International Review of Social Sciences and Humanities
Vol. 6, No. 1 (2013), pp. 41-52
www.irssh.com
ISSN 2248-9010 (Online), ISSN 2250-0715 (Print)

Evaluation of Internet Voting Systems based on Requirements Satisfaction

Martin Vejačka
Department of Applied Mathematics and Business Informatics
Faculty of Economics, Technical University of Košice
Nemcovej 32, 04001, Košice, Slovakia
Email: martin.vejacka@tuke.sk

(Received: 14-5-13 / Accepted: 28-6-13)

Abstract
Internet voting allows citizens to vote in elections and referendums on nationwide or municipal level from virtually anywhere using computer with connection to Internet. This paper is aimed to identify and summarize multiple requirements on any Internet voting systems. Evaluation method based on these requirements is developed and applied on three real Internet voting systems (Edmonton, Estonia, Washington, D.C.). Evaluation of mentioned internet voting systems is provided and explained. Further, the reasons of the criticism of Internet voting are mentioned and possible threats to Internet voting are discussed. Arrangements and precautions to answer these possible security threats of Internet voting are provided. Due to necessity of basic computer literacy of voters is Internet voting not available for all eligible voters and therefore not suitable for implementation as the only one voting system in any election.

Keywords: Internet voting, e-government, Internet voting requirements, electronic identity.

1. Introduction

Expansion of the Internet and its broad availability in developed countries brought us possibility to use it in many areas of public administration. Elections and voting systems are important part of public administration framework in any democratic country and development of Internet allowance of voting in public elections via Internet. The allowance of voting in elections and referendums via the Internet is called Internet voting or i-voting. Internet voting is in several countries (e.g. Estonia, Canada, Switzerland, Norway etc.) in some form implemented at different levels [15]. Multiple other states are planning to introduce Internet voting in future. In Slovakia i-voting is not allowed at all, but in the referendum in year 2010 great majority of voters (70.46%) agreed with possibility of Internet voting introduction for Slovak national and parliamentary elections [16]. However this was the opinion of general public, professionals might have other opinion. Mostly they question the security of such elections.

Internet voting, because of its utilization of the Internet, brings multiple advantages in comparison to traditional types of voting. Basic advantage of Internet voting in comparison with traditional voting is better accessibility and comfort of voting (also for disabled or

citizens currently abroad) as long as it does not require physical presence at ballot box. Possibility of voting through Internet may lead to higher participation in elections (i.e. higher voter turnout) thanks to mentioned better accessibility and comfort of use. This helps to promote principles of democracy in given country [7]. Very important feature of Internet voting is its wide usability in all forms of municipal, public and state elections and referendums. Further advantage of Internet voting is greater speed and accuracy of results data processing, while it is done electronically. Very positive aspects for voters are also their lower costs of voting considering time consumption and transportation (to and from voting premises) costs.

Internet voting brings multiple advantages, but on the other hand Internet voting has rather high fixed costs of introduction. Highly important is the question of trust in electronic environment of Internet voting system, similarly to electronic markets and e-commerce applications [4]. The trust of voters in Internet voting system can be earned very slowly especially in early years after its introduction [19]. Many technical issues must be solved during introduction of i-voting. Basically Internet voting system (IVS) must comply with requirements stated in following chapter.

2. Identified Requirements on Internet Voting

Internet voting process consists of several phases. All these phases can be found in traditional elections and must be made in the exact same order and are the basis for the implementation process of Internet voting elections [2]. Internet voting must be adequate to traditional voting with regard to different environment of its implementation.

Internet voting must allow voters to record their votes safely and secretly. Also communication between voter's computer and election server must be secure, while third party might try to change the votes during its transfer to server. Therefore secured communication (e.g. using SSL/TLS protocol) via Internet must be employed. Using cryptography and encryption definitely increases the secrecy of ballot and the whole voting. Very important is processing all votes into corresponding and true results by technological means. Internet voting in elections should be implemented as additional possibility of utilization of voting rights by country citizens and must answer all requirements on traditional forms of elections. The Internet voting solution must be user-friendly to allow the most of voters use it conveniently.

Internet voting system (IVS) should usable for different elections [2]. It should not be designed for one use, but to be easily adjusted for another cases of use (various referendums and elections). Voting ballots must be designed as distinct as possible for voters to minimize the possibility of miscasting votes due to any misleading aspect of ballot design.

