E-DEMOCRACY: INTERNET VOTING

Dr. Guido Schryen
Department of Economical Computer Science und Operations Research, University of Technology Aachen
Templergraben 64,52062 Aachen, Germany
schryen@winfor.rwth-aachen.de

ABSTRACT

Voting via the Internet is part of electronic government and electronic democracy. However, there are many obstacles which have to be overcome, especially legal restrictions have to be transformed into technical and security solutions. In the first part the article discusses advantages and disadvantages of Internet elections, shows different application fields, and presents important international pilot schemes (political and business ones). In the second part, due to democratic basic principles, technological security aspects are worked out.

KEYWORDS

Internet Voting, Online polls, E-Democracy, Security

1. INTRODUCTION

This article focusses on technological security needs of Internet elections as part of E-Democracy. These needs exist just due to constitutional law principles. However, not only political online elections are regarded, but also ballots in universities, for staff councils, in shareholder meetings, etc. The objectives are twofold: (1) giving a descriptive overview of the landscape of worldwide online elections and (2) working out technology oriented security aspects due to democratic basic principles in order to execute legally accepted online polls. First, substantial arguments of proponents and opponents of the Internet elections are presented, so that the reader may recover his own poise already here. Subsequently, application fields and precise pilot projects are presented. Finally, due to democratic basic principles technological security aspects are worked out.

2. PROS AND CONS

Substantial general arguments for the implementation of online elections are the following ones:

Increasing turnout: To what extend a significantly higher election turnout can be achieved, has not been sufficiently empirically examined so far. Even if voter turnout information about several pilot projects was published, it is difficult to interpret these very numbers, since (1) it is unknown how many voters would have otherwise casted their vote traditionally, and (2) these numbers have to be adjusted to temporary effects due to advertisement and press coverage. The online election´s influence on the turnout will probably not only depend on the kind of poll, but for example also on the respective cultural, political and geographical conditions: Australia´s low population density, Greece´s demand to select in one´s birth municipality, and the political establishment of referendums in Switzerland are crucial characteristics.

Cost reduction: Cost savings can occur, if less personnel for performing absentee voting and for counting is necessary or if travel activities are reduced. On the other hand building up and operating the poll infrastructure as well as equipping the voters with essential hardware cause cost. Furthermore, in the foreseeable future of political elections no polling stations will become obsolete. The discussion whether and at which elections cost savings will occur is presently speculative.

Decrease of invalid votes: Invalid votes can be produced consciously or unconsciously. Consciously producing invalid votes are presumably protest against politics in general, therefore they must be provided in online elections. Unconsciously produced invalid votes could be already identified at “feeding time“ with plausibility checks, so that the voting software could point out this mistake. This means a difference to traditional polling booths. Whether this kind of restricting the democratic “principle of equality” is tolerable has to be examined legally.

Lower election fraud in endangered countries: The security of traditional elections bases on the confidence in persons and in the independence of election committees. In endangered countries with young democracies the confidence in these mechanisms is lower, and a shift from organizational security precautions to technical ones (e.g. cryptographic coding) might be helpful. However, it it necessary to mention that the coexistent use of organizational and technical security precautions features a gradual character, i.e. the securest technology can always be annulled, if all organizational units involved cooperate corruptingly.

Support of basis democracy: As soon as an Internet-based poll infrastructure is built up basis-democratic voting processes become more feasible.

On the other hand there is strong concern about online elections:

Security: Ranking first is security doubt. In traditional elections it is obvious for anyone that a mapping of voters on the votes is impossible, because the voting process itself takes place behind physical barriers and each voter drops his “locked“ envelope into the voting box. The voter himself monitors the adherence of the principle of secrecy. However, regarding absentee voting which is socially, political and legally accepted this looks different: There is no guarantee to the voter that his vote won´t be changed, he just trusts in the integrity of the involved persons and organizations as well as in the sanctity of the mail. These and many further aspects of election security like the warranty of the ballot paper´s “arrival” don´t come up to discussion.

The Internet Voting Task Force (2000) is concerned about the security of computer clients, as the presence of worms, viruses and Trojan horses can not be sufficiently surely excluded.

Low Transparency: Obviously, implementing security requirements with information technology is not trivial, even if cryptography offers a rich bundle of methods and instruments. Anyway, using complex security procedures leads to increased intransparency to the voter, so that problems regarding elector´s acceptance are likely.

