Practical Security of Large-scale Elections: An Exploratory Case Study of Internet Voting in Estonia

Guido Schryen

International Computer Science Institute, Berkeley CA 94704, USA,
schryen@gmx.net,
WWW home page: http://www.icsi.berkeley.edu/~schryen/

Abstract. The Estonian parliamentary election in 2007 is regarded as a success story of large-scale Internet elections. I use this election in a single case study on practical security to show that low quality of security and its management does not necessarily prevent large-scale Internet elections from being conducted. I also provide research propositions with regard to future challenges for large-scale Internet elections.

Key words: Internet voting, large-scale election, Estonian parliamentary election, security, security management

1 Introduction

In the course of the recent development of electronic democracy, electronic voting has drawn remarkable attention. Beyond direct recording electronic (DRE) voting machines in designated polling places, remote electronic voting (Internet voting) has come into consideration, and it even reached for governmental elections on the national level in Estonia first [23]. With that event, Internet voting has finally reached the stage of international attention even though experts warned three years earlier in the SERVE report that the Internet is not ready for elections yet [17]. According to Krimmer [19], *"[...] most other nations are still in the phase of experimentation, while most trials do not follow classical experimental setups [2] and are embedded in their national context [32], which makes it hard for comparison and learning from others."* An overview of more than 100 elections with remote e-voting option [19] shows that while remote e-voting has arrived at the regional level, at the national level it is a very rare phenomenon.

Internet voting has turned out to be challenging for two different reasons: First, in the presence of threats due to denial-of-service (DoS) attacks, malware distribution and botnets, tools and infrastructures for large-scale attacks against Internet voting systems are available. Second, procedures related to traditional e-Commerce are limited in their applicability on Internet voting because of their very different nature [17]:

- Elections are inseparably linked to democracy and malfunctioning election processes can directly and decisively influence it. Democracy relies on broad confidence in the integrity of elections. Thus, Internet voting requires a higher security level than e-Commerce does.
- It is not a security failure if your spouse uses your credit card with your consent, but the right to vote is usually not transferable.
- A DoS attack might occur and prevent consumers from performing e-Commerce transactions. However, generally there is a broad time window and once DoS attacks have been detected and mitigated, business can be transacted. In the context of Internet elections, a DoS attack can result in irreversible voter disenfranchisement and the legitimacy of the entire election might be compromised.
- Business transactions require authentication by sending passwords, PINs, or biometric data. In the context of Internet voting, however, authentication procedures shall only be applied to voter registration and voter authorization. The transaction (vote polling) itself requires anonymity. This duality leads to the requirement of implementing much more complex security procedures, be they organizational or technologic.
- People can detect errors in their e-Commerce transactions as they have audit trails: they can check bills and receipts and when a problem appears recovery is possible through refunds, insurance, or legal action. Vote receipts (showing the vote decision) must not be made out, as otherwise votes can be paid and extortion might occur.

Apparently, security issues are a main concern of researchers, practitioners and politicians. But although numerous security procedures for Internet voting have been proposed, there is only a few documents (e.g. [20, 24]) that analyze security of real, large-scale Internet elections. In compliance with the objectives of the Web 2008 workshop - to discuss success stories and lessons learned and to map out major challenges - the overall goals of this work are to explore how election security has been practically considered in the past and to deduce implications for the prospective implementation of secure large-scale Internet elections. This leads to the following research questions:

1. What was the role of IT security and its management in large-scale Internet elections?
2. What are future challenges for secure large-scale Internet elections?

The type of these research questions methodologically calls for an exploratory case study analysis, with the large-scale governmental election in Estonia being considered as case.

I present my single case study following a linear-analytic structure, as proposed by Yin [36, pp. 151ff]: In Section 2, I provide the theoretical background of my work, including a brief literature review. Section 3 substantiates single-case study as an appropriate research methodology and presents a precise description of my methodology. Section 4 contains the exploration of the Estonian case. In

Section 5, I provide an analysis of the case aiming at answering the research questions and at generalizing to theoretical propositions for the prospective consideration of security issues in large-scale elections. I conclude my work in Section 6 with an outlook on the role of security in prospective large-scale Internet elections.