IVS must be robust to prevent electoral frauds (insider attacks) or attacks from outside the system. All types of attack must be considered while implementing the technical solution of Internet voting system. Cooperation of the all technical components and services used should allow assuring interoperability and proper functionality of IVS, therefor use of suitable open standards in electronic data interchange should be recommended. Internet voting system must be very reliable and the results must be correct and consistent with the votes casted by voters. It must be functional under any circumstances, even when some problems occur (like network outages, hardware failures, hacker attacks etc.). System's reliability must be tested, evaluated and improved continually. The Internet voting system has to be uninterruptedly available for voters. Its interface should be easy-to-use and all voters should have possibility of equal access to it, regardless of age, education, physical and mental condition. All components of information and communication technologies must be tested, that they comply with technical requirements [17]. The whole Internet voting system has to be subject of external audit and testing of intrusion possibilities, while its conclusions should be taken into account in further use and development of the system. [13]

Ensuring the accuracy, completeness of information and votes processing methods assures integrity of Internet voting system. The outcome of voting matches voter intent and all votes are casted as intended by voter. Accessibility of IVS allows the usability of information to authorized users when needed. It includes the process of protecting data against any misuse by attacker inside or outside the system. [20]

Voter's ballot must be secret and no one should be able to determine how voter voted, even if voter tries to prove how he (or she) voted. Here can be used the principle of asymmetric encryption utilizing pair of keys (this principle is used also by digital signature). Encrypting the vote by public key of election authority and storing it on the server during the electoral process, which does not have access to the private key of election authority. After the elections, only votes (not pairs of vote – voter) should be sent to the votes counting server. This server would have access to election authority's private key, but it contains only votes without possibility to pair it with voter. This method provides high level of confidentiality and privacy in Internet-voting. [2]

Voters must be registered in register and it must be continuously updated to allow only eligible citizens to vote. Voters should have a possibility to request changes of their information in this register if necessary. Information on voters can be utilized from countries birth record registers. Their identification in electronic environment with possibility to compare their identity with register must be assured with combination of electronic authentication of their votes [13]. Only authorized voters could cast votes and each voter could only vote up to the permitted number of times [2]. The best solution of electronic authentication is considered digital signature, which can be issued to all eligible voters (for example in form of ID card with electronic chip) [6]. Digital signature is based on principle of asymmetric cryptography, using pair of keys (private and public) to verify identification of signer (and authorize access to Internet voting system) and authenticity of electronic document (in case of Internet voting – voting ballot). [1]

Furthermore it can be used for encrypting electronic message for only specific recipient (e.g. encrypted electronic ballot decipherable only by central election authority), so it can excellently serve for multiple purposes in Internet voting system. This is the key aspect of Internet voting system and ideal form of electronic identification of citizens used in Internet voting system should be usable in other e-governmental systems or in private sector. Its universality and reusability would stimulate development of e-governmental applications and decrease additional costs.

The voter should be able to check if his vote was recorded and added to the results of elections, but he should not be able to prove how he voted to another person to prevent coercion or buying votes. However, general verifiability of election results is necessary to enable the possibility of verification by voters if the votes were properly recorded and accurately counted. Forcing or buying the votes can be prevented by enabling to recast vote during elections interval by electronic or traditional way.

Another important aspect of Internet voting is fact that all authorized voters must have the opportunity to vote. Internet voting system must be able to accept all votes on schedule and process election true results in acceptable time. IVS should be also intelligible and cost effective. [13]

3. Method of Evaluation

Based on identified requirements on Internet voting system, we specified 14 groups of requirements containing multiple sub-requirements. Each group has maximum score assigned according to importance of requirements which it contains. Overview of requirements groups and its scores are stated in following table. This table allows the evaluation of multiple different i-voting systems and comparison of these systems on the relevant basis universal to all Internet voting systems independently on their technical solution.

Table 1: Evaluation of each group of requirements on Internet voting systems

Group of Requirements	**Maximum Score**
Safety and secrecy of voting	10%
Robustness of Internet voting system	10%
Authorization and authentication of voters	10%
Eligibility	10%
Availability, reliability and operability of voting	10%
Testing and certification	10%
Auditability	5%
User-friendly usability	5%
Transparency of voting	5%
Enfranchisement and uniformity of voting	5%
Verifiability, repeatability and controllability of vote counting	5%
Unprovability of voting	5%
Possibility for re-vote	5%
Supremacy of conventional voting	5%
Total evaluation	**100%**

The table shows the assignment of the maximum score on the individual requirements of the Internet voting system. The maximum score was assigned according to importance of the aspect on IVS. Most requirements include multiple of other sub-requirements for IVS solution, but detailed list of sub-requirements and their exact evaluation go beyond the extent of this paper.

