broken. Yet, the extent of the gained trust strongly depends on the degree of separation (organizational, architectural, and evolutionary). While there is an obvious benefit in running computations independently at different sites (architectural), the payoff is limited when each party runs the same software, since trust in the overall system again reduces to one entity, i.e. the producer of the software. Similarly, separation of duty is not fully in place when all involved parties need to store their data at a common central server despite using self developed software (evolutionary). On the other hand, splitting responsibilities to a full degree is expensive and operationally complicated. Nevertheless, there are technical measures to allow critical computations to be performed not necessarily by the full group of players, but only by a fraction [23]. Thus, the failures of few system players will not affect the success of the whole system.

Separation of duty only makes sense if it is taken as a guideline that is consistently followed. For instance it will not help much to define a system in which secrecy-critical information, such as the secret keys for decrypting votes, is initially generated by one single entity on behalf of all other parties. If there is a need for making such compromises, it is inevitable to declare the risk openly in the documentation at an early stage. If the security gap is discovered at a point when elections have already been held under the impression of separation of duty, voters may feel misled.

7.3 Systems in Use

A minimal degree of separation of duty on the organizational level will need to be implemented in any system. Otherwise at least one employee could inherently access the critical data.

In that sense the Estonian system employs multiple servers to provide separation of duty on an organizational level. By having multiple election officers provide their individual keys to decrypt the votes contained by the hardware security module (HSM), the regular decryption process cannot be executed prematurely. Before the votes reach the HSM they are mixed by one server for anonymization. Thus, here separation of duty is not implemented as there is only one server mixing the encrypted votes. (The server holds the information showing the order of the decrypted votes and can thus reveal privacy.)

Polyas and the Norwegian system both distribute secrecy critical duties between two sites. In the case of Polyas, one site is provided by its producer Micromata, the other site is operated by the organizer of the election. In Norway information is split between two governmental organizations that act independently and are located 700 km apart.

Helios provides the possibility to select more than one "trustee" and the idea is that only if all trustees collaborate maliciously the secrecy of the vote can be broken. However, using only the software from the web would also mean that the software for different entities is programmed by the same team and also all components are hosted by this team. Correspondingly, before using Helios for legal binding elections software components have to be re-programmed and hosted by different parties.

Note, in all four cases the employed software is produced by the same company, which is not ideal. We conclude that separation of duty is implemented to some degree in all projects. However, there is much potential for improvement.

8. VERIFIABILITY

In traditional voting voters witness their ballot reach its destination inside the ballot box themselves. Knowing that the ballot box is under constant surveillance, they are reassured that their vote will be included in the counting procedure. In some countries concerned citizens are even allowed to witness the counting and verify that the staff performs their tasks with care. It seems natural that citizens who appreciate these privileges will ask for strong integrity reassurances in internet voting as well. Based on a verdict of the German federal constitutional court in 2009, German voters are even explicitly required to be able to verify that their vote is correctly recorded and considered in the final outcome. Complying with this requirement involves introducing appropriate technical measures.

8.1 Description

Voting systems are widely considered verifiable (also called end-to-end verifiable) when corresponding with the following three properties.

- According to [1],[24], individual verifiability enables the voter to verify that his vote is cast as intended and that it is stored in the electronic ballot box as cast.
- According to [1],[24], universal verifiability enables the voter and everyone else to verify that all votes stored at the voting server are properly tallied.
- According to [25], eligibility verifiability enables anyone to check that each vote in the election outcome was cast by a registered voter and there is at most one vote per voter.

Ideally, the available mechanisms will offer verifiability without requiring voters to trust any system players. The key to achieving that lies in publishing the electronic ballot box along with all data needed to assert the correct execution of the tallying procedure. Apart from information taken from the cast ballots, the data will generally comprise so-called zero-knowledge proofs to justify all partial computation steps on a public bulletin board. These proofs

mathematically reveal enough information to provide evidence of correct tallying; however they do not reveal any secrecy-critical information.

8.2 Discussion

The application of the required cryptographic techniques yields the outlined approach very promising. However, it comes along with drawbacks that may lead to the decision not to provide full end-to-end verifiability because of security gaps that are introduced due to its implementation.