2 Theoretical Background

As the description and the analysis of the Estonian case study is guided by a theoretical framework, I briefly provide the theoretical background of the different parts of this framework. These parts refer to (core) security and the security related issues of usability, transparency, quality and the electoral process.

2.1 Security

Security issues are considered most relevant in the discussion of electronic voting in general and Internet voting in particular. Based on characteristics of systems described in the literature, Cranor [7] formulates desirable characteristics for Internet elections, the directly security-related ones being as follows: a) accuracy: votes must not be altered or eliminated, invalid votes must not be counted, and the vote tally must be correct, b) democracy: eligible voters can vote, but only once, c) privacy: a link between cast and voter must be impossible, and the voter must not be capable of proving that s/he voted in a particular way, d) verifiability: anyone can independently verify the correctness of the vote tally. Schryen [29] proposes a theoretical framework, in which security requirements are derived from other, non-technological requirements, such as legal, economic and ergonomic ones.

Many technological voting protocols have been proposed, most of which are based on cryptography. One of the earliest protocols that rely on two agencies, an electronic validator and a tallier, was proposed by Nurmi et al. [21]. Based on blind signatures [5] is the two agency protocol [13], which was expanded in the Sensus system [8], that introduces a pollster, a third agency acting as a voters' agent. Protocols that address (the first part of) privacy by means of a "mix net" [6] are proposed by Jakobsson et al. [16] and Juels et al. [18]. Approaches that focus the second part of privacy, being designed to make voting receipt-free, are proposed by Benaloh and Tuinstra [3], Sako and Kilian [28], Okamoto [22], and Hirt and Sako [15].

Another critical part of the overall voting infrastructure is the users' end devices. The importance of the protection of such devices is stressed in the SERVE report, where Jefferson et al. [17, p. 3] argue that an *"[...] Internet- and PC-based system [...] has numerous other fundamental security problems that leave it vulnerable to a variety of well-known cyber attacks (insider attacks, denial of service attacks, spoofing, automated vote buying, viral attacks on voter PCs, etc.), any one of which could be catastrophic."* The following methods have

been proposed to overcome the challenge of insecure voting devices [33]: voter manual regarding security measures, voting operating system, trusted computing elements, and code sheets.

2.2 Further Security Related Issues

The following issues seem to be relevant to security:

- *Usability*: The voter needs some kind of software and hardware to communicate with the server and to run the voting protocol. The most accessible implementation requires only a web browser, with either only SSL being enabled or, additionally, Java being enabled; further advanced approaches provide specific voting software, which needs to be installed. Depending on the authentication technique in place, in addition to software also hardware, such as a card reader, might be required to be available to the voter.
- *Transparency*: As the Internet voting system as a whole is probably not understood by most voters, it is necessary to implement procedures that increase transparency. This can be done by providing verifiability and open access to all information about the election and its procedures. According to Pieters [25], the following types of verifiability can be distinguished: *individual verifiability* allows voters to verify whether their votes have been counted, and *universal verifiability* allows anyone to verify the overall correctness of the tally. During the development of the election system and the election itself many documents including the source code and procedural documents are generated. The access to these documents can be generally permitted, allowed for particular groups, such as evaluators and observers, allowed for everyone (at a particular place after having signed a non-disclosure agreement), or allowed for everyone by making this documents public (e.g. on the Internet).
- *Quality Management*: There exist several options to ensure the quality of the technologic election system and the processes. The most popular ones are test elections (the voter can practice and get used to it), system evaluations (either by a security experts or according to a security standard like the Common Criteria), audits of the election procedures, or observations made by independent authorities.
- *Electoral Process*: The electoral process consists of two mandatory phases, complemented by an optional, third phase:
  1. Registration phase: In order to electronically check the user's eligibility to cast a ballot, an electronic version of the electoral register is required. This register can either be generated in the registration phase, in which those voters who want to cast their vote electronically apply and are thus added to the register, or by integrating the existing registers into a single one.
  2. Voting Phase: Voting is either enabled only before the election day, only on the election day, or during both periods.
  3. Vote Updating: An Internet voting system can support vote updating: for different implementation options see [34]. Thus a voter who casts his vote but is coerced, distrust her device, or changes his mind can update her vote

later again, either using the same or a different electronic device, or even paper.