Safety and secrecy of voting measures show how safely are votes transferred between voter and election server, stored at server and also privacy during casting the vote. This is very important requirement group to get true results of voting, so its weight is set at 10 percent. Robustness of Internet voting system stands for the protecting of data against any misuse by attacker inside or outside the system including prohibition of falsification of votes, so no-one should be able to change votes given by voters or add falsified votes to the system (e.g. vote in place of voters who did not participate in the elections). Evaluation of these characteristics of IVS is weighted with 10 percent from whole evaluation of the system.

Authorization of voters ensures that only voters who are included in the voters' list according to local legislation can vote and one can only vote for the candidates applicable in his electoral district. This involves the necessity to authenticate the voter with any appropriate and safe solution. This group of requirements is evaluated with 10 percent from whole evaluation and closely relates to eligibility of voter.

Eligibility of voter is verified against register of voters and it must be assured, that all of votes casted by the voter, only one final vote will be counted, regardless of the way the votes were given. Eligibility of voter requirements has weight of 10 percent in whole evaluation of IVS. Availability and operability of IVS assures that the election system is be able to accept all votes on schedule and produce results in a timely manner and assure the usability of information to authorized users when needed. Operability of IVS includes the requirements of reliability of its operation, availability to voters and those responsible for the organization of voting during necessary time, operation with adequate speed, ensuring the preservation of

data and presentation of voting results. These requirements create 10 percent of whole IVS evaluation.

Testing and certification of IVS is necessary to assure all functions and parts of the system are properly functional and operational. Proper external testing and certification should be allowed. Fulfillment of testing and certification requirements of IVS is evaluated by maximum of 5 percent in our evaluation. Auditability means that specifically authorized persons must have the opportunity to check that the whole process of voting has been conducted correctly. The society and the parties involved have to believe both before and after the voting that i-voting is (and was) a trustworthy way of giving one's vote. Auditability has maximum of 5 percent in our evaluation.

User-friendly usability of Internet voting allows using voting via Internet all voters with at least basic computer literacy provided that they have available computer with Internet access. Score in user-friendly usability creates 5 percent of our evaluation. Transparency of Internet voting system is assured when the process and mechanisms of voting public and understandable. With transparency is narrowly related with requirement of verifiability and controllability of vote counting, which mean that every interested person (including persons not engaged in the system) should be able to prove the final calculation of results and also the process of counting i-votes is repeatable. This group of transparency requirements weighs 5 percent in final evaluation. Uniformity and enfranchisement of voting represents principle of equal voting possibilities should be ensured to all voters. All authorized voters should have the equal opportunity to vote. This requirement is virtually impossible to meet completely only by Internet voting method, basically because not everybody has access to Internet and not all voters are computer literate enough to be able to use Internet voting application. However we considered 5 percent maximum evaluation for this requirement.

Unprovability of voting respects privacy of voter while using his right to vote. This requirement relates to requirement of secrecy of voting, but allows keeping secret if voter voted and even disable possibility of voter to prove to another person that vote has been cast. Unprovability is a method aimed at protecting voluntary voting (freedom of voting, uncoercibility). Uncoercibility requires that the voters are free in their choice. It should be impossible for the voter to prove how he (or she) voted rules out controllable selling and buying of votes or any other form of coercion. Evaluation of this requirement constitutes 5 percent of final evaluation of IVS.

Possibility for re-vote allows the voter to recast vote while using Internet voting or to replace his i-vote with conventional vote to substitute possible faulty vote casted via Internet voting. This helps also prevent possible coercion and this requirements is weighted by 5 percent. Supremacy of conventional voting assures that any other method of voting annuls all i-votes given by the voter, what helps to prevent coercion and allow voting when Internet voting is not available. If this requirement is fulfilled completely, IVS would be evaluated by 5 percent in our evaluation.

It is reasonable to presume, that no real current voting system can meet all these requirements and acquire ideal total score of 100 percent in this requirement satisfaction evaluation.

