Trustworthiness in Electronic Voting System Design

PETR SILHAVY, RADEK SILHAVY, ZDENKA PROKOPOVA
Faculty of Applied Informatics
Tomas Bata University in Zlin
nám. T. G. Masaryka 5555, 76001 Zlin
Czech Republic
rsilhavy@fai.utb.cz  http://fai.utb.cz

Abstract: - In this contribution the principle of the trustworthiness and user trust is discussed. The research aim was to discuss a users trust and its issues, which are connected to the electronic voting. The electronic voting seems to be more problematic in case of system trustworthiness. Trustworthiness can be defined as user relation to the system or software solution. The four more significant factors are described.

Key-Words: - system engineering, system design, trustworthiness, electronic voting systems.

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 overview. Chapter 3 describes the problem formulation. Chapter 4 describes the selected questions, which have to be solved to achieve trustworthiness of the electronic voting. Finally chapter 5 is the discussion.

2 Electronic Voting Conditions

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 log-in 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 deals 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 described on Fig. 1 [6].

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.

3 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 dependant 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 we will try to offer a solution, which brings a better approach for system design.

4 Achieve of Trust

The voting system, the electronic voting systems 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 alternatives 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-know 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 systems. 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 behaviour 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 closed 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 behave 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 deals 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. Moreover 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.

Thirdly, the system architecture is important for building user trust. The typical electronic voting architecture can be found in the Fig 2. [6].

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.

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 discussed 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 credit.

5 Conclusion

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

Trustworthiness can be defined as user relation to the system or software solution. Firstly, users are building their opinion 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.

References: