

User Testing and Trustworthy Electronic Voting System Design

Petr Silhavy¹, Radek Silhavy¹ and Zdenka Prokopova¹

¹Tomas Bata University in Zlin, Faculty of Applied Informatics, nam. T.G.M. 5555, Zlin
76001, Czech Republic
{psilhavy, rsilhavy, prokopova}@fai.utb.cz

Abstract. In this contribution the user interface design for trustworthy system is presented. The principle of the Electronic Voting is discussed. The research aim was to discuss a users trust and its issues, which are connected to the design process of the prototype electronic voting system.

Keywords. Electronic voting, system design, user testing

1 Introduction

Discussing of the trustworthiness in the scope of the system engineering discipline takes key role in systems designing. If trustworthiness is discussed reliability, safety and security are discussed. The issue of trustworthiness is connected to the level of the user acceptance [1]. The word “system” stands for on-line systems. It means systems, which are realized on basics of Internet, or similar communication systems.

The organization of this contribution is as follows. Chapter 2 describes a basic electronic voting theory. Chapter 3 describes electronic voting conditions. Chapter 4 describes the problem formulation. Chapter 5 describes the selected questions, which have to be solved to achieve trustworthiness of the electronic voting. Finally chapter 6 is the discussion.

1.1 Electronic Voting in Brief

The electronic government, the actual point of the computer-social investigation, uses several methods for improving governmental processes in Europe. These electronic methods allow the improvement in direct democracy. Probably, the most relevant solution is remote Internet voting. The remote voting solution allows participation in election process with respect to personal conditions and to the physical accessibility of polling stations, which may possibly prevent citizens from casting their votes. Therefore, remote Internet voting should effectively support voters, who are resident abroad. These voters use at present the embassy election rooms only.

There are several conditions for electronic voting systems, which were discussed several times and now are accepted as facts. The appropriate system has to follow the technical and process conditions listed below:

- Participation in the voting process is granted only for registered voters.
- Each voter has to vote only once.
- Each voter has to vote personally.
- Security and anonymity of voters and voting.
- Security for the electronic ballot box.

The first condition for electronic voting means, the voter should be registered by voting committee in the list of voters. This list is used as the basis for distribution of login information. If the voter is registered, they will be able to display the relevant list of parties and candidates.

Voters could also vote more than once, but only the last attempt will be included in the final results of the election. This possibility varies in different e-voting systems. If it is not possible to vote more than once, there should be more complicated protection for the election against manipulation and assisted voting.

The third condition – Right to vote personally – is closely connected to the previous. On the other hand this is the basic responsibility of each voter to protect his private zone for voting – in the case of the internet-based remote voting. In the “in-site” voting the system of privacy protection will be similar to the current situation.

Security and anonymity of voters and voting is probably the most important issue in the electronic voting process. The appropriate voting system should be realized in two separate parts. The first part should be responsible for authorization of the voter and the second for storing votes. Therefore the system will support anonymity. The voter should check his vote by the list of collected votes. The voter will know the unique identification of vote only. Using a cryptographic principle will protect the voting process. One of the many applicable solutions is Private Key Infrastructure. This approach deals with two pairs of keys in the first part of voting system – for authorization. In the second part of voting system – storing votes – it should deal with a public key for protection of the vote in the transport canal.

The electronic ballot box should form as a database. The public key of the election committee will cipher votes in the database. Members of the committee will hold the private key, which is necessary for decrypting votes. Each member will hold only part of the key.

The sample system, which follows the defined requirements, is shown on Fig. 1 [6].