3.1 Results

Using our method of Internet voting systems evaluation based on compliance with the multiple requirements, we evaluated three Internet voting systems. Specifically, we evaluated the IVS used in Estonia for parliamentary and local elections; IVS intended to allow overseas absentee voting and deployed on a test election in 2010 in Washington, D.C., USA and IVS tested in Edmonton, Canada for the 2013 General Election, which has been tested in 2012 Jellybean Internet Voting Election. All three systems have their particularities and various technical solutions, but necessarily have to comply with the requirements for IVS (which we used for our evaluation of Internet voting) at the highest possible level. For each requirement in each group was assigned evaluation based on personal experience of public testing of IVS,

the available literature sources relating to the IVS, the personal examination and testing of the IVS web interface and based on available documentation of these systems. The assessment itself can be seen in the following table.

Table 2: Evaluation of selected Internet voting systems

Group of requirements	Maximum score	Estonia	Washington D.C.	Edmonton
Safety and secrecy of voting	10%	9.1%	3.9%	7.4%
Robustness of Internet voting system	10%	7.6%	3.2%	6.7%
Authorisation and authentication of voters	10%	9.7%	6.1%	7.8%
Eligibility	10%	9.8%	6.5%	7.9%
Availability, reliability and operability of voting	10%	8.9%	7.3%	9.3%
Testing and certification	10%	8.3%	9.2%	9.8%
Auditability	5%	4.8%	4.7%	4.1%
User-friendly usability	5%	4.2%	4.6%	4.7%
Transparency of voting	5%	3.8%	3.7%	4.0%
Enfranchisement and uniformity of voting	5%	4.8%	4.7%	4.8%
Verifiability, repeatability and controllability of vote counting	5%	3.9%	3.7%	3.5%
Unprovability of voting	5%	4.2%	2.9%	3.6%
Possibility for re-vote	5%	5.0%	4.0%	4.5%
Supremacy of conventional voting	5%	5.0%	0.0%	5.0%
Total evaluation	**100%**	**89.1%**	**64.5%**	**83.1%**

Internet Voting System introduced in Estonia is the only one of the three evaluated, which is already used in the real long-term operation and was therefore tested several times by the real actual voting. Very good evaluation in groups of authorization and authentication requirements and eligibility of voter requirements was scored because of utilization of identification through electronic ID. This electronic identification is distributed to Estonian citizens in the form of an identity card with a chip containing a digital signature of the person issued by public administration authorities. This way allows excellent authorization and authentication of a particular person in any electronic environment in public administration systems in Estonia (including the Internet voting system). This electronic ID developed into more forms (ID card, digital ID and mobile-ID) and the most of Estonians have their electronic identity in some of these forms securely assigned already. Using this electronic identity they can vote in i-voting elections, since the local elections of 2005, when more than 9000 voters casted their ballot via the IVS (about 2 percent of all participating voters). In following years Internet voting has been used in four more elections with increasing trend in percentage of Internet votes casted. In last nation-wide elections (Estonian Parliamentary elections in 2011), almost one quarter of votes (24.3%) were casted via Internet [9]. Furthermore it is probable, that the significant part of votes was casted only because of possibility of Internet voting and voters would not cast them, if they would have to go personally into polling rooms. [5]

Key features of Estonia's Internet voting model that have contributed to citizen uptake and its continued success include: Internet penetration, public support and trust, a supportive legal framework, and a secure and reliable authentication system [11]. Process of casting Internet-vote (guaranteeing the anonymity of vote) in Estonian IVS is following. The application downloaded in the voter's computer during Internet voting encrypts the vote. The encrypted vote can be regarded as the inner, anonymous envelope. After that the voter signs his encrypted vote with his digital signature (from ID card, digital ID and mobile-ID) to confirm his choice. By digital signing, the voter's personal data or outer envelope are added to the encrypted vote. Before the final counting of votes, the encrypted votes and the digital signatures with personal data or inner and outer envelopes are separated. Then anonymous i-votes without personal data are opened and then counted. This assures high secrecy of voting and also our evaluation in this category was high (9.1% from maximum possible 10%). [20]
The Internet-voting in Estonia is possible during 7 days in advance polls (from 10th day until 4th day prior to Election Day). This guarantees that only one (last) vote is counted for each voter. To diminish the threat of coercion, it is allowed to change their electronic vote by voting again electronically during advance polls or by voting at the polling station during Election Day. If voter has voted both via Internet and with paper ballot, the information is sent to the central electoral committee, which cancels voters' i-vote. This assured to Estonian IVS full score in possibility of re-vote and supremacy of conventional voting. [8]