3 Methodology

I approach methodology in two parts. The first part describes why I choose to select case study as research strategy. The second part explains how I apply case study research in order to answer the research questions.

3.1 Research Strategy

As my approach is to choose research methodology problem-driven, I need to match the research questions with the characteristics of different research methodologies. The research questions, stated in the introduction and aiming at identifying (a) the role of IT security in large-scale Internet elections (b) future challenges for secure large-scale Internet elections, are of multidisciplinary nature and embedded in a multi-faceted social context. In order to appropriately consider the multi-facets of this context, I explored research methodology of the social sciences and considered as relevant research strategies the "experiment", "survey", "archival analysis", "history" and "case study". With regard to the latter research strategy, an early, conventional view was that a case study is not a valuable research methodology, as a case study cannot provide reliable information about the broader class [1, 4]. However, during past years the acceptance of case study methodology as a necessary and sufficient method for many important research tasks has increased [27, 31, 35, 36]. More precisely, I follow the arguments of Flyvbjerg [12], who shows in his literature synthesis that (1) general, theoretical (context-independent) knowledge is not necessarily more valuable than concrete, practical (context-dependent) knowledge, (2) one can generalize even on the basis of individual cases so that the case study can contribute to scientific development and (3) it is often not difficult to summarize and develop general propositions and theories on the basis of specific case studies.

Adopting the case study definition of Yin's [36, p. 13f] seminal work (see Definition 1), we find a good match between what is studied (large-scale Internet elections) and what can be investigated by using a case study, thereby identifying case study research as one candidate for methodology. However, we also need to consider the appropriateness of other research strategies. Thereto, I apply the methodological framework proposed by the COSMOS corporation and elaborated by Yin [36, Chapter 1], according to which the appropriateness of a research strategy depends on the "values" of three attributes: (1) the form of research question, (2) the control of behavioral events, and (3) the focus on contemporary events. As our research (1) poses what and how questions, (2) does not allow for controlling or manipulating behavioral events (elections) and (3) focuses on contemporary elections, in accordance with this framework, I choose to select case study as research methodology.

Definition 1. *"Case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident.* [...] *The case study inquiry copes with the technically distinctive situation in which there will be many more variables of interest than data points.* [...]*"*

Having identified the case study as appropriate research method, now the case study design has to be specified.

3.2 Case study design

The design of the case study is based on the suggestion of Yin ([35, Chapter 1] and [36, Chapter 2]), who regards the following components as important:

- Determination of the specific type of case study
- Definition of the study's questions
- Development of a theoretical framework
- Case selection
- Providing criteria for interpreting the findings

Type of Case Study. According to Yin [35, 36], the type of case study is determined by three decisions:

1. Is the research exploratory, explanatory, or descriptive?
2. Does the research cover a single case or several cases (multiple case study)?
3. Does the study follow an embedded or holistic design?

I now briefly answer these questions with regard to this research: (1) While a descriptive case study presents a complete description of a phenomenon within its context and an explanatory case study presents data bearing a cause-effect relationship, an exploratory case study mainly focuses what questions and is aimed at developing pertinent hypotheses and propositions for further inquiry. In accordance with the research questions, I therefore apply an exploratory case study. (2) To explore practical election security in detail, it is advisable to choose cases, which are embedded in an innovative environment, which implement comprehensive security procedures, and for which sufficient data is available. To my best knowledge, this set of conditions is met only by the Estonian parliamentary election, which took place in 2007. Consequently, I select to consider only this case, resulting to a single case study. (3) If we need to address several units of analysis in the same context, the case study is denoted as embedded. Otherwise, the case study is holistic. As we have only on unit of analysis (one election), my case study is holistic.

Research Questions. The study's research questions are

1. What was the role of IT security and its management in large-scale Internet elections?
2. What are future challenges for secure large-scale Internet elections?