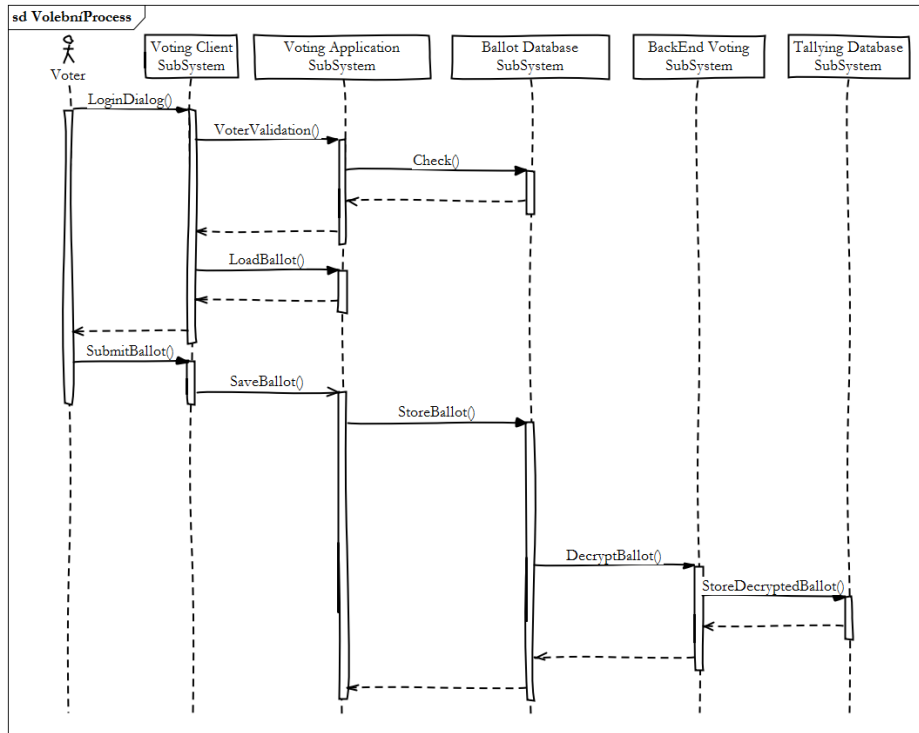


Fig. 1. Generic Voting Schema Design [8]

Probably, the most significant results is remote Internet voting in appropriate form, which understandable and clearly usable.

Internet voting solutions are usually divided the tree basic categories – poll site, kiosk and remote voting.

In the poll site voting, election technology is located in the election rooms. Comparing poll site voting to traditional paper-form voting, poll site brings more flexibility and usability, because voters are allow to vote from elections room up to their choice. There is no restriction to geographical locations. Poll site voting represents concept of the electronic voting. Poll site voting is effective in votes casting and tallying, because it allows certain and quicker processes.

Internet concepts allow expanding poll site voting to self-service kiosks. These kiosks should be placed in various locations. Authorities – local election committee, usually monitor elections room; kiosk should be monitored by physical attendance or by using security cameras.

Remote Internet voting is probably the most attracting methods of using Internet voting process. Remote voting expands remote voting schemas, which are used in some countries. These schemas compared to postal voting, offers improved casting ballots from remote locations. Voters are allows voting from home, office or other places, which are equipped by computers and Internet connections.

By investigation of these conditions and by the determination of the initial technological principles, authorities will be able to establish law to support the electronic voting system. The voting public's consensus to the electronic voting is quite important for the parliament process too.

The typical electronic voting architecture can be found in the Fig 2. [8]. The web-based approach is useful for electronic voting systems. This technology is based on a client-server. The client-server technology has advantages in the field of support and installation.

The voting system consists four main parts [8]:

- Voting Client Subsystem (VCS)
- Voting Application Subsystem (VAS) and Ballot Database Subsystem (BDS).
- Voting Backend Subsystem (VBS) and Tallying Database Subsystem (TDS).
- Voting Results Subsystem (VRS)

In the figure 2 can be seen Voting System Architecture. The three separate parts are recognized [8]. Part A is used for casting votes and contains Voting Client Subsystem, Voting Application Subsystem and Voting Database Subsystem. Voting clients represent voting terminal in elections rooms, kiosk voting or voters own computers.

Voting Application Subsystem is represented by web-based application, which contains user interface for voters, voter validation services and communication interface for Ballot Database Subsystem.

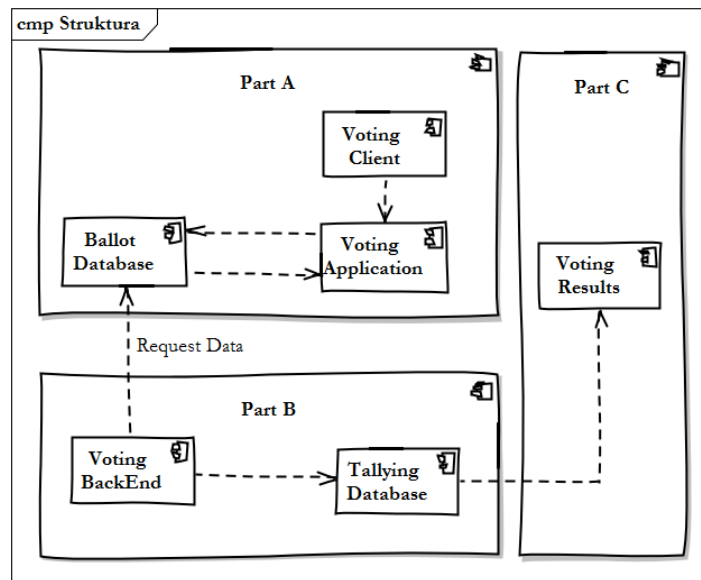


Fig. 2. Electronic Voting Architecture Design [8]

There are two most significant tasks for BDS. Votes are cast there and default ballots are generated for individual voter. Votes are cast in encrypted form, which depends on cryptographic methodology adopted for the election. For the protection against manipulation with votes in BDS HASH algorithm is implemented. HASH value is calculated irregularly based on votes, which are cast. Default ballots are generated for individual voter with respect to the election district he belongs to.