Furthermore, Internet voting for given elections may be tested for three days. Test allows checking whether voters computers has the right settings, ID-card (or mobile-ID SIM card) certificates are valid and PIN codes exist. If any problems occur, there is still enough time to solve them prior to elections. However open public mock voting was not allowed prior to last elections to further test the robustness of IVS so the score in testing and certification was slightly lowered (8.3%). [14]

In total the evaluation of Estonian IVS was the highest from all three evaluated systems with score of 89.1%. It reflects its quite long usage in real praxis, which led to removal of basic issues common when introducing new systems. However its further development is necessary, improvement are possible in areas of testing, transparency and user-friendly usability. Still Estonian IVS is the evidence that it is possible to successfully introduce and continually use Internet voting in significant extent.

The second evaluated Internet voting system for overseas absentee voting in Washington, D.C. was not deployed of the system in final, because public testing of this IVS administered by public administration authority in 2010 showed huge issues it had. Especially in the field security major deficiencies were identified through public test, which could experts from outside of system in the development of IVS to test its safety. Possibility to openly test this system by experts from outside the system however brought to this IVS high score in category of Testing and certification (9.2%) in our evaluation. On the other hand, the results of this testing were disturbing in many other categories. Team from University of Michigan, which attended this public test of IVS, managed to change all votes, steal database passwords and authentication elements, reveal votes and expunge of tracks of their attack. This attack proved poor quality of protection and attack prevention implemented in Washington, D.C.'s Internet voting system [18]. Low scores in robustness (3.2%) and safety and secrecy of voting (3.9%) consent with this fact. The test also proved that eligibility of voters (6.5%), availability and reliability of IVS (7.3%) cannot be fully assured what further decreased score of IVS. Also authorization by password and PIN delivered by mail was not evaluated as the best solution and led to lower score in category of authorization and authentication (6.1%). Supremacy of conventional voting was not assured at all and score was therefore at minimum (0.0%). In other categories Washington, D.C.'s IVS scored evaluation comparable with other systems. Total evaluation of this IVS was relatively low at level of 64.5% and thanks to its security issues it is not suitable for introduction into real usage.

Internet voting system in Canadian city of Edmonton was tested in 2012 in a test of Internet voting known as the 2012 Jellybean Internet Voting Election. The purpose of this test was to gauge the readiness of Edmontonians to use Internet voting as a valid alternative in later

elections and to test technological readiness of IVS. Outstanding evaluation scored this IVS in testing and certification (9.8%) and in availability, reliability and operability of voting (9.3%). [3]

However in area of authorization and authentication of voters (7.8%) and eligibility of voters (7.9%) it has lower evaluation, while no register of voters existed for Edmonton's elections and for Internet voting voters must to pre-register and get their electronic identification usable only for those elections. Fact of security issues of pre-registering lowered evaluation in categories of robustness and safety of voting. On the other hand, the user-friendly usability of this IVS was very high (4.7%), so as enfranchisement and uniformity of voting (4.8%). Possibility for re-vote was assured conventionally with its supremacy over i-vote casted so evaluation was at 4.5%, respectively 5.0% in these categories. In all other categories Edmonton's IVS score was similar to other evaluated systems. Final evaluation of this IVS was at 83.1 percent what is satisfying score, however Edmonton officials in February 2013 decided not to introduce this IVS system into praxis yet for upcoming 2013 General Elections. On the other hand, analogous solution of Internet voting is already used in over 60 municipalities in Canada. [10]

4. Discussion

This evaluation method based on IVS requirements provides assessment, which well reflects the IVS readiness to implement in practice. The evaluation of partial requirements and their score is possible to modify the requirements of specific public administration at IVS. In principle this evaluation can be considered indicative for the need for a decision about introduction of IVS into use. However, this decision is often political issue.

Even if Internet voting systems fairly comply with all requirements, many experts in field of computer sciences (e.g. Rivest, Simons, Jones) however doubt about security of their use [13]. In the case of Internet voting these risks are even considerably higher, given the indisputable importance of equitable elections in democratic countries. They warn against putting them into practice, primarily due to safety requirements (especially safety and secrecy of voting, robustness of Internet voting system and authorization and authentication of voters) and their possible imperfect satisfaction.

