Farhad F. Yusifov
Institute of Information Technology of ANAS, Baku, Azerbaijan
farhadyusifov@gmail.com
DOI: 10.25045/jpis.v09.i1.03

RANKING OF THE ELECTRONIC VOTING SYSTEM SECURITY THREATS ON THE BASIS OF MULTI-CRITERIA EVALUATION METHOD

E-voting is considered one of the most important applications of e-democracy. Although the implementation of the e-voting system has various purposes, the main advantages are the selection of candidates with the appropriate competencies, increased mobility of voters, participation of citizens outside the country in the elections, expansion of disabled individuals' access to democratic procedures, independent and operative proclamation of election results and etc. Security issues play a crucial role in the implementation and development of e-voting systems. The article examines the approaches to e-voting systems and the security threats to the system. An empirical evaluation of security threats to e-voting system based on the multi-criteria evaluation method is reviewed.

Keywords: *e-voting, Internet voting, e-democracy, security threat, multi-criteria evaluation.*

Introduction

E-voting system is one of the most important applications of e-democracy in terms of voting secrecy, protection of personal data and transparency [1, 2]. E-voting is the most vital components of e-democracy covering actual research areas such as mechanisms of participating in voting, provision of security and legitimacy, technological solutions for e-voting and their efficient use. In a complex approach, e-voting is referred to an important part of e-elections.

Different approaches to voting types with the use of ICT are available in scientific sources, and there is a need for the unification of the terms used. Basically, the terms "e-voting" and "Internet-voting" are used to express online voting [2-4]. Although the term "e-voting" is broadly used, "Internet voting" is only one of its forms.

E-voting has already implemented by governments due to the rapid development of information technology and advanced cryptographic techniques. Nonetheless, taking into consideration the democratic principles, e-voting procedures and its security issues are still being argued. Transparency of voting process in the political arena, calculation of votes in accordance with the democratic principles, protection of the rights of candidates and voters are of great importance.

The application of the e-voting system can influence the existing political processes in the country and relates to critical security systems [5]. From this point of view, identifying and evaluating the security threats to e-voting is one of the topical issues for ensuring the transparency and citizen's involvement in democratic processes. In this study, the gaps in the e-voting system are explored and the evaluation of security threats to the system is considered.

E-voting for e-democracy

The development of e-voting, public forums, open government, public opinion analysis and feedback mechanisms are the basis of e-democracy formation, which is the final stage of e-government establishment [6]. E-democracy, particularly e-voting, has led to broad discussions in practice and literature [4-7]. As the major discussion topics, the security issues and the impact of e-voting on socio-political processes are highlighted. Therefore, security issues play a crucial role in the application of e-voting systems. Voting is viewed as a system that is characterized by the participation of citizens in democratic processes and shapes the general opinion. However, many experts estimate e-voting as more complex and sensitive system. Security of the election process must be considered at the national security level. Because, legitimacy of democracy depends on the transparency, openness and trustworthiness of elections. From this point of view, e-voting

system has commitments in society, and its failure can lead to serious problems related to the confidence of citizens in political processes [7].

In general, the tendency of decrease in the number of voters participating in the election process creates new opportunities for e-voting, which is supported by the rapid expansion of Internet access. No unambiguous approach to e-voting is available in any scientific literature or electoral practices [7]. Some researchers believe that e-voting is a technological solution emerged due to the consideration of voters' convenience in terms of e-democracy development. On the other hand, a group of experts believe that the voters', particularly young people, participation in the electoral process can be ensured through e-voting.

To facilitate e-voting and to ensure its more efficient and inexpensive realization, it should be implemented in the following two forms with the use of electronic tools: e-voting observation - requires a representative of government or electoral authority and/or remote e-voting - does not require an observation by the representative and can be implemented via the Internet voting or mobile devices [2,5,7]. In the context of remote e-voting via the Internet, e-voting solutions in the literature are grouped into three major categories: booth voting, Internet voting in the voting center, and remote Internet-voting [7]. Although different approaches to e-voting are available today, it is believed that mobile voting solutions are estimated to be developed in the near future taking into account the factors urging e-voting.

