Security Aspects of 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 has become a feasible option for political as well as non-political ballots. However, there are many obstacles which have to be overcome, especially legal restrictions have to be transformed into technical and security solutions. The article starts with a brief presentation of advantages and disadvantages of Internet ballots and presents application fields and pilot schemes. Then, technological security aspects are derived due to democratic basic principles. Especially the applied voting procedures are critical in security terms. Hence, the most relevant cryptographic protocols are presented and their drawbacks and shortcomings are identified. However, this article does not propose a new voting protocol. Beyond fixing cryptographic procedures for ballots, more elements are to be specified, e.g. responsibilities and rights of involved authorities or security precautions regarding hardware and software. For this reason, a structural security framework for electronic voting systems is presented which can be used for their composition and analysis.

1. Introduction

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 second section the article discusses advantages and disadvantages of Internet elections. The third section shows different application fields, and presents important international pilot schemes (political and business ones). Due to democratic basic principles (general, direct, free, equal, and secret elections), technological security aspects are derived in section four. Especially the applied voting procedures are critical in security terms. Hence, the fifth section presents the most relevant cryptographic protocols also giving a brief overview about the most important general concepts of cryptography. Drawbacks and shortcomings of these protocols are identified showing the necessity to extend them or to develop new ones. However, this article does not propose a new protocol.

Beyond fixing cryptographic procedures for ballots, more elements are to be specified, e.g. responsibilities and rights of involved authorities or security precautions regarding hardware and software. For this reason, in section six a structural security framework for electronic voting systems is presented which can be used for their composition and analysis.

2. Pros and cons

Substantial general arguments for the implementation of online elections are the following ones [24]:

Increasing turnout: As Internet voting is an additional channel for eligible voters the turnout might increase substantially. Especially for older, handicapped, or sick people or those who cannot go or travel to their polling station it is a voting option.

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 (see section four). 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. For example, in the context of German political polls in any polling station at any time there are several persons belonging to different parties, and the counting takes place at another location by other people. 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 is 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 [24]:

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, which also contains the envelopes of many other voters. 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, probably for habit reasons or as they are implicitly sensed as realized. Rightfully, in the context of Internet polls security aspects are addressed again. The California Internet Voting Task Force [2] is concerned about the security of computer clients, as the presence of worms, viruses and Trojan horses can not be sufficiently surely excluded. Technological voting security is multi-faceted, section four addresses it more detailed.

In this context it is interesting to notice that the German Constitutional Court classified absentee voting as legal two times in 1967 and 1981 [18]), although it does not guarantee keeping the principle of secrecy to a degree traditional polls with voting stations do, because spouses or friends could watch them voting. Important to know is that (1) a conclusive prevention reason has to be present and (2) at the times of these decisions the portion of absentee voters was quite small (5-7%). If necessary a renewed examination is advised.

As Internet voting is a remote election procedure, too, it could be treated equally or similarly.

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 [2] 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)
4. from any access point

This article focuses requirements and experiences with stage no. 4.

Pilot projects in political and non-political environments have been accomplished [25]. Due to their exceptional position and legal meaning political elections will be considered first.

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 [18].

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 [18]. As mentioned above in 2000 about 40,000 entitled voters used the opportunity to cast their vote online during Democratic Party's Presidential Primary election [8]. This vote has been accompanied by election.com and was discussed in detail [15;19]. Several security problems occurred, e.g. denial-of-service attacks as well as the uncertainty of the voter, if his vote was really counted.

As mentioned above 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 eligible voters elected online [11]. 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 [17].

Philippsen [18] 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 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, and to the student parliament at the University of Technology in Auckland.

3.3. Security

Various activities in the field of online voting motivate a closer look at security requirements which have to be satisfied by such elections. On one hand not all security problems are published right away, on the other hand due to still moderate attacks some might have not been detected yet. With an increasing number of online elections these attacks will certainly become more seriously and systematically. For this reason the author pleads for numerous pilot projects with complete transparency of used procedures and infrastructures. Attack efforts should be explicitly welcome in order to identify weak points. In cryptology this proceeding worked outstandingly.