Experts indicate higher risk in comparison to traditional paper ballot voting, while using Internet for voting, because complete results can possibly be changed by single attack on central election server. On the other hand, public administration authorities and IT experts continuously develop the possibilities of diminishing the threats by taking multiple precautions and arrangements for optimizing Internet voting process' security. Two main groups of threats of Internet voting are discussed, client-side threats and server-side threats.
On the client-side, coercion can be considered as the biggest nontechnical problem of Internet voting. Voting distantly (via Internet or post) always has the problem that voters can be intimidated to vote in way the intimidator (person who is trying to coerce voter) wants. This problem is rooted in lower privacy of Internet voting in comparison with traditional paper ballot voting system. Lower privacy of Internet voting arises from the fact that while in traditional voting voter votes alone in private voting booth. Using Internet voting voters votes via Internet through computer at home or job, where other people (e.g. family) can see "over his shoulder" his votes casted. There are however few ways to counteract the problem of coercion in case of Internet voting. Basic way is to enable Internet voting for longer period (e.g. for week) before traditional election with possibility of recasting the ballot via Internet (as implemented in Estonian IVS). If voters can vote only once and when the ballot is cast and cannot be changed or replaced by new one respectively, then voter cannot recast his vote at the time, when he is no longer under pressure of coercion. On the other hand if recasting is enabled voter can still change his vote later when he has privacy for voting. However this recasting gives coercer the possibility to coerce voter to change his vote, even if he already casted it, but still voter has possibility to recast it again according his own will later. This recasting lowers coercer's possibility to coerce bigger number of voters, while he had to control all of them during the end of Internet voting period. Moreover there can be introduced

possibility to cast vote traditionally on Election Day, even after multiple recasting by Internet voting (in compliance with the requirement of supremacy of conventional voting). This vote cancels all votes through Internet voting and assures higher privacy of traditional paper ballot casting.

Malware is traditional problem of Internet users. It threatens not only Internet voting, but also Internet banking or any other communication via Internet involving interchange of sensitive information. For example key-logging malware may steal credentials of voter during voting process or change votes before sending it to the election server. Therefore it is necessary to prevent malware infection of voters' computers by proper antivirus protection. This is basic recommendation for all computers connected to the Internet. Pre-emptive virus scan and disinfection with up to date antivirus software before casting vote is also very desirable action.

Credential theft is another issue that relates also to many other activities on the Internet (like Internet banking) not only to Internet voting. Technical solution of authentication of voter in Internet voting system should be as safe as possible. Here rises the problem of identity of voter in electronic environment. Securing it only through login and password (or PIN respectively) is considered by experts to be weak solution. Better solutions include dynamic component of authentication (one-time passwords, hardware tokens). The most secure of suitable and available solutions is use of digital signature distributed to all eligible voters. This can be achieved by issuing IDs to citizens with integrated digital signature as it is done in Estonian case and several other EU countries. Secured storage of voter information on server side in highly encrypted form is very desirable requirement.

Imposters' sites that pretend to be election server and redirect or change true votes are another issue of Internet voting. This can be prevented mainly by certificating election server and recommending voters to check correct address of website and validity of server's certificate. List of security recommendations and arrangements that should voters take, while utilizing Internet voting, is necessary to be published by election authorities. These precautions are also sub-requirements of safety and secrecy of voting requirement in our evaluation.

Botnets are networks of computers connected to Internet, but remotely controlled by third party users (attackers). Control over these computers is acquired by breaching their security. These botnets can be used to send spam or for various attacks e.g. denial of service attacks (see below). Another possibility of misuse is manipulation votes from computers in botnet and sending them to election server as correct ones. For avoidance of the voter's computer becoming part of botnet, its proper antivirus protection is crucial. It is obvious that safe and secure use of Internet voting is dependable also on IT skills of voter, what can be considered as key problem of its introduction in praxis. Furthermore IT professionals [13], while criticizing the security of Internet voting, often identify and induct following threats on the election server side of Internet voting system:

Denial of service (DoS) is common type of attack on server or network resource with aim to make unavailable to users by overloading with too many attempts of connection at the same time. This type of threat is conducted mainly in form of distributed denial of service (DDoS). Botnets are often used for DDoS attacks. DDoS attack can be mitigated by intrusion prevention systems, proper firewall settings, use of specialized anti DDoS hardware solutions and multiple technics for diverting suspicious traffic. DoS and DDoS attack prevention however requires qualified IT specialists and lots of resources. Therefore denial of services attacks' prevention is more effective when Internet elections are centrally based rather than precinct based. Also availability of voting during longer period of time (e.g. for a week) gives higher chance to access voting server when it is not blocked by DDoS attack during whole period. [12]

Insider attacks are serious threat for Internet voting. IT professionals with legitimate access to election server might potentially change results of elections or at least change multiple votes according their will. This threat must be prevented by using cryptography and encryption to

restrict their possibility to access and change the data. Also external independent tests of implemented Internet voting solution are necessary to find and eliminate any potential flaws in securing election data. Precautions for prevention of these attacks are included in our evaluation (the sub-requirements of robustness of IVS).

Remote intrusion is another significant threat which will be very probably attempted by adversaries in case of Internet voting implementation. Prevention of remote intrusions lays great demands on protection of centralized election system and its solutions are offered by big IT firms and highly qualified IT professionals must be employed in this prevention. Independent external tests aimed on attempts of remote intrusion must be administered to thoroughly test Internet voting system on any potential flaws and their consequential elimination.

State sponsored attacks represent attacks supported by foreign states with aim of destabilizing the government and political system in given state. Any form of stated threat can be sponsored by foreign states, but server-side attacks are more probable. Prevention of all types of attacks is considered in our evaluation of IVS in various groups of requirements. In compliance with stated arrangements, precautions and requirements it is possible to significantly diminish (but probably not completely erase) the risk of mentioned ways of Internet voting security breaches. To comply this arrangements and requirements, it is the best to implement the Internet voting system in centralized form on national level (not on local level or state level as in USA), while funds are more concentrated. Single national election authority can employ more and better qualified IT specialists to provide continuous protection of Internet voting system than multiple precinct or local authorities with equal budget in the aggregate. It is obvious that protection arrangements on the client's side of Internet voting system require at least moderate IT skills (safe use of computer, antivirus and firewall control) from its users. This fact is not possible to catch in our evaluation completely and it restricts general usability of IVS and therefor it should not be the only voting system implemented in a given country.[7]

5. Conclusion

Allowing elections by Internet voting facilitates access for the most citizens to utilization of their right to vote as basic principle of democracy. Elections become more available for disabled people and more excluded groups of citizens, however for Internet voting utilization voters need Internet access and basic computer-literacy. Internet voting also encourages the development of a democratic society by improving the possibilities of direct democracy. These benefits are undoubted and they are acquirable for acceptable costs.

We proposed evaluation of Internet voting systems based on multiple requirements in various groups. Very important is evaluation of requirements regarding security of Internet voting. Experts specify several threats of Internet voting in this area. Election authorities must prevent various types of possible attacks on such attractive target for attackers as Internet voting system is. However, high grade of protection and security on election server side is possible to achieve by stated arrangements (hardware anti-DoS protection, firewalls, intrusion prevention systems, encryption etc.). The weaker point of Internet voting system's security is on the side of voter. Arrangements of secure use of Internet voting system on their side involve slightly higher than basic computer skills (like protection against malicious software, imposter sites detection etc.). Internet voting, because of demanding some IT skills from voter, restricts its usability by any voter (though it can be more suitable and convenient for voters with impaired mobility and similar handicaps), so it cannot be implemented as the only one voting system in any elections.

By evaluating three different IVS solutions used in Estonia, Washington, D.C. and Edmonton we have tested our evaluation method. The best evaluated IVS was Estonian voting system with score of 89.1 percent. This corresponded with fact that this system is implemented in praxis for several years and it is therefore verified by real use. IVS from Canadian city of Edmonton was also evaluated positively (83.1 percent), but by political decision it was not

implemented in praxis yet. The voting system tested in 2010 in Washington D.C. was evaluated significantly lower with bad score in robustness and safety of voting. That corresponded with declining the introduction of this IVS into praxis. Implementation of IVS in Estonia is example that Internet voting can be successfully and securely used, what proved years of use and also evaluation by proposed method. It is vital concept, especially in countries, where electronic IDs with digital signature embedded are issued, while it provides very good identification of voter in IVS. Countries when considering the introduction of Internet voting could inspire by IVS solution used in Estonia.