Part B represents Backend Voting Subsystem and Tallying Database Subsystem. The part B is securely connects to BDS from part A. The BVS is used by electoral committee. The BDS is responsible for auditing elections by comparing HASH based on votes and stored HASH value. The BVS deals with decryption of votes, validating of them and storing in TDS. The TDS is used for storing votes in open form. Part B is realized as web-based application and relational database server. Final part – part C – is responsible for counting final Results of the election. Part C is realized as web-based application.

Finally the last important aspect is the marketing. This classical business case is mention because there is very close link between user trust and how the system is presented and described to the public – future users. We have disused already, that user trust in technological system is based on social or more precisely mental aspects. It means users only believes or not, that system is reliable and then they trust to the system. Therefore the role of marketing seems to be significantly important. We do not deal with manipulation but with methods, how the system is presented to the users. The users need to be able to use the system in advance. In public election, is also important if the local authorities have appropriate level of the credibility.

2 Problem Formulation

In the socio-technical systems a human or humans which act as a users are taking important role. The system non-function requirements that are influencing the trustworthiness are safety, security and reliability. Those three basic aspects cannot be achieved by the technical design only [2]. The system architect has design the system with emphasis on process or procedural part of the system.

In the system engineering we usually follows basic recommendation about the system design which resulting in the reliable system. A reliable system does not equal to trustworthy system. The reliability refers to the system characteristics. It means, that users can use a system, which activity has no hazard state. The main task of this paper is to present the important characteristics, which take the key role in user's final system evaluation. Furthermore success of the on-line system is dependent on users acceptance.

The electronic voting is an example of the socio-technical systems. Technologically, there is chance to achieve an appropriate level of the reliability [3] and trustworthiness. Users of such system – voters – have usually difficulties to trust e-voting systems.

The reasons can be found in a fact of black-box design. In the following chapter will evaluate such system by using experimental study by using set of users and we will present a solution based on results of such study.

3 Study Design

The system described in Chapter 2, were used as input for our experiment. We have evaluated the system design in controlled environment by using a group of students. There were 100 person examined in our study. In the Table 1, there can be seen, that second and third grades were interested in study as two most important groups.

Table 1. % of Students in Sample by study Grade

Study Years	%
First Grade	3
Second Grade	26
Third Grade	25
Fourth Grade	17
Fifth Grade	24
Doctoral Grades	5

For the study we deals only with students, which are informatics or non-informatics discipline. In the Table 2, you can find the summery involved disciplines.

Table 2. Study discipline overview

Study Discipline	%
Informatics	70
Non-Informatics	30

As can be seen students, which are studied informatics related discipline are able to cooperate on such study more frequently.

3.1 Survey Design

There were nine basic questions, which were evaluated in our study. We have study each question in interval of four replies. In the Table 3, you can se list of question and scales, which were pre-prepared for each of examined user.

The structured questions were followed by open text filed, where each of examined subjects can enter individual response to presented voting schema design.

Table 3. List of Questions used for examination

Question	Scale
System processing speed	
System controls satisfaction	
User Interface Design	Strongly Agree
Instruction for Users	Agree
Support for EV idea	Disagree
Can EV simplify participation?	Strongly Disagree
Can EV improve participation?	

4 Results

As can be seen in Table 3 there were three questions, which represents general attitude to electronic voting. Firstly as can be seen in Fig. 3. more than 70% of participants believe, that electronic voting can be useful for improving general attitude to autonomy.

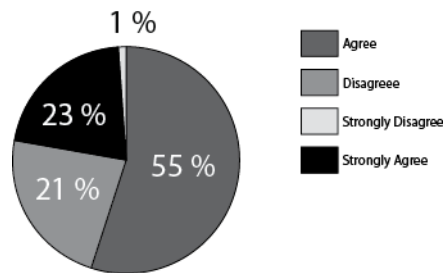


Fig. 3. Support for Electronic Voting

More than 97 % agree or strongly agree that electronic voting can improve participation in closed election. In the Figure 4, you can see that only 3 % disagree.