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).

In the context of integrating Internet elections in society and comprehensive requirements for them Kubicek et al. [14] use the expression "interdisciplinary connectivity". Already in 1996 Cranor [5] formulated general requirements for electronic elections.

Figure 1 doesn't show all dependencies, but the arrows indicate the most important ones. The technological security requirements are part of the critical technological requirements, as legal requirements take effect especially on them. They are focused below.

The necessity to systematically analyze security requirements is substantiated by the security problems arisen in practical pilot schemes.

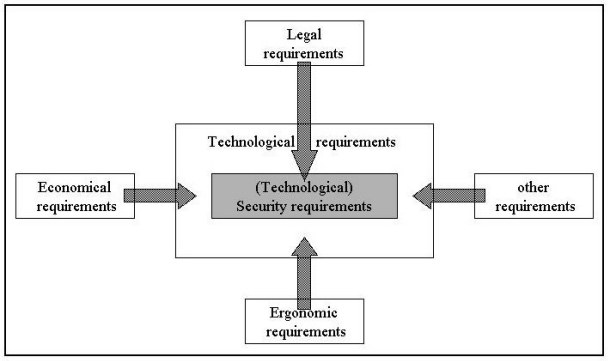

Figure 1. System of requirements

The accurate security conditions depend on the concrete election. For example, a country-wide political ballot requires different instruments than a local or regional student parliament 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, e.g. electoral laws (horizontal expansion of requirements). It is conceivable that for certain ballot types different sets of requirements will be set up. It should be stressed that concrete security arrangements of an election aim at accomplishing a ballot-specific security level (vertical expansion of requirements), since getting at absolute security seems to be impossible.

Even in polling stations the corrupting cooperation of the canvassers cannot be ruled out reliably. Furthermore, sending the vote via mail the voter cannot be sure that his vote will arrive and be considered.

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 [21] 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, for instance) 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, but it might be easier to handle this due to the controllable environment. 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. The author claims that an absolute reliability of all assigned systems cannot be guaranteed. 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 some 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". Although these are no technological security requirements, but only technological ones, it discloses that legal implications shown in figure 1 do not only refer to security aspects. (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. An example of use is online banking with HBCI (Home Banking Computer Interface) where dedicated chip-card

reader are used [26]. 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. The implementation of this requirement calls for additional infrastructural and organizational measures. 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: Malicious software scanning data possibly run on the voter's computer. Also remote administration software can intervene here. 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.

If one considers further aspects of various electoral laws, then additional requirements appear, e.g. meeting dedicated time slots.

In order to validate and verify a technological voting system the set of technological security requirements has to be consulted systematically. Section six sketches a possibly helpful framework. As voting protocols form the core of election infrastructures and significantly influence the security the next section sketches its' cryptographic principles.

5. Cryptographic voting concepts

Proposed concepts for implementing electronic elections base on cryptographic procedures. Fundamental work was done by Diffie & Hellman [7] concerning asymmetric encoding and by Rivest, Shamir & Adleman [20] concerning digital signatures and public key systems. In principle, each person gets a pair of keys consisting of a private key (only the person itself knows the number) and a public key. If Bernhard wants to send an encoded message to Bianca he just applies the encoding function on the message and her public key. Using the corresponding decoding function only Bianca can decode the encoded message as she needs her private key. Systems basing on these mechanisms are called "public key crypto(systems)" and are widely spread nowadays. Digital signature procedures use the keys in inverse order: Bernhard signs a document by using his private key (and the decoding function, not the coding function). If applying the coding function (not the decoding function) on the signed message and the public key of Bernhard results in the original message then Bernhard must have signed it because he is the only one who knows his private key. Crucial in security context are the generation and distribution of the keys.