E-voting system

Implementation of e-voting system may reduce the errors occurred in the election process, ensuring the comprehensiveness, transparency and convenience of the election process. Despite the advantages of using e-voting system, this process is accompanied by numerous social, legal and technical problems. Moreover, the problems may also include provision of equal access to voter centers, confidentiality, prevention of intervention, threat assessment, verification, modification and approval of other procedures, universal confirmation, voting right, preservation of the principle of "one voter and one vote", and error resistance. From this point of view, the inevitability of transforming legal restrictions into technical and security solutions should be emphasized. The factors imposing e-voting are:

Security: One of the most argued issues in the application of the voting system is security [8-11]. Obviously, in the traditional election system, it is impossible to identify voters by their votes. Because, the election process is carried out through secret ballot, and each voter drop the attached envelope into the ballot box. Each voter follows the principle of confidentiality. However, this does not mean the transparency of the election process. For example, a voter has no guarantees that his/her voice will not be changed later. Despite the e-voting efforts to ensure security, e-voting is considered as a real threat to the confidentiality of personal data.

Transparency failure: Undoubtedly, ensuring security requirements with information technology, and even using cryptographic techniques and tools promotes transparency in the election process. However, it is uncertain whether the voters will have difficulties to accept and follow safety requirements or not [4,5,8 , 9].

e-Democracy development: Developing efficient e-voting mechanisms is crucial for shaping and developing e-democracy. Government agencies, political parties and politicians focus on e-voting as a powerful tool for ensuring democratic principles. E-voting is of great importance in terms of eliminating digital divide in the developing countries that initiate the democracy, establishing close links between provinces and centers, preserving democratic values and holding fair elections.

Election fraud: It should be noted that security of traditional elections are based on the human trust and independence of election committees. Past experiences reveal that in developing countries with emerging democratic rules, the trust in these mechanisms is low. And, therefore, transition into technical security, i.e., cryptographic coding may be more effective rather than the

organizational security. It should be noted that the joint use of organizational and technical security measures is gradual. In other words, if the organizational authorities are corrupted, even the most reliable technology can be abandoned. Additionally, joint use of organizational and technical security measures will gradually have the same character [9, 12-14].

Voter participation: The impact of E-voting on the voter attendance is expected to be characterized not only by the voting form, but also by relevant cultural, political and geographical conditions. For example, low density of the Australian population, migration of majority of Estonian population to other European countries due to unemployment, the resettlement of voters in the countries of political conflict or war, etc.

Eliminating invalid votes: Invalid votes may be intentional and unintentional stemmed from technical issues. Fraud of votes is regarded as a step contradicting the democratic principles. The increase in the number of invalid votes puts the election results under suspicion.

Invalid votes in the e-voting process can be detected during inspection. Adjustments to the software through feedback can minimize the number of invalid votes. From this point of view, this kind of obstacles, which restrict the democratic "equality principle," should be officially investigated whether they are legitimate or not [1-4,13,15].

Cost saving: The costs can be minimized with the physical presence in voting and the minimal number of staff recruitment or reductions in travel costs. On the other hand, building voting system requires providing the voters with the necessary technical equipment. In addition, in the near future, the polling stations will lose their power in political elections. Despite all this, e-voting is still the subject of discussion in terms of saving money spent on the election.

In the scientific literature, the legal framework for elections is extensively argued, and, consequently, it is believed that legal solution of the problem is related to the transition from law to technology.

The gaps in e-voting system

Modern democratic countries hold elections through e-voting system. The use of ICT makes the electoral process more effective in terms of voting and increasing the number of voters. This is explained by the fact that e-voting facilitates and supports the voting process. The main contribution of e-voting and, in particular, Internet-based voting systems, is the voters mobility support, which in turn enables voters to attend elections from anywhere via the Internet access. The key gaps associated with e-voting are related to the voter authentication and, principally, threats to the Internet voting software, such as viruses, malware, and Trojan horse [5]. Internet voting problems may include completeness of voter information, reliable transfer and storage of votes, prevention of voice duplication and so forth [5,7-13].