Theoretical Framework. In an exploratory case study, the theoretical framework should specify what is being explored, thereby guiding the description and analysis of the case. The framework provides a level at which empirical results of the case study are compared and at which the generalization of the case study results will occur. In order to address the research questions, the case is being explored with regard to security, quality, usability and transparency of the electoral process.Overall, for the Estonian case I explore

- what electoral environment was present,
- how the holistic electoral process was conducted with particular regard to the integration of anonymity and identification, which are core concepts of governmental elections,
- how technical and organizational security measures were implemented,
- what audits, tests and evaluations were conducted to assure quality,
- how usability (for voters) was determined through the usage of hardware and software, and
- how transparency in terms of verifiability and accessibility was assured.

Case Selection. The selection of cases in case study methodology does not focus on statistical sampling but much rather on theoretical sampling. This term was introduced by Glaser and Strauss [14] where they aim to gain a deeper understanding of analyzed objects in contrast to studying all possible variations of an object. This can be seen as a collection of independent pieces of information to get a better understanding of a thing that is only known in part [26].

For my case selection, I need to cope with the fact that the number of uses of Internet voting in large-scale Internet elections to date is limited [19]. As already mentioned above, the Estonian parliamentary election is the only one of these, for which sufficient data is available. Estonia is the first (and only) country worldwide to introduce legally-binding, nation-wide Internet voting without any preconditions.

Interpreting the Findings. The interpretation of the findings is intended to answer the research questions. This analysis will be done by investigating to what extent the technologic state-of-the-art in terms of security was implemented, to what extent security management was implemented, and how election security was perceived by different stakeholders.

4 The Case: Parliamentary Elections in Estonia

This case study refers to the 3 March 2007 parliamentary (Riigikogu) elections in Estonia, which was the first parliamentary election in the OSCE area in which voting by Internet was available (but not obligatory) to all eligible voters in order to increase voter turnout. The exploration of this election is based on publicly available reports of the OSCE Office for Democratic Institutions and Human Rights (ODIHR) [23], the European Union Democracy Observatory [11] and the Estonian National Electoral Committee [9, 10]. For a brief overview of political issues see [30].

4.1 Electoral Environment

In the Estonian electoral system, the country is divided into 12 multi-mandate electoral districts. Political parties compete for the 101 parliamentary mandates distributed in an electoral district by registering with the National Election Committee (NEC) the lists of candidates for each electoral district contested. To cast a ballot, voters write the registration number of the candidate of their choice on the ballot when voting by ballot paper or mark the name of the preferred candidate when voting by Internet. Voters were offered different options to use advance paper ballot voting, voters could cast their ballot in polling station at the day of election, and voters could cast their ballot in advance through the Internet (due to an amendment of the Riigikogu Election Act). The law permitted voters to change their votes during the advance voting period, either by voting again through the Internet or by casting a ballot paper at a polling station. The voter could change his/her vote an unlimited number of times electronically, with the last ballot cast being the only one counted, but a vote cast by paper is final and annuls all Internet votes cast by the voter. Voters who casted a vote by Internet were not allowed to cast a vote on election day itself.

4.2 Usability

The technical cornerstone of the Internet voting system in Estonia is the use of a personal identification document (ID card), which is already legally accepted for identification via the Internet and to sign documents digitally. The computer used by the voter must have a smart card reader installed in order to process the digitally-enabled ID card, as well as two PIN codes associated with the ID card. Installation software must be downloaded. With regard to the user's Voting Application, voters using Microsoft Windows (98.9%) use a web browser, while for voters who use Mac OS (0.75%) or Linux (0.42%) the voting interface is a stand alone program. The voting interface itself is only available in the Estonian language.

4.3 Electoral Process

In the course of general voter registration, the distribution of designated voting cards, PIN codes, keys or certificates for Internet voting was not necessary, because the already deployed Estonian ID card contains a user-specific certificate and a private key on an embedded chip. Together with two PIN codes, the card allows the holder to authenticate and digitally sign during the Internet voting process. This voting process is displayed in Figure 1 and involves the following steps:

1. The *Voter Application* requests data from the voter's ID card. To proceed, the voter types a personal code (PIN1) to identify her/himself. Through an SSL connection between the *Internet Server* and the voter's computer, the *Voter Application* checks whether the voter is on the voter list.