1. If voters are provided with a proof to confirm that their vote will be counted as intended, they can use that proof to reveal to a third party how they voted. The existence of such „receipts“ increase the risk of vote buying. Technical approaches to solve that dilemma have been introduced [26], however it will take further research before these ideas have sufficiently matured for efficient application in practice.
2. Privacy relies on the long-term security of the employed cryptographic techniques. While experts will find it reasonable to believe that these are powerful enough to maintain privacy during the coming few decades, one must assume that somewhen in the far future the privacy of today's electorate will be broken. Whether coming generations may be made responsible for unpopular political views of their ancestors is a matter of debate.

These concerns may lead to a solution where only auditors are given the access to the full collection of voting data and perform the remaining verification steps not granted to the public. Nevertheless, under the assumption of appropriate separation of duty, voters can be strongly reassured that their vote is counted as intended. In that case it is crucial that voters are told what they actually verify themselves and what aspects are delegated to auditors. This can be easily explained in terms of separation of duty as exposed in the previous section. The trust among the public then depends on the trust they bring forward towards these authorities and their ability to publicly confirm that they have performed their tasks independently and truthfully.

Further, end-to-end verification using the contemporary methods grounds on calculations one cannot perform with pen and paper. Successful verification thus requires the electorate’s trust in the programs provided to perform the verification and the integrity of the computer the verification is performed on. Nevertheless, verification steps can be repeated using different platforms and independent third party software.

The responsible authorities need to establish legal guidelines to handle cases where voters claim that their verification failed. Apparently, vote updating, discussed in the next section, constitutes an appropriate auxiliary instrument.

8.3 Systems in Use

The Helios system is the strongest in fulfilling the criteria for end-to-end verifiability: The relevant cryptographic data is displayed to the user who can then use third party software and verify that his vote has been considered in the final tally along with all other ones. However, note that the strong sense of verifiability allows voters to obtain a receipt to reveal to others how they voted. The Polyas system only provides universal verifiability and the possibility to verify that votes have been cast as intended. However voters need to trust in one specific site in the backend (i.e. one server) in storing their vote correctly. The Norwegian system also provides verifiability in terms of “cast as intended”, while “stored cast” is granted under the premise that *at least* one of any of the two backend sites follows its procedures correctly. However, the universal and eligibility verification is only granted to auditors, not to the people sitting at home. The election officials have chosen this approach for making it impossible for voters to prove to third parties that do not participate in the system infrastructure how they voted. In the Estonian system, no verifiability is provided.

9. VOTE UPDATING

Vote updating (re-cast and replace the previously cast electronic vote) is a measure to establish trust regarding integrity of the published result, in the sense that the published result captures the electorate’s free will.

9.1 Description

In many cases remote electronic voting is introduced as an additional channel to traditional paper based elections at polling stations. For the traditional channel the vote casting process is protected by a polling booth and the poll workers, whereas for the remote electronic voting channel, the vote casting process is conducted in an uncontrolled environment, i.e. where the voter might be observed or influenced when casting his vote. In order to undermine voters' fears and inherently generate trust in the remote electronic voting system, the election authorities should implement vote updating. This allows a voter to update his electronic vote multiple times, particularly until he is convinced that he successfully cast his vote unobserved and without being influenced. Given this possibility, vote-buying becomes far less interesting.

Voters might distrust the voting system only after the experience of casting their vote. This might occur for instance when they misinterpret information presented to them, or when detecting malware on their PC after casting their vote. Correspondingly, they would not know whether their vote is sent and stored properly or whether the process was interrupted before. Again, in order to take away corresponding fears from the voter and correspondingly gain trust in the remote electronic voting system, the election authorities can implement vote updating including overwriting the e-votes with a paper vote.

9.2 Discussion

There are different ways to implement vote updating (compare to [27]) while they have different advantages and disadvantages. In general, replacing electronic votes by a paper one can support receipt-freeness in the context of verifiable electronic voting systems. A general challenge is to ensure that the last vote is counted and no problems by replay-attacks or delays on the network can cause that an earlier vote is counted.

Opponents of vote updating argue that vote updating influences the value and character of an election. They argue that the act of casting a vote is something special and should not be repeatable otherwise it gets the character of a game.