There are many vulnerabilities related to different e-voting systems [2-5,8,11-14]. Most available e-voting systems are not satisfactory for holding reliable elections, since current practice shows that there is no evidence to prove their truthfulness. The main reason for restricted implementation of e-voting is the lack of confidence. However, in the near future, the development of effective mechanisms promises more reliable e-voting.

E-voting system is grouped into 3 main categories: hardware, software and human factor . The safety elements of hardware include electromechanical and electrical parts [2]. Security features of software include operating systems, compilers, databases, software rules, and so on. Ease of use, transparency, confidence, and adoption are the security elements for humanware or voter. In literature and practice, each category is equally important in terms of safety [2].

Regulation of functional and constitutional obligations by the state leads to deal with numerous problems of e-voting system. From this point of view, e-voting system must totally meet the electoral principles. This approach becomes security requirement for technological solution and must be implemented in the voting environment. Technical and security features of effective e-voting system include accuracy, verification, democratization, agility, mobility, reliability,

unchangeable, public acceptance, etc. Other desired requirements include comfort, transparency, measurable and economic feasibility. Although there are various approaches to e-voting security in scientific literature, most of above requirements are unambiguously accepted by researchers [1, 13–17].

However, some of requirements are controversial. For example, the controversy emerging the conflict between authentication and confidentiality is the requirement to verify whether the voter has the right to vote or not, including the requirement to provide the confidentiality of the voter's vote.

Security threats to e-voting system

Research in the field of e-voting is considered to be one of the important aspects in the development of e-democracy mechanisms. Establishing comfortable and secure e-voting system can become a powerful tool for gathering people's ideas and opinions in cyberspace. E-voting system can be attacked in different ways. Threats can cause the system failure by affecting its different security areas. Potential threats to e-voting system may include the followings [5, 8, 9–11, 15]:

Technical vulnerabilities. Software developers or system administrators create an inaccessible administrator account for operators. Administrator account is used for troubleshooting, prevention of system errors, or for personal purposes. These accounts can be hijacked and used for malicious purposes. These vulnerabilities are referred to technical threats.

Denial of Service - DoS attack. DoS attacks cause destructive results and, in most cases, affect the system stability making it inaccessible. Hackers may endanger e-voting system access using various methods, including the Ping of Death and Packet Flooding. These types of attacks do not affect all systems in the same way. Thus, some systems may stop functioning, while others may not be affected at all.

Viruses. Computer virus is a computer program with self-recover function and cause undesirable effects on computers where it is activated. Viruses can destroy e-voting system. A virus attack can jeopardize the system access in the course of election and force the government and institutions to hold re-election. Attacks on emails are most common attacks and referred to technical threats.

"Worms". These viruses are spread without modifying available programs and files. It spreads to become active in other systems by creating own copies on infected computers. If a virus is intentionally developed, it may invalidate elections by changing files and voting results.

"Trojan horse". The Trojan horse virus is a malicious program code downloaded once the computer is connected to the Internet. At first glance, this virus can seem undisruptive; however it may delete an important file on computer, create a malicious virus, and even seize user passwords. This virus is a serious threat to the data integrity and confidentiality in e-voting system.

"Phishing". Some "phishing" swindlers develop forged Web pages similar to legitimate ones and illegally get voter information, and misrepresent election results using their rights. This threat may be related to both technical and social categories depending on the type of attack.

Physical attacks. Numerous physical attacks to e-voting system can be realized to disrupt the electoral process. Malefactor's access to the Internet and interference to the power supply can ultimately lead to the loss of votes. Hard drive or smart-card removal or substitution with fraudulent data, and capturing voter's personal data is a serious threat to e-voting process.