2. The voter chooses one candidate by clicking on the name of the candidate and then confirming the choice. Unlike the paper balloting, the system does not allow voters to cast a blank ballot or to spoil their ballot.
3. The vote is encrypted with the public key of the *Counting Server*. In order to cast the vote, the voter must type in a second personal code (PIN2). This code is the confirmation that it is the voter him/herself who is voting. The PIN2 enables the card to sign the encrypted vote.
4. The encrypted vote is then sent to the *Internet Server* which checks whether the digital signature corresponds to the session owner.
5. The Internet Server then forwards the encrypted vote to the *Vote Storage Server*, which requests a check of the validity of the voter's certificate from the *Certification (Authority) Server*. If valid, the *Internet Server verifies* the digital signature using the voter's public key from the voter's certificate.
6. At the end of the voting process, the voter receives an on-screen confirmation that the vote has been cast. The encrypted vote remains on the *Vote Storage Server* until counting and tabulation is performed on election day.

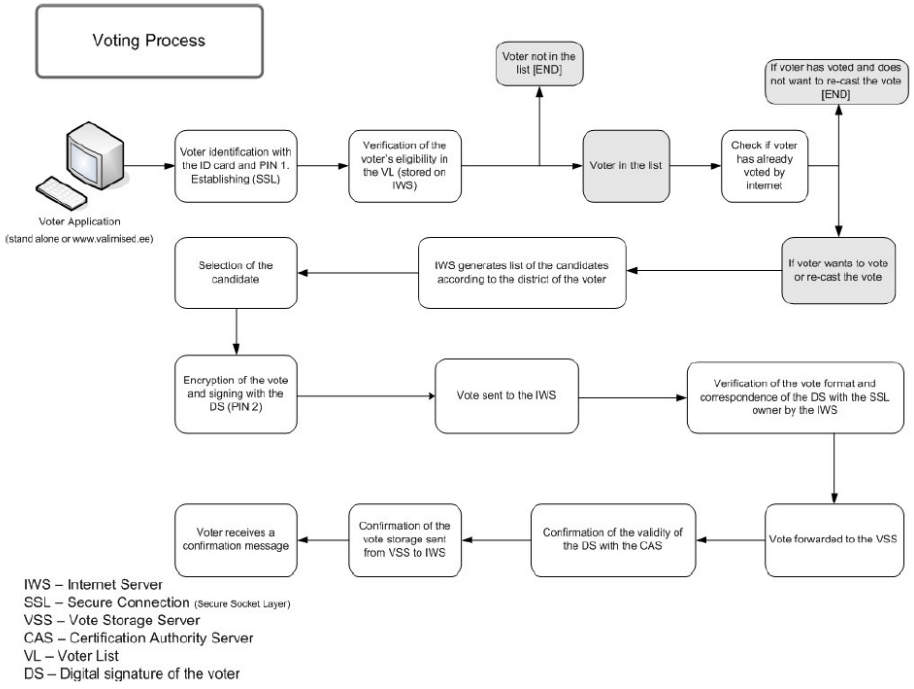

Fig. 1. Internet voting process in Estonia's 2007 parliamentary elections; source: [23, Annex 2]

As voters could select advance ballot voting in addition to Internet voting, a consolidation of votes needed to be conducted: After receiving lists from polling

stations regarding any voters who cast a paper ballot during advance voting and who also cast a vote by internet, NEC staff mark the corresponding electronic votes on the *Vote Storage Server* as "not to be counted". The process of canceling votes is logged. The advance paper ballot is counted in the normal counting process. Finally, the NEC staff burns a CD from the *Vote Storage Server* that contains the last electronic vote of each voter. This CD is sealed and given to the Chairman of the NEC.