9.3 Systems in Use

Vote updating has become popular after Estonia has implemented it for its parliamentary elections in 2007. Apart from Estonia, it is also applied in the Norwegian and the Helios system.

The only system that does not offer vote updating is Polyas. They claim that this is to maintain the seriousness of an election. Also

from a technical point of view, vote updating would not easily be integrated as the system separates information on the voter from information on the vote already during the stage of casting. Thus it becomes problematic to elicit the vote to be replaced.

10. TEST ELECTION

Test elections before the binding elections enable voters to get familiar and learn how to use the system properly.

10.1 Description

All the other described trust establishment measures can be supported by implementing test elections before the main election. Such test elections would enable voters to "play" with the new voting system, get used to it, cast test votes without being afraid to make mistakes. They can also get used to new mechanisms like verifiability and vote updating.

Such a test election should be as similar to the main election as possible in order not to confuse voters, i.e. they should receive their login data through the same channel as for the main election. Also the hotline to call in case of questions or problems should be available.

It is not recommended to use a pre-system for test elections, with reduced functionality as this might confuse the voter to see a different system for the real election. In addition, there should be enough time for the test election. Thus, every potential voter should have the chance to test the system.

Besides running a test election right before the main election one could also run a mock election in parallel to a paper based election and enable everyone who is interested in to cast in addition an electronic vote. Here, the paper votes are the legal binding ones and the electronic voting system is only to enable voters to gain experience with the internet voting system.

Sometimes, 'test elections' are also implemented with selected voters to get feedback about the interface. As this is part of the usability evaluation this does not count under the category test election.

10.2 Discussion

Almost no disadvantages can be identified for this measure. The only disadvantages are the additional costs and the additional time required to run the test election. Notably, the final system needs to be ready prior to the real election.

10.3 Systems in Use

In most of the projects they have test elections but in general not for all voters but only for a selected group.

Estonia runs test elections before all parliamentary elections but due to our knowledge only for selected voters. The same is true for the GI elections. For each GI election, Micromata runs a test election for 100 randomly selected voters. They can also give feedback to further improve the system. Thus, this helps only partially to get used to the system. However, the situation is different as Polyas has been used for GI elections since 2005. Thus, most voters are already familiar with the system.

As Helios is an open source system, it is easy to conduct a test election. When the system was used for the IACR elections they formally run a test election.

In Norway, they currently run test elections, however using a system with reduced functionality; particularly the SMS for verifiability is not yet implemented.

11. ALLOWING INDEPENDENT IMPLEMETATIONS OF VOTING CLIENT

Allowing and supporting the development of client software by third parties is meant to address concerns regarding the trustworthiness of the official product.

11.1 Description

Voters need to have a high degree of trust in the client side voting software they run on their home PC because the software generally gets secrecy-critical information, i.e. the vote to be cast and also the identity of the voter at authentication. By sending out that information fairness and privacy can be broken. Furthermore, voters may fear that the software neglects the user's input and casts a vote for the wrong party and misleads at verification.

Voters who personally feel that the official vendor was the wrong choice will benefit from this measure, too. Thus, the voter does not need to trust one particular client but can use one from any entity he thinks is trustworthy, for instance his preferred party.

Further, a variety of clients is likely to attract more voters. For instance, people who fear being misled during the voting process due to their own inexperience with the internet may be provided with a client that offers the guidance tailored for their needs.

11.2 Discussion

By publishing a documentation of the technical interface used on the backend site, it becomes very simple for third parties to develop their own voting client. Even people with limited engineering experience will be able to produce and distribute their own software. This effect will allow voters to choose their preferred product out of a great choice.

Although this freedom of choice will improve the trust of individual voters regarding their own vote, the approach holds the risk of having malicious software in the market. Client software could potentially be designed to influence voters in their choice, or even worse, reveal or alter their choice unnoticed. Under this premise voters may tend to lose confidence in the integrity of the published election outcome. Nevertheless this can be mitigated by allowing only clients that have been assessed by accredited institutions. In any case voters need to be educated on their risks when using software from a third party. Election authorities need to assess whether the gained trust due to this approach is likely to outrule the risk of malicious software being spread.