Cost: It is yet unknown, to what extend and when cost for establishing and operating an Internet-based poll infrastructure redeems. Disputants of Internet elections deny its´ potential to medium-term cost savings.

3. APPLICATION FIELDS AND PILOT SCHEMES

Seminal application fields for online elections are especially large-scale ballots with a tremendous organizational work. Polls in small communities like schools or for municipal councils are regarded to a lesser extend, rather political elections like diet elections, elections to the German Bundestag, referendums, or EU elections, polls within a corporation (workers’ council, board of directors), votes at stockholders´ meetings or other annual meetings, or committee elections at universities and schools. Remarkably there is a broad consensus that political online voting is not meant to be substitutional rather complementary to traditional voting procedures. There is no such consensus about non-political polls. There are several ways to execute Internet votes. The California Internet Voting Task Force (2000) differentiates the place from where the vote is casted via Internet, referring to a plan by stages: Vote via Internet at (1) a dedicated polling station, (2) any polling station, (3) a certified voting terminal (e.g. at a public place), or (4) from any access point. This article focusses requirements and experiences with stage no. 4. Due to their exceptional position and legal meaning political elections will be considered first. The pilot projects presented below do not claim completeness. However, the author thinks he pointed out the essential projects.

3.1 Political Elections

Security concerns are surely high when voting online within political range. Not only poll-specific laws must be observed but also constitutional principles. Up to now no such election has taken place in Germany. According to a statement of the current Federal Minister of the Interior Otto Schily polling stations (approx.

80,000 in Germany) shall be equipped with voting computers for the forthcoming election to the German Bundestag in 2006. The first Internet election is planned to take place in 2010 (Philippsen, 2002). In 2000 approx. 250 soldiers could use a “certified virus-free” computer to participate in the US-presidential election. Unfortunately, there is only few information about the Internet voting procedure (Philippsen, 2002). In 2000 about 40,000 entitled voters used the opportunity to cast their vote online during Democratic Party´s Presidential Primary election (Election.com, 2000; Mohen & Glidden, 2000; Philips & von Spankovsky, 2001). Several security problems occurred, e.g. denial-of-service attacks as well as the uncertainty of the voter, if his vote was really counted. In 2003 for the first time in Switzerland the Geneva suburb Anières accomplished an official Internet election within the scope of a municipal project; about 28% of the eligibles voters elected online (Geneva, 2003). To what extent this percentage just based on the innovative character and publicity is not known. Furthermore there is no information about emerged security problems.

3.2 Non-Political Elections

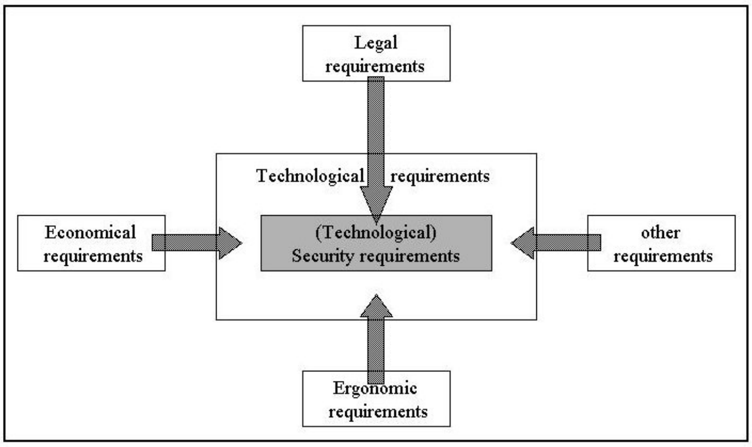
Elections at universities and schools are also classified as non-political ones although they might have a political facet. There have been already numerous pilot schemes in different countries and contexts. The “Forschungsgruppe Internetwahlen” supported by the Federal Ministry of Economics and Technology contributed some pioneer work in Germany and created a special voting software called i-vote. Several ballots have been accomplished with this software, for example in February 2000 the representatives for the student parliament at the University of Osnabrück could be voted electronically (Otten, 2001), and approximately 400 students voted via Internet. In May 2002 the workers’ representation at the LDS Brandenburg (state office for data processing and statistics) was elected by the workers only at dedicated voting terminals with special signature cards. These cards were intended to be used afterwards as part of the e-government programme in Brandenburg. Philippsen (2002) took a closer look at the student parliament election and identified some security problems. Furthermore he found fault that the exact procedure is still confidential and yet no source code has been published. With support of the German Federal Ministry of Economics and Work in 2002 the project W.I.E.N. (Elections in electronic nets) was initiated aiming at developing and testing online voting procedures in economy. Coexistently, the German Federal Ministry of the Interior tries for getting experience with political online elections. Internationally-active is the company election.com which accomplished numerous polls via Internet. Beside the Democratic Party´s Presidential Primary election the company was also assigned to execute an election for the English Sheffield City Council, for the Australian Information Industry Association (AIIA), and to the student parliament at the University of Technology in Auckland.