Acknowledgement

The paper was prepared within the national project "Security models of distributed systems providing electronic services" (Contract No. 1/0945/12) funded by Grant Agency for Science; Ministry of Education, Science, Research and Sport of the Slovak Republic.

References

[1] T. Bálint, J. Bucko and M. Esser, Electronic identity, risks if its abuse and its importance for the development of e-commerce, In: *Hradecké Ekonomické Dny 2011: Economic Development and Management of Regions, International Scientific Conference Proceedings*, Hradec Králové, Czech Republic, (2011), 24-25.

[2] G.A. Brewer, B.J. Neubauer and K. Geiselhart, Designing and implementing e-government systems: Critical implications for public administration and democracy, *Administration & Society*, 38(4) (2006), 472-499.

[3] City of Edmonton, *Internet Voting*, Online at: http://www.edmonton.ca/city _government/municipal_elections/Internet-voting.aspx, Accessed on January 13 (2013).

[4] R. Dráb, Ekonomické aspekty reputačných mechanizmov na elektronických trhoch, In: *IDIMT 2011: InterDisciplinarity in Complex Systems: 19th Interdisciplinary Information Management Talks*, Johannes Kepler Universität, Linz, Austria, (2011), 329-340.

[5] E. Estonia, *Internet Voting in Estonia, e-Estonia the Digital Society*, Online at: http://e-estonia.com/components/i-voting, Accessed on December 19 (2012).

[6] ePractice.eu, *The Estonian ID Card and Digital Signature Concept*, Online at: http://www.epractice.eu/en/library/281287, Accessed on December 15 (2012).

[7] Estonian National Electoral Committee, *E-Voting Concept Security: Analysis and Measures*, Online at: http://www.vvk.ee/public/dok/E-voting_concept_security_ analysis_and_measures_2010.pdf, Accessed on January 6 (2013).

[8] Estonian National Electoral Committee, *Internet Voting in Estonia*, Online at: http://www.vvk.ee/voting-methods-in-estonia/engindex/, Accessed on January 21 (2013).

[9] Estonian National Electoral Committee, *Statistics about Internet Voting in Estonia*, Online at: http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics, Accessed on January 6 (2013).

[10] N. Goodman, Internet voting in Canadian municipalities: What can we learn? *CEU Political Science Journal*, 5/4(2010), 492-520.

[11] N. Goodman, J.H. Pammett and J. De Bardeleben, A comparative assessment of electronic voting, *Report Prepared for Elections Canada*, (2010).

[12] B.B. Gupta, R.C. Joshi and M. Misra, Distributed denial of service prevention techniques and member, *IEEE - International Journal of Computer and Electrical Engineerin*g, 2(2) (April) (2010), 1793-8163.

[13] D.W. Jones and B. Simons, *Broken Ballots Will Your Vote Count?* (2012), Stanford, California, USA: CSLI Publications.

[14] T. Martens, Estonia - The Country with Identification Infrastructure, Online at: http://siteresources.worldbank.org/extedevelopment/Resources/Martens_Estonia.ppt, Accessed on December 18 (2012).

[15] A. Salner and J. Mišina, *Stav eGovernmentu na Slovensku, Príčiny a Riešenia*, Bratislava, Inštitut pre Dobre Spravovanu Spoločnosť, (2007), 8-21.

[16] Statistics Office of the Slovak Republic, *Results of Referendum 2010*, Online at: http://app.statistics.sk/ref2010/, Accessed on January 4 (2013).

[17] M. Vejačka, I-voting and its possible application in Slovak condition, In: *ICTIC 2012: Proceedings in Information and Communication Technologies - International Conference*, Žilina, Slovakia, 19(2012), 106-110.

[18] S. Wolchok, E. Wustrow, I. Dawn and A.J. Halderman, Attacking the Washington, D.C. internet voting system, In *Proc. 16th Conference on Financial Cryptography & Data Security*, Divi Flamingo Beach Resort, Bonaire, Netherlands, (2012).

[19] A. Xenakis and A. Macintosh, Trust in public administration e-transactions: e-Voting in the UK, International Teledemocracy Center, Napier University Edinburgh, *Lecture Notes in Computer Science*, 3184(2004), 162-171.

[20] E. Zakareya and Z. Irani, E-government adoption: Architecture and barriers, *Business Process Management Journal*, 11(5) (2005), 589-611.