11.3 Systems in Use

None of the projects in our scope encourages people to develop further voting clients. Nevertheless, the Helios system is open source and thus allows deducing rather easily how to develop another voting client. Similarly in Polyas one can elicit how to make a client by reading the html code in the browser. As in Helios the same should be possible in the Norwegian project as soon as the source code is made available. Whether they plan to publish technical documentation of their server interface and motivate to use it for engineering voting clients is still unclear. The Estonian system does not publicly document its software on a technical level, which makes it rather difficult to deduce the necessary details to implement an own client.

12. CONCLUSION

Technical research in voting technology has made significant advances. Many schemes have been proposed to meet the high security standards required at elections. Although not all concerns can yet be addressed simultaneously, experts feel that the contemporary state of research allows developing solutions that yield remaining risks and dangers negligible. We have argued that the discussed measures are suited to allow the broad public to feel alike. Further measures will be discussed in a survey in the near future.

We have argued that transparency will allow independent experts to assess a system's qualities and establish their opinion. Since transparency relates to a system's technical security features, experts are likely to gain rather than lose trust in a system, given that it exhibits the expected qualities. Under this premise alone, the technical laymen still do not know which experts to take as their reference. Hereby, the primary difficulty does not lie in estimating whether the experts have the skills it takes for a thorough assessment. The difficult question lies in estimating which experts share their moral standards. The transparency measure, thus being the most critical one, foresees a documentation to address the majority of the public who are not aware of technical particularities. We have explained why the documentation should describe the remaining dangers and risks in a non-technical language. This allows anyone who is interested to assess the trustworthiness of a system on the base of their own moral standards. Since irregularities during an election process can be explained in terms of the widely accepted risks, it seems less likely that voters lose their trust once it has been established.

We have shown that each of the proposed measures is employed by at least one of the four presented internet voting systems. While some have been consciously ruled out (e.g. Polyas explicitly excludes “vote updating”), others are often implemented only to a minor degree.

It is the task of the responsible election authorities to estimate which concerns regarding security are the most prominent among their citizens. The measures should then be selected accordingly.

13. REFERENCES

[1] Directorate general of democracy and politcal affairs. 2010. *Guidelines on transparency of e-enabled elections*. Technical Report. GGIS (2010) 5 E, Council of Europe.

[2] Volkamer, M., Schryen, G., Langer, L., Schmidt, A. and Buchmann, J. 2009. *Elektronische Wahlen: Verifizierung vs. Zertifizierung*. In *Proceedings of the Informatik 2009: Im Focus das Leben, Beiträge der 39. Jahrestagung der Gesellschaft für Informatik e.V. (GI)* (Bonn, Germany, 2009). Gesellschaft für Informatik, LNI 154, pp. 1827 – 1836.

[3] Volkamer, M. and Grimm, R. 2009. *Determine the Resilience of Evaluated Internet Voting Systems*. In First International Workshop on Requirements Engineering for E-Voting Systems, IEEE CS Digital Library, 10.1109/RE-VOTE.2009.2, 47–54.

[4] Volkamer, M. and Schryen, G. 2010. *Measuring eTrust in distributed systems - General Concept and Application to Internet Voting*. In *Proceedings of the 23rd Bled eConference* (Bled, Slovenia, June 20-23, 2010, forthcoming)

[5] Volkamer, M. 2009. *Evaluation of Electronic Voting - Requirements and Evaluation Procedures to Support Responsible Election Authorities*. Volume 30 of LNBIP, Springer.

[6] National Electoral Committee (NEC). 2005. *E-Voting System – Overview*. Online available http://www.vvk.ee/public/dok/Yldkirjeldus-eng.pdf

[7] National Electoral Committee (NEC). 2007. *Parliamentary Elections 2007: Statistics of E-Voting Estonian*. Online available http://www.vvk.ee/english/Ivoting_stat_eng.pdf

[8] OSCE/ODIHR Election Assessment Mission Report. 2007. *Parliamentary Elections in Estonia OSCE*. Online available http://www.osce.org/odihr/elections/estonia/25925

[9] European Union Democracy Observatory. 2007. *Report for the Council of Europe: Internet Voting in the March 2007 Parliamentary Elections in Estonia*. Online available http://www.vvk.ee/english/CoE_and_NEC_Report_E-Voting 2007.pdf

[10] E-vote 2011-project webpage; Online available http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html

[11] Gjøsteen, K.: *Analysis of an internet voting protocol*. Cryptology ePrint Archive, Report 2010/380 (2010), http://eprint.iacr.org/

[12] *e-Vote 2011 Security Objectives.* Report; Online available http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/tekniskdok/Security_Objectives_v2.pdf

[13] Adida, B. 2008. *Helios: Web-based open-audit voting*. In *Proceedings of the 17th Symposium on Security* (Berkeley, CA, USA, 2008), Usenix Association, pp. 335 – 348.