Many voting protocols basing on cryptographic elements have been proposed: [1;6;10;12;16;22] belong to the most important ones; Schlifni [23] presents a good survey. Obviously, a secure election system consists of more than just one organizational unit or else the only unit could map the vote on the voter. Consequently, maintaining the voters' list must be separated from counting the votes. Among the approaches implementing this division of powers two of the most important ones are sketched below.

5.1. Trustworthy entities

Beside the entity responsible for generating and distributing keys we need an administrator (sometimes called validator) who is responsible for maintaining the list of voters and a collector (sometimes called psephor) who collects and counts the votes. The procedure illustrated in figure 2 works as follows:

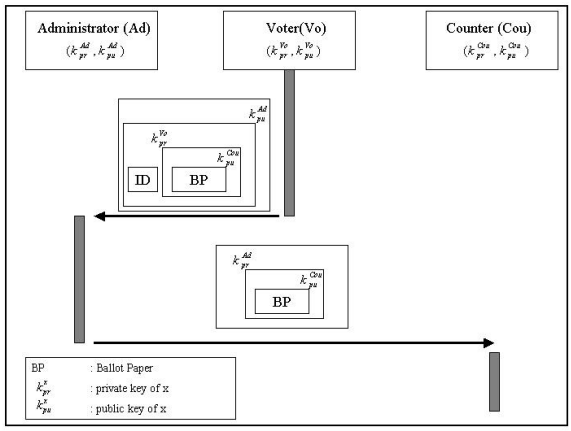

Figure 2. Voting procedure with trustworthy entities

Each voter, the administrator as well as the counter get a private key and a public key. The counter also gets an identifier (ID) with which he is associated in the voters list. The voter completes his ballot paper and encodes it with the public key of the counter, then he signs it (with his private key). Together with his ID he encodes it with the public key of the administrator. The administrator gets this message and decodes it with his private key - he is the only one who knows this key – getting the voter's ID.

In addition to this he also has to check if the message is authentic: this is possible by using the public key of the person associated with the ID. It is important to remark that the administrator cannot identify the voter's decision; it remains the ballot paper encoded with the counter's public key. Finally the administrator signs this encoded ballot paper with his private key ensuring that the counter can verify the sender (the administrator). Knowing the public key of the administrator and the own private key the counter gets a(n) (anonymous) vote.

Apparently, this procedure has some weaknesses [18, p. 143f]:

- The administrator can destroy and add votes.
- The counter can change, destroy, or add votes.
- If the administrator and the counter cooperate, then a secret election is not guaranteed.

Concerning a secret election you have to trust the entities. A more complex procedure not requiring this faith uses blind signatures and anonymous communication channels.

5.2. Blind signatures and anonymous channels

This procedure bases on Fujioka et al. [10] and uses the same entities as the "procedure of trustworthy entities", but differs from it regarding these essential items:

- The voter doesn't have to trust any entity, moreover he can detect any malpractice of administrator and counter.
- Not the administrator, but the voter is responsible for sending his vote to the counter.
- The communication between voter and counter takes place via anonymous communication channels.

Figure 3 shows the procedure.

Each voter possesses another pair of keys valid for just one election and (in the beginning) only known to the voter. The voter needs this pair in order to check if his vote was counted correctly. First, the ballot paper is encoded with the first vote-specific key; this encoding gets reversed not until the procedure's end meaning that no one except the voter knows his decision as long as the voter keeps his second (vote-specific) key private. Then a blind signature is applied: this concept is illustrated by analogy to carbon-paper-lined envelopes. If you seal a slip of paper inside such an envelope and a signature mark is later made on the outside, then when you open the envelope, the slip will bear the signature mark's carbon image.