4. SECURITY REQUIREMENTS

Legal, political science based, and social requirements on elections are deep-seated in appropriate laws and have been primarily addressed with organizational measures so far. For example, physical barriers contribute to ballots´ secrecy and the legally prescribed temporal restriction of vote casting is implemented with opening times of the polling stations. Absentee voting already requires a special treatment and had to be legally anchored. In order to guarantee a ballot´s secrecy the sanctity of the mail was consulted, but the legal anchorage of Internet elections will probably become even harder. Information technology opens a new dimension, which has to accommodate legal general conditions. In other words, these basic conditions and laws must be technologically implemented in Internet elections. Technological efforts may not be an end in itself, but they make for implementation of those basic conditions. One can also call it a mapping of basic conditions on technological components. Beyond that further requirements occur, in particular economic and ergonomic ones, i.e. Internet elections should be as inexpensive and user-friendly as possible (see figure 1); already in 1996 Cranor formulated general requirements for electronic elections.

Figure 1 doesn´t show all dependencies, but the arrows indicate the most important ones.

Figure 1: System of requirements



The necessity to systematically analyze security requirements is substantiated by the security problems arisen in practical pilot schemes. The accurate security conditions depend on the concrete election. Nevertheless, at least the election-oriented democratic principles as fixed in the German "Grundgesetz" (constitutional law) can be consulted as starting point for the formulation of security-technological requirements. Supplementing, at each case further legal basic conditions are to be considered. It should be stressed that concrete security arrangements of an election aim at accomplishing a ballot-specific security level and that technology alone cannot solve the security problem: security is the result of organizational, legal, and technological measures. In the German "Grundgesetz" they say (translated): "In the counties and townships the people must have representatives which have been elected in general, direct, free, equal, and secret elections." They also say:" The representatives of the ´Bundestag´ are voted in direct, free, equal, and secret elections." Including the juridical-oriented discussion of Ruess (2000) one can bridge from law to technology:

General election: The basic principle "generality" assures the option to vote to all eligible voters. Since voting via Internet represents an additional way to voting, there seems to arise no problem. However, it has to be discussed whether the breakdown of technical system components limits the general right to vote, if five minutes before the end of voters´ time slot no connection to the polling server can be established due to its capacity overload. Thinking in terms of a client-server-architecture the following requirements result: On the client side the voting software and hardware (card reader, e.g.) must work properly. The voter is partially in charge for this, as he has to ensure that on its computer no disturbing software runs, which makes the network device fail, e.g. The same applies to the server side. One of the largest problems is the disturbance of a network connection basing on a (partial) Internet breakdown. For example, denial of service attacks can paralyze routers and polling servers. Yet, due to the coexistence of traditional voting channels the question whether such a reliability has to be guaranteed at all arises.

Direct election: The ballot´s directness means that between casting of votes and their counting only the mathematical determination may occur, thus no electors may be instituted. This is a matter of no importance in the context of Internet elections, even though the implementation of election processes has to fulfill this requirement.

Free election: According to this principle the poll procedure must not be affected by public force or private pressure. In this regard, to the Internet elections the same items and doubts apply as in case of absentee voting, because preventing an influencing control technologically is impossible. Lodging the claim that the voter receives a proof that his vote was counted unchanged one can think of a receipt mechanism, which however must not show the vote´s content. Lacking provableness is against extortion and paid votes.