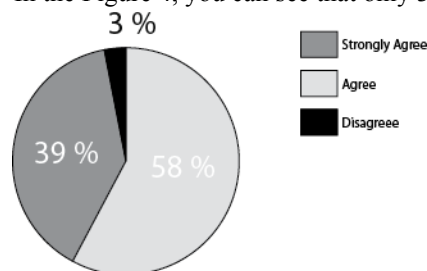


Fig. 4. Improving Participation

The majority of participants believe that electronic voting can simplify voting participation and speed-up voting process. In the Fig. 5 you can see that only 2 % disagree, that electronic voting can guarantee simplification of the voting process.

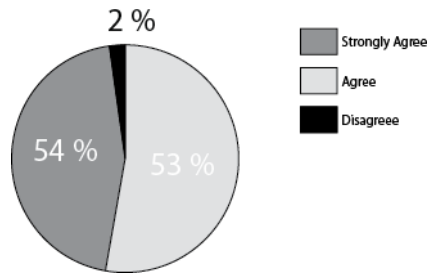


Fig. 5. Simplification of voting process

Table 4. Summary of User Evaluation

Question	Strongly agree	Agree	Disagree	Strongly Disagree
System processing speed	45	50	3	2
System controls satisfaction	30	65	2	1
User Interface Design	28	52	17	3
Instruction for Users	30	60	8	2

In the table 4 can be found the summary of user survey, which is focused on user experiences with proposed voting schema an its representation in prototype system.

In Fig. 6, there can be seen graphical representation of results, presented in Table 4.

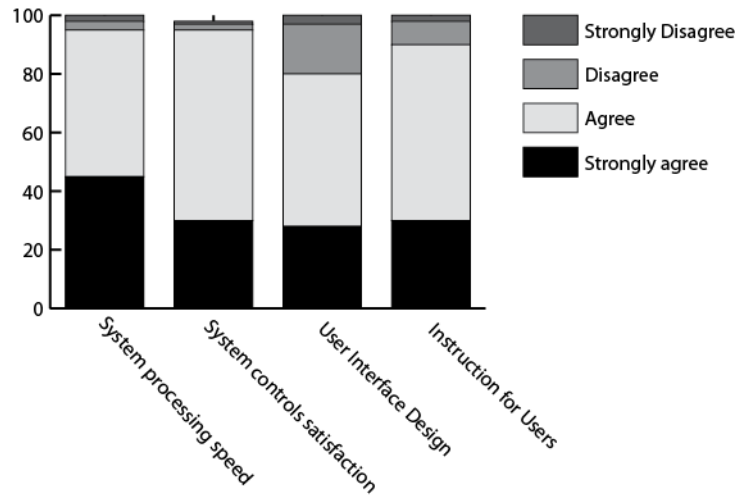


Fig. 6. Results Overview

The following system was designed as results of our study. The system is based on comments and user requirements, which were gathered in our study. We proposed a system for the closed election at the academic level.

5 Conclusion

The idea of the research was to discuss a user's trust and its issues, which are connected to the electronic voting. The electronic voting seems to be more problematic in case of system trustworthiness.

The voting system, the electronic voting system is the new approach. Users have no personal experience with using such system. According [4], [5] there is a difference between a trust and a confidence. If the users have no choice or not consider alternative solutions, they have confidence to the system. In this chapter we deal with trust, because we expected, that users have choice vote by electronic voting or by well-known legacy paper ballot based system.

Firstly, users usually trust the system if they are familiar with it. Voters trust traditional voting concepts, because they are used to participate for many years. Breaking the barrier is possible by making the electronic voting optional for participation in the election. If the voters will have the opportunity to use – study the system, they will build trustworthiness.

The system complexity is reduced if the users are familiar with the system or with similar system.

People have to believe, that electronic voting is better than legacy version of the voting process. The user familiarity is based on the user interface design.

User makes mistakes. The user interface has to follow simple schema of the voting process and only limited number of the information have to be shown. The proper design of the voting system user interface is based on showing the appropriate amount of the information. The voting schema has to follow the traditional concepts of the elections.

The user satisfaction is rising if the system behavior is predictable. The users build their model or presumptions. Therefore the predictability how the system will behave is significantly important for building system trustworthiness. The second fact, which is very close to previous discussion, is a communication between the user and system. User have to be sure, that system will be able to inform users about its state or activity. Previous thoughts are resulting in interaction design and in the principle of consistency. Consistency is a prerequisite of the predictability. Users expect, that same command or similar command will cause similar behavior of the system.