The voter puts his encoded ballot paper together with his identifier (ID) into such an envelope and sends it (signed with his private key and encoded with the administrator's public key) to the administrator; from the algorithmic point of view the voter uses a random number. Only the administrator can read the message and check the authenticity. He notes the ID and the voter's activity, signs the envelope with his private key (without knowing the envelope's content), encodes the signed envelope with the voter's public key, and sends it back to the voter. The voter has to remove the blinding envelope resulting in a ballot paper signed by the administrator. He then encodes this signed envelope with the counter's public key and sends it to the counter. This communication takes place via anonymous channels [4] so that the counter cannot trace back the vote.

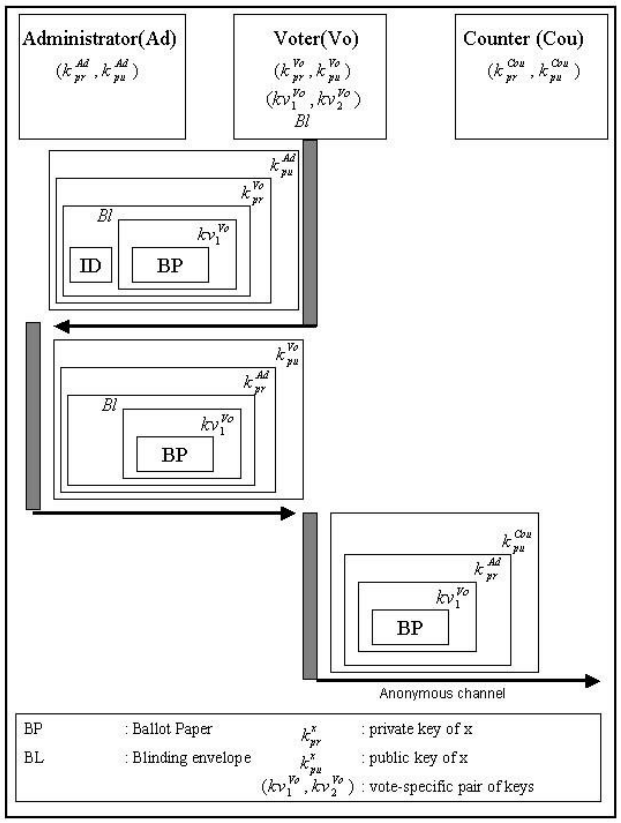

Figure 3. Voting procedure with blind signatures and anonymous channels

After receiving the anonymous (and still encoded) vote the counter assigns a number to this vote and publishes this number together with the encoded vote in a result list in the Internet. The number is sent back to the voter via the same anonymous channels which have kept the connection. At this time the vote is still encoded.

Later the voter sends the second vote-specific key together with the number (via anonymous channels) to the counter who can then decode the vote (associated to the number) and transparently documents the correct counting of this vote in the vote list in the Internet.

Drawbacks of this procedure are the following ones:

- Due to the complexity the implementation is difficult and error-prone.
- The voter gets a receipt of his vote which can be used for demonstrating his decision.
- Under certain circumstances (uncooperative behavior of the voter) an intermediate counting is possible: vote counting is possible as soon as the counter gets the second key which, ideally, is send not until the election's end.

6. Framework for voting systems

Although voting protocols are the core of voting systems they cannot work without corresponding organizations (e.g. voting authorities), data (e.g. digital certificates), functions (e.g. encoding and decoding algorithms), and computers (special hardware and software). Together with Protocols and their linking function they form an abstract framework that might be seen as a reference framework (figure 4).