Equal election: The principle of equality subsumes two aspects: (1) All voting cards are to be granted same status, so that those in the Internet must have the same appearance and the same structure as all other voting cards. Demanding the use of dedicated hardware (chip-card reader with integrated display and input device), consequently the same requirements are to be made against this hardware. Particularly, the voting card as a whole has to be displayed and may not be implicitly weighted by the "scrolling feature". (2)

Regarding the individual voter it must apply strictly that each vote has same weight. This means first that any eligible voter may only vote once (authentication is necessary). In order to implement authentication (and authorization) digital signatures can be applied. Secondly, it means that any vote has to be supplied unaltered (integrity). It must be assured that no malfunctioning or cankered software (viruses, worms, Trojan horses etc.) changes the vote notelessly. This can probably only be ensured if secure auxiliary hardware featuring a peculiar display and input device (e.g. keyboard) is applied. Moreover, the vote must not be corrupted during its transfer. For this purpose, proven cryptographic methods can be consulted. Furthermore, the vote must not be changed on any election server. Thirdly, the electronic vote may not be copied by anyone.

Secret election: The keeping of vote secrecy together with the consideration of equality and the aligned integrity belong to the most difficult tasks. In this regard, accepting absentee voting a compromise was already made. Compromising attacks can occur at the same spots already discussed above. The transmission of all data to voting servers must be encoded. On vote servers´ side is has to be ensured that no mapping from voter on his vote decision is possible. Beyond public key infrastructures this also requires organizational measures. For instance, there is a strict necessity to have at least two entities: a voting host controlling authorization and authentication, not being able to read the vote, making it anonymous, and forwarding votes to a voting box (or many) which just counts the (anonymous) votes.

5. CONCLUSION

During the past years many pilot projects were conducted, which examined Internet elections in different contexts with large commitment. Unfortunately, assigned procedures are often not disclosed probably for entrepreneurial reason. There is also a need for basic research, e.g. it is still open how casted votes should be receipted and which voting protocols should be used in which case. Furthermore there is a lack of appropriate methods for developing security standards and checking the implementation of security requirements.

Despite encouraging theoretical and empirical results research is still in its infancy and many problems will probably be detected first in the course of further pilot projects.

REFERENCES

California Internet Voting Task Force, 2000. Final Report Online. Available from <http://www.ss.ca.gov/executive/ivote> [Accessed 13 April 2003].

Cranor, L.F., 1996. Electronic Voting. Computerized polls may save money, protect privacy. In *ACM Crossroads Student Magazine* Vol. 2, No. 4, Available from <http://www.acm.org/crossroads/xrds2-4/voting.html> [Accessed 14 April 2003].

Election.com, 2000. Arizonans register overwhelming support for online voting. Online Vote More than Triples 1996 Returns. Available from <http://www.election.com/us/pressroom/pr2000/0312.htm> [Accessed 16 April 2003].

European Studentvote, 2002. Available from <http://www.eu-studentvote.org/> [Accessed 16 April 2003].

Geneva, 2003. Site officiel de l'Etat de Genève. Available from <http://www.geneve.ch/votations/20030119/resultats.html> [Accessed 13 April 2003].

Mohen, J., and Glidden , J., 2001. The Case for Internet Voting. In *Communications of the ACM,* Vol. 44, No. 1, pp. 72-85.

Otten, D., 2001. Wählen wie im Schlaraffenland? Erfahrungen der Forschungsgruppe Internetwahlen mit dem Internet als Wahlmedium. In: *Holznagel, B.; Grünwald, A.; Hanssmann, A. (Hrsg.): Elektronische Demokratie. Bürgerbeteiligung per Internet zwischen Wissenschaft und Praxis*. Beck. München, pp. 73-85.

Philippsen, M., 2002. Internetwahlen. Demokratische Wahlen über das Internet? In *Informatik Spektrum,* Vol. 7, No. 2 , pp. 138-150.

Philips, D.M., von Spankovsky, H.A., 2001. Gauging the Risks of Internet Elections, In *Communications of the ACM,* Vol. 44, No. 1, pp. 73-85.

Ruess, O.R., 2000. Wahlen im Internet. Wahlrechtsgrundsätze und Einsatz von digitalen Signaturen. In *MultiMedia und Recht,* Vol. 3, No. 2, pp. 73-76. Available from <http://www.Internetwahlen.de/ruess-ns.html> [Accessed 13 April 2003].