The counting of the electronic votes takes place on election day, one hour before the closing of the polling stations:

1. The encrypted votes are transferred to the *Counting Server* by a CD-ROM. All entries transferred to the *Counting Server* are logged. The *Counting Server* decrypts the votes using the *Hardware Security Module (HSM)* and counts them. In order to enable the *HSM*, six physical keys must be inserted. By law, at least half of the NEC members must be present in order to decrypt and count the votes.
2. After the votes are counted on the *Counting Server*, a new CD is burned with the results. The CD is taken to a personal computer where the results are processed so that they can be viewed in a spreadsheet.

4.4 Security

The core security architecture of the Internet voting system is based on the separation of the *Vote Storage Server* connected to the Internet and the offline *Counting Server*. With regard to specific security prerequisites, the following provisions were taken:

- The installed voting software was checked to ensure that it was identical to the software received.
- There is a firewall between the *Internet Server* and the *Vote Storage Server*.
- Traffic to the *Internet Server* was monitored by system operators to attempt to identify any abnormalities or external attacks.
- The *Internet Server* and the *Vote Storage Server* were located in a locked room which was guarded by a policeman and continuously filmed. In addition, these servers were sealed.
- To ensure the availability of the election results in the event of failure of the *HSM*, there was a backup of the private key which was kept secret by one of the members of the NEC.
- To limit the likelihood of attacks to voters' computers, the NEC advised voters to type in the correct IP web address, published the server certificate and provided information to the voter to verify whether he/she has the proper voting application.

4.5 Quality

There was no obligation to certify or test the system, the Internet voting system was not officially certified by an independent body and no full end-to-end logic

and accuracy test were performed on the system. The auditing was conducted by an external auditing company, which monitored and checked the activities of the NEC against written documentation, which describes the necessary steps and procedures. In addition to the formal auditing, all of the above steps were videotaped. However, the final report is not public, and the external auditing company was not requested to conduct any post-election audits. It is not clear to what extent the voting software was formally audited after being received from the company.

4.6 Transparency

Main characteristics of the Estonian Internet voting system are that (1) no "Voter Verified Paper Audit Trail" as an independent verification system was implemented so that the voter receives no proof that his/her vote has been counted (correctly) and (2) the separation of voter's decision and identity is realized at organizational level, not providing the voters any option to monitor this separation.

The NEC stated that all political parties and accredited observers were invited to observe the administration of Internet voting in every phase of the process, including the opportunity to review the documentation of the system, the source code of the software, and all of the setup procedures in the process. However, overall, there appeared to be no oversight of the Internet voting process by political parties or civil society.

5 Analysis

In this section the Estonian election is analyzed with regard to the extent the technologic state-of-the-art in terms of security was implemented, to the extent security management was implemented, and how election security was perceived by different stakeholders.

For authentication and confidentiality, strong cryptographic solutions based on digital signatures and a public key infrastructure were used. However, voters used their PCs with card readers attached, and possible threats against these PCs were neglected. For example, web side spoofing and malware, which makes the card reader sign other data than displayed on the screen, were not seriously addressed or even not considered. Anonymity was established in the post-election period (the encrypted votes are linkable to voters) at organizational level: links were removed before decrypting the votes. No designated e-voting protocols were applied. Even worse, the voters got no proof of the separation of their decision and their identity. As no voter verified paper audit trail was implemented, voters did not know whether their vote had been correctly counted. Summing up, the Estonian election did not implement or seriously consider designated protocols provided in the e-voting literature.

Although some general IT security provisions were taken, these were kind of ad-hoc approaches, as the Riigikogu Election Act does not contain specifications

of the Internet voting system, does not foresee the responsibility of any institution, and does not provide for sanctions in case of failure of the system. Main concerns about the security quality of the Internet voting system are raised in the report of the OSCE/ODIHR Election Assessment Mission team [23]. For example, if the *Certification Server* were to fail or be unavailable, voting by Internet would not function. Furthermore, there did not appear to be a formal plan to monitor network traffic and to deal with the risk of DoS attacks against the *Internet Server*.