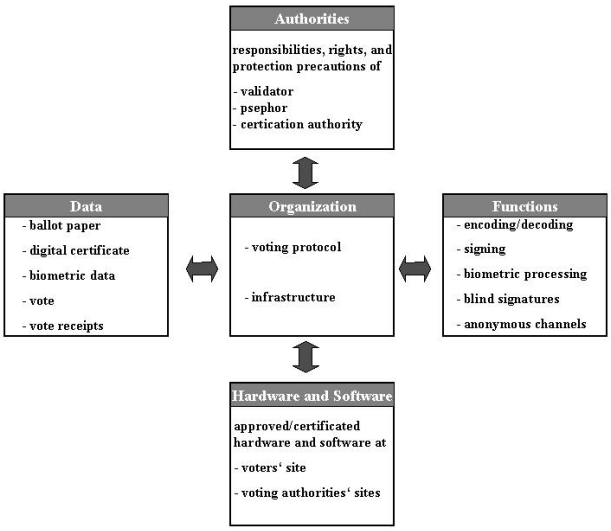

Figure 4. Framework for electronic voting systems

As security requirements always have to apply to the whole system – any insecure element can compromise the entire (voting) system – design tasks and security analysis of voting systems have to account for each element; a security specification of a voting system can become operationalized by specifications of the five elements.

Data: Different kind of data appear during an election and content as well as structure have to be defined. First, there is the electronic ballot paper sometimes signed by a voting authority to make it valid. Secondly, we have digital certificates which allow to prove identities and encode data in order to make it readable only for a selected person or institution. Unfortunately, there are many incompatible standards for digital certificates, e.g. X.509 [13], SPKI [9], and OpenPGP [3]. If biometric data is used for identification one has to define how fingerprints, facial recognition data, or/and iris scan data are stored. Thirdly, the votes itself must be stored. Fourth, a big problem are vote receipts. If used, should they contain the voter's decision or mustn't they?

Functions: Core aspects are algorithms for encoding and decoding (including key length), signature algorithms as well as algorithms for blind signatures and anonymous channels. Where applicable, precise biometric identification algorithms must be applied.

Authorities: Different authorities have been proposed for making a ballot secure. Many voting protocols in literature integrate a validator, a psephor, and a certification authority (see section five). Beyond the question which authorities are involved in elections their responsibilities, rights, and even protection precautions regarding rooms, servers, etc. have to be specified.

Hardware and Software: At each side security requirements for hardware and software are important. Regarding the voter's PC at home think about malfunctioning software (viruses, worms, Trojan horses, etc.) that could change, delete or read the voting decision unnoticed. A solution might be external devices like smart card readers with a keyboard and/or display that work as an interface to smart cards (with own memory and microprocessor). Approved or certified software can be stored on the smart card which is responsible for secure encoding and signing. Moreover on all computers only approved or certified software should be applied.

Organization: The core element of electronic voting systems are the (static) infrastructure and the (dynamic) protocol subsumed as organization, as they integrate and combine all other elements. The protocol (see section five) determines the voting process: who does what with which data and how? The infrastructure determines which devices and software reside where (e.g. how many voting servers exist, level of redundancy) and how they are linked to each other including technical protocols. One of the most challenging security requirement is protection against DOS (denial of service) attacks.

Only if each element accomplishes specified security requirements we can get a secure voting system.

7. Conclusion

There are many application fields for Internet ballots in political as well as in non-political context. During the past years many pilot projects were conducted, which examined Internet elections coming upon large commitment. However, Internet ballots make high demands on security and theoretical research has to be

done regarding security aspects of data, functions, hardware and software, authorities, and protocols and infrastructure. For example, it is still open how casted votes should be receipted and which voting protocols should be used in which case.

There is also a strong need for empirical research: not much experience is available concerning the practical implementation of Internet voting and its acceptance. Many problems will probably be detected first in the course of further pilot projects.

Talking about Internet elections and security we should keep a trade-off in mind: Enlarging security also means an increase of effort, costs, and complexity. For that reason, we will carefully have to specify the level of security of each voting system.

[1] Benaloh, J.; Tuinstra, D., 1994. Receipt-free secret-ballot elections. In *Proceedings of the Twentysixth Annual ACM Symposium on the Theory of Computing*, May 23-25, 1994, pp. 544--553.