Users expect, that system will use an appropriate interaction styles. In this case we will discuss ability of confirmation messages and error messages. The ballot casting in the electronic voting is a serious task. Many of users will think about the system in that way. Therefore is useful to create deep analysis of interactions. In interaction design we deal not only with the steps of the voting schema, but also how the step should be achieved. The implantation of each step has to be non-destructive. Moreo-

ver with ability to make a back-step without data lost. The system should be communicative. It means, that each of steps will contain a confirmation message.

Secondly we will discuss a technological aspects and its impact to trustworthiness. As was shown in previous paragraphs, trust is more sociological than technological issue. This obvious fact is based [3] on the situation in which users make a certain type of the risk analysis. The mentioned analysis is subjective. Subjective analysis is usually based on user interface. The technical point deals with objective risk analysis. There is an issue, because users have to understand the system internal processes. It is impossible to for common user to understand a complex system internal processing.

In the scope of the voting system, they have been familiar with voting schema and number of non-trivial technologies. In [6], there can be found an analysis of reliable voting schema. The verification is based on mathematical approach and on empirical approach.

The key factors why users trust to the systems can be found in similarity. Users are used to trust to the similar systems. Many of the users are able to use an e-commerce system, electronic banking or electronic payments systems.

The similarity of systems is based on their core components. E-voting system and other e-processing system contains communication over the Internet, cryptography, and authentication. This fact should have a positive impact to building user trust.

The system architecture has only limited influence on the system trustworthiness. But has significant impact on user trust. Users = voters response, that trusts in the electronic voting system is based on anonymity and auditability. Users need is to check, that their ballots is counted in proper way. In means the each successful electronic voting schema have to implement a mechanisms for such control system.

Trustworthiness can be defined as user relation to the system or software solution. Firstly, users are building their option and thoughts on the experiences with the system itself. Secondly, users attitude is based on experience with the similar systems. The similarity of systems is based on their core components. E-voting system and other e-processing system contains communication over the Internet, cryptography, and authentication. This fact should have a positive impact to building user trust.

The electronic voting system design has to reflect the situation in the concrete society. There is no silver bullet solution, which is applicable everywhere. The user interface of the system should reflect the tradition of the ballot design. The basic principles of the design should reflect the core electronic voting issues – privacy, security.

This research work is not limited to potential of the electronic voting. Therefore the results and ideas should be valid for e-processing system in general.

Further research is focused on the improvement of the electronic voting, particularly in security and privacy, which seem to be important for user trust. In addition, issues connected to the cohesion among voting technology, legal principles and public attitude should be under the investigation.

6 References

1. R. J. Vidmar. On the use of atmospheric plasmas as electromagnetic reflectors. *IEEE Trans. Plasma Sci.* [Online]. 21(3). pp. 876—880. Available: <http://www.halcyon.com/pub/journals/21ps03-vidmar>
2. Balla, J. 2011, Dynamics of mounted automatic cannon on track vehicle. *International Journal of Mathematical Models and Methods in Applied Sciences*, Vol. 5, No. 1, page numbers (423-432), ISSN 1998-0140
3. Ciulanesu, M. V. & Diaconu, A. (2009). Mobile Robot Control using the Bluetooth Technology, *Annals of DAAAM for 2009 & Proceedings of the 20th International DAAAM Symposium*, 25-28th November 2009, Vienna, Austria, ISSN 1726-9679, ISBN 978-3-901509-70-4, Katalinic, B. (Ed.), pp. 1115-1116, Published by DAAAM International Vienna, Vienna
4. Ribu, K. (2001) *Estimating Object-Oriented Software Projects with Use Case*. Unvirstiy in Oslo, Oslo.
5. Silhavy R., Silhavy P. & Prokopova, Z. (2011). Clustered Requirements in System Engineering Project Estimation. *International Journal of Mathematical models and Methods in Applied Sciences*, Vol. 5, No. 1, (June 2011) page numbers (1052-1059), ISSN 1998-0140
6. Quarda, H. 2011. Cognitive tasks behavior of intelligent autonomous mobile robots, *International Journal of Mathematical Models and Methods in Applied Sciences*, Vol. 5, No. 3, page numbers (610-619), ISSN 1998-0140
7. Silhavy, R, Silhavy, P, Prokopova, Z. Systematic modeling process of system behavior. *International Journal of Mathematical Models and Methods in Applied Sciences* [online]. 2011, vol. 5, iss. 6, s. 1044-1051. [cit. 2012-10-08]. ISSN 1998-0140.
8. Silhavy, R., Silhavy, P., & Prokopova, Z. (2010). Architecture of COOPTO remote voting solution. Paper presented at the *Advanced Techniques in Computing Sciences and Software Engineering*, 477-479.