According to [23], there was no obligation to certify or test the system. The Internet voting system was also not officially certified by an independent body and no full end-to-end logic and accuracy test was performed on the system. Although some auditing was conducted by an external auditing company, the final report is not public. Even worse, the external auditing company was not requested to conduct any post-election audits. Overall, the security management was at a poor level. Taking this essential weakness into consideration, the fact that no security incidents have been reported does not mean that none occurred.

Although the overall level of security (management) was quite poor, no severe complaints were reported. The election and its security (management) seem to have been broadly accepted by voters, politicians, and election officials. This might be due to the fact that this Internet voting project was a milestone project.

Having addressed the first research question, I now formulate the research propositions, which are intended to be a starting point for further research:

1. Low quality of security (management) does not necessarily prevent authorities to conduct Internet elections for the sake of technologic leadership.
2. The propagation of carelessness with regard to security would attract serious large-scale attacks against Internet elections, once the voter turnout increases.
3. The diffusion and adoption of large-scale Internet elections will fail, unless profound knowledge about the implementation of sophisticated e-voting protocols and infrastructures as well as comprehensive and transparent security management is available.

6 Conclusions and Outlook

The Estonian election analyzed in this paper shows that the implementation of secure large-scale Internet elections is still a hard task, even in a highly innovative environment. It remains a future challenge to bridge the gap between what has been proposed in the literature and what is implemented in practice. In addition to conducting research along the propositions of this paper, the implementation of further pilot projects and comprehensive testing seem preconditions for any further adoption of Internet voting. Although the Estonian case is regarded as a success story in the press, serious security (management) concerns raise the question whether such elections are useful for the prospective adoption of Internet voting.

Acknowledgments. This work was supported by a fellowship within the Postdoc-Programme of the German Academic Exchange Service (DAAD).

References

1. Abercrombie, N., Hill, S., Turner, B. S.: Dictionary of sociology. Penguin, Harmondsworth (1984)
2. Alvarez, R. M., Hall, T.: Point, Click, & Vote. Brookings Institution Press, Washington, D.C. (2004)
3. Benaloh, J., Tuinstra, D.: Receipt-free secret-ballot elections. In: STOC 1994, pp. 544–553 (1994)
4. Campbell, D. T., Stanley, J. C.: Experimental and quasi-experimental designs for research. Rand McNally, Chicago (1966)
5. Chaum, D.: Blind signatures for untraceable payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) Crypto 82, pp. 199–203 (1983).
6. Chaum, D.: Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. CACM (24:2), 84–88 (1981)
7. Cranor, L.F.: Electronic Voting: Computerized polls may save money, protect privacy. ACM Crossroads Student Magazine (2:4) 1996
8. Cranor, L.F., Cytron, R.K.: Sensus: A Security-Conscious Electronic Polling System for the Internet. In: HICSS 1997, pp. 561-570 (1997)
9. Estonian National Electoral Committee: Main Statistics of E-Voting, http://www.vvk.ee/english/Ivoting comparison 2005_2007.pdf (2007)
10. Estonian National Electoral Committee: Parliamentary elections 2007: Statistics of e-voting, http://www.vvk.ee/english/Ivoting_stat_eng.pdf (2007)
11. European Union Democracy Observatory: Report for the Council of Europe: Internet Voting in the March 2007 Parliamentary Elections in Estonia, http://www.vvk.ee/english/CoE and NEC_Report E-Voting 2007.pdf (2007)
12. Flyvbjerg, B.: Five Misunderstandings About Case Study Research. Qualitative Inquiry (12:2), 219–245 (2006)
13. Fujioka, A., Okamoto, T., Ohta, K.: A Practical Secret Voting Scheme for Large Scale Elections, In: Seberry, J., Zheng, Y. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 244–251. Springer, Berlin, Heidelberg (1993)
14. Glaser, B., Strauss, A.: The discovery of grounded theory: Strategies for Qualitative Research. Aldine, New York (1967)
15. Hirt, M., Sako, K.: Efficient receipt-free voting based on homomorphic encryption. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 539–556. Springer, Berlin, Heidelberg (2000)
16. Jakobsson, M., Juels, A., Rivest, R.L.: Making mix nets robust for electronic voting by randomized partial checking. In: USENIX Security Symposium 2002, pp. 339–353 (2002)
17. Jefferson, D., Rubin, A.D., Simons, B., Wagner, D.: A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), http://www.servesecurityreport.org (2004)
18. Juels, A., Catalano, D., Jakobsson, M.: Coercion-Resistant Electronic Elections. In: De Capitani di Vimercati, S., Dingledine, R. (eds.) WPES 2005, pp. 61–70. ACM Press, New York (2005)