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

[3] Callas, J.; Donnerhacke, L.; Finney, H.; Thayer, R., 1998. OpenPGP Message Format, *RFC 2440*. <Available from http://www.ietf.org/rfc/rfc2440.txt> [Accessed 13 September 2003].

[4] Chaum, D.L., 1981. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. In: *Communications of the ACM,* Vol. 24, No. 2, pp. 84-88.

[5] 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].

[6] Cranor, L.F.; Cytron, R.K., 1997. Sensus: A Security-Conscious Electronic Polling System for the Internet. In *Proceedings of the Hawai`i International Conference on System Sciences*, January 7-10, 1997, Wailea, Hawai`i, USA. IEEE Computer Society Press, pp. 561-570, Available from http://lorrie.cranor.org/pubs/hicss/ [Accessed 13 September 2003].

[7] Diffie, W.; Hellman, M.E. 1976. New Directions in Cryptography. In *IEEE Transaction on Information Theory*, Vol. 22, No. 6, pp. 644-654.

[8] 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].

[9] Ellison, C.; Frantz, B.; Lampson, B. ; Rivest, R. ; Thomas, B. ; Ylonen, T. 1999. SPKI Certificate Theory. RFC 2693. <Available from http://www.ietf.org/rfc/rfc2693.txt> [Accessed 13 September 2003].

[10] Fujioka, A., Okamoto, T., Ohta, K., 1992. A Practical Secret Voting Scheme for Large Scale Elections. In: *Advances in Cryptology. Proc. of AUSCRYPT '92: Workshop on the Theory and Applications of Cryptographic Techniques.* Lecture Notes in Computer Science 718. Springer. Berlin et al, pp. 244-251.

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

[12] Hirt, M.; Sako, K., 2000. Efficient Receipt-Free Voting Based on Homomorphic Encryption. In *Advances in Cryptology - EUROCRYPT 2000: Workshop on the Theory and Applications of Cryptographic Techniques*, pp. 539-556.

[13] Housley, R.; Ford, W.; Polk, W.; Solo, D., 1999. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. *RFC 2459*. <Available from http://www.ietf.org/rfc/rfc2459.txt> [Accessed 13 September 2003].

[14] Kubicek et al., 2002. Wahlen und Bürgerbeteiligung via Internet. In *HMD,* Vol. 39, No. 226, pp. 21-36.

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

[16] Nurmi, H.; Salomaa, A.; Santean, L., 1991. Secret Ballot Elections in Computer Networks. In: *Computer and Security*, 36(10), pp. 553-560.

[17] 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.

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

[19] 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.

[20] Rivest, R.; Shamir, A.; Adleman, L., 1978. A method for obtaining digital signatures and public-key cryptosystems, In *Communications of the ACM,* Vol. 21, No. 2, pp. 120-126.

[21] 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].

[22] Sako, K.; Kilian, J., 1995. Receipt-free Mix-type Voting Scheme. In *Advances in Cryptology - EUROCRYPT '95*, pp. 393-403.

[23] Schlifni, M., 2001. Electronic Voting Systems and Electronic Democracy. Participatory E-Politics for A New Wave of Democracy. Available from <http://members.chello.at/manhard.schlifni/Webpub/Inhalt/Inhalt.htm> [Accessed 13 September 2003].

[24] Schryen, G., 2003. E-Democracy: Internet Voting. In *Proceedings of the IADIS International Conference WWW/Internet 2003*, Algarve, Portugal, 5-8 November 2003

[25] Schryen, G., 2003. Internet-Wahlen. In *Proceedings of the 6. Internationale Tagung Wirtschaftsinformatik 2003, Medien - Märkte – Mobilität*, Dresden, 17-19 September 2003

[26] Staiger, A., 2002. HBCI und digitale Signatur. Neue Lösungen für das Onlinebanking der Zukunft. In *HMD,* Vol. 39, No. 224, pp. 29-33.