[14] Helios Voting System webpage; Online available http://heliosvoting.org/

[15] Documentation site for the Helios Voting System; Online available http://documentation.heliosvoting.org/

[16] Helios video; Online available http://usg.princeton.edu/%20index.php?option=com_content&view=article&id=230:guide-to-helios&catid=78:elections&Itemid=115

[17] Yaroshefsky, M. 2009. *Guide to Helios*. Princeton University. Online available http://usg.princeton.edu/usg-senate/elections-center/guide-to-helios.html

[18] Adida, B., Pereira, O., Marneffe, O. D. and Jacques Quisquater, J. 2009. *Electing a university president using open-audit voting: Analysis of real-world use of helios*. In Electronic Voting Technology/Workshop on Trustworthy Elections (EVT/WOTE (2009).

[19] Reinhard K. and Jung W., “Compliance of polyas with the BSI Protection Profile - Basic Requirements for Remote Electronic Voting Systems,” in Proceedings of the 1st international conference on E-voting and identity, ser. LNCS. Springer, 2007, pp. 62–75.

[20] Menke N. and Reinhard K., “Compliance of POLYAS with the Common Criteria Protection Profile - A 2010 outlook on Certified Remote Electronic Voting,” in Proceedings of the 4th International Conference on Electronic Voting 2010, ser. LNI. Springer, 2010, pp. 109 – 118.

[21] Polyas webpage; Online available http://www.polyas.de

[22] Brown M. and Rose M. (2004-02) *Investigating the relationship between internet privacy concerns and online purchase behavior*. Journal of Electronic Commerce Research, 5 1: 62-70.´

[23] A. Shamir. *How to share a secret*. Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.

[24] Gharadaghy, R. and Volkamer, M. 2010. *Verifiability in Electronic Voting - Explanations for non security expert*. In *Proceeding of the Electronic Voting 2010 - 4th International Conference* (Bonn, Germany, 2010). Gesellschaft für Informatik, LNI 167, pp. 151 – 162.

[25] Kremer, S., Ryan, M., Smyth, B.: *Election verifiability in electronic voting protocols*. In: Proceedings of the 15th European conference on Research in computersecurity. pp. 389–404. ESORICS'10, Springer-Verlag, Berlin, Heidelberg (2010).

[26] Juels, A., Catalano, D., Jakobsson, M.: *Coercion-resistant electronic elections*. In: Atluri, V., De Capitani di Vimercati, S., Dingledine, R. (eds.) WPES'05, 4th ACM Workshop on Privacy in the Electronic Society. pp. 61-70. Alexandria, USA (2005)

[27] Volkamer M. and Grimm R. 2006. *Multiple Cast in Online Voting - Analyzing Chances*. In Electronic Voting 2006. 2nd International Workshop, volume 86 of LNI, pages 97-106, Bonn, 2006. Gesellschaft für Informatik.

[28] ISO 15408– Common Criteria for Information Technology Security Evaluation (CC) Online available at http://www.commoncriteriaportal.org/

[29] Volkamer, M. and Vogt, R. 2008. *Basic set of security requirements for online voting products*. Common Criteria Protection Profile BSI-PP-0037, 2008. Online available http://www.bsi.de/zertifiz/zert/reporte/pp0037b.pdf

[30] ISO/IEC 27001: *Information technology – Security techniques – Information security management systems – Requirements*. Online available http://www.27001-online.com

[31] ISO2: ISO. Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems , 2011.

[32] Weber; J. and Hengartner, U. 2009; *Usability study of the open audit voting system helios.* Online available http://www.jannaweber.com/wp-content/uploads/2009/09/858Helios.pdf