19. Krimmer, R., Triessnig, S.,Volkamer, M.: The Development of Remote E-Voting Around the World: A Review of Roads and Directions. In: Alkassar, A., Volkamer, M. (eds.) VOTE-ID 2007. LNCS, vol. 4896, pp. 1–15. Springer, Berlin, Heidelberg (2008)
20. Mohen, J., Glidden , J.: The Case for Internet Voting. CACM (44:1), pp. 72–85 (2001)
21. Nurmi, H., Salomaa, A., Santean, L.: Secret ballot elections in computer networks. Computers and Security (36:10), pp. 553–560 (1991)
22. Okamoto, T.: Receipt-free electronic voting schemes for large scale elections. In: Christianson, B., Crispo, B., Mark, T., Lomas, A., Roe, M. (eds.) Workshop on Security Protocols 1997. LNCS, vol. 1361, pp. 25–35. Springer, Berlin, Heidelberg (1997)
23. OSCE: OSCE/ODIHR Election Assessment Mission Report in the 2007 parliamentary elections in Estonia, http://www.vvk.ee/english/OSCE report_EST_2007.pdf (2007)
24. Philips, D.M., von Spankovsky, H.A.: Gauging the Risks of Internet Elections. CACM (44:1), pp. 73–85 (2001)
25. Pieters, W.: What proof do we prefer? Variants of verifiability in voting. In: Ryan, P. (ed.) Proceedings of the Workshop on Electronic Voting and e-Government in the U.K., http://www.cs.ru.nl/∼wolterp/Verifiability.pdf (2006)
26. Punch, K. F.: Introduction to Social Research: Quantitative and Qualitative Approaches. Sage Publishing, London (2005)
27. Ragib, C. C., Becker, H. S. (eds.): What is a case? Exploring the foundations of social inquiry. Cambridge University Press, Cambridge (1992)
28. Sako, K., Kilian, J.: Receipt-free Mix-type Voting Scheme. In: Guillou, L., Quisquater, J.-J. (eds.) EUROCRYPT 1995. LNCS, vol. 921, pp. 393–403. Springer, Berlin, Heidelberg (1995)
29. Schryen, G.: Security Aspects of Internet Voting. In: HICSS 2004 (2004)
30. Solvak, M., Pettai, V.: The parliamentary elections in Estonia, March 2007. Notes on Recent Elections/Electoral Studies (27:3), 547–577 (2008)
31. Stake, R.E.: The art of case study research. Sage Publications, Thousand Oaks, London (1995)
32. Svensson, J., Leenes, R.: E-Voting in Europe: Divergent democratic practice. Information Polity (8:1-2), 3–15 (2003)
33. Volkamer, M., Alkassar, A., Sadeghi, A.-R., Schultz, S.: Enabling the Application of Open Systems like PCs for Online Voting. In: FEE 2006, http://fee.iavoss.org/2006/papers/fee-2006-iavoss-Enabling_the_application_of_open_systems_like-PCs_for_Online_Voting.pdf (2006)
34. Volkamer, M., Grimm, R.: Multiple Cast in Online Voting – Analyzing Chances. In: Krimmer, R. (ed.) Electronic Voting 2006. LNI, vol. 86, pp. 97–106. Springer, Berlin, Heidelberg (2006)
35. Yin, R.K.: Applications of case study research, 2nd ed. Sage Publications, Thousand Oaks, London, New Delhi (2003)
36. Yin, R.K.: Case study research: design and methods, 3rd ed. Sage Publications, Thousand Oaks, London, New Delhi (2003)