Threats to the integrity of computing subsystem and system. Computing subsystem attacks may falsify and alter it through the client software or the server in accordance with the malefactor's request. This threat can be classified into both technical and social threats.

Threats to User computer. In scientific literature, compared to other operating systems, the Windows system is estimated to have more vulnerabilities. When updating any popular software in the Windows environment, the viruses such as "Trojan horse" and "backdoor" can be invisibly

uploaded to the computer while the user computer is run for various purposes. Widespread use of this operating system and the availability of numerous gaps and being easily defined by hackers may cause serious threat to e-voting.

Empirical calculation

Assume that local elections are decided to be held via e-voting system. The ranking of threats to e-voting system using the multi-criteria assessment method is reviewed. The following four threats are predicted to e-voting system: $A=\{A_1, A_2, A_3, A_4\}$.

Here, A_1 - denotes DoS attacks, A_2 - virus attacks, A_3 - phishing threats, and A_4 - physical attacks.

The criteria used to evaluate the threats are as follows: $C=\{C_1, C_2, C_3\}$

C_1 - denotes the system interruption, C_2 - violation of data integrity and confidentiality, C_3 - falsification of election results.

Step 1. If the Saaty approach [18,19] is used, then the ranking $\frac{R_i}{R_l}$ of alternatives on each criterion $c_j \in C$ can be shown as follows. Here, A_l - is the worst $l-ci$-th alternative among the alternatives A_i $(i=1,4)$.

$$\frac{R_i}{R_l}=\begin{cases} 1, \text{ if identitic to } A_i\ A_l, \\ 3, \text{ if relatively better than } A_i\ A_l, \\ 5, \text{ if better than } A_i\ A_l, \\ 7, \text{ if much better than } A_i\ A_l, \\ 2,4,6 - \text{mean values.} \end{cases}$$

Evaluation of each threat by criteria is shown in Table 1.

	C_1	C_2	C_3
A_1	7	5	2
A_2	5	1	3
A_3	3	6	1
A_4	1	4	7

Table 1. Evaluation of threats by criteria

Step 2. Assume that alternative A_l is the worst alternative with weight w_l and rank R_l. Using the worst-case method, the weight of the worst alternative for each criterion is calculated using the following formula [19, 20]:

$$w_l=\frac{1}{\sum_{i=1}^{4}\frac{R_i}{R_l}}$$

According to the worst-case method, the condition $w_1+w_2+...+w_l=1$ is met and the weights of remaining alternatives are calculated [19]. Table 2 illustrates the weight of alternatives calculated through the worst-case method. The calculated weight of alternatives by criteria allows to express the criteria as fuzzy universal sets [19].

Table 2. Weights of alternatives calculated through the worst case method

	C_1	C_2	C_3
A_1	0,438	0,333	0,154
A_2	0,313	0,067	0,231
A_3	0,188	0,400	0,077
A_4	0,063	0,200	0,538

Step 3. According to the Belman-Zadeh principle, the best alternative (A_{opt}) can be found within the intersection of the fuzzy sets of these criteria [19]. Then, intersection $A_{opt} \in D = C_1 \cap C_2 \cap C_3$ builds a fuzzy set. According to the fuzzy sets theory, the maximum weighted alternative $A_{opt} \in D$ is chosen as the best alternative (A_{opt}) by replacing the intersection with $\cap \to \min$. As can be seen in Table 3, alternatives are ranked in the following sequence: A_1, A_3, A_2 and A_4.

Table 3. Threats ranking

	D	Rank
A_1	0,154	1
A_2	0,067	3
A_3	0,077	2
A_4	0,063	4

Step 4. According to Zadeh approach [21], alternatives can be ranked by the importance of criteria taking the weight coefficients $\alpha_1 = 0.6$ (very important), $\alpha_2 = 0.3$ (important) and $\alpha_3 = 0.1$ (less important). The weights of alternatives are shown below.

$$D^{\alpha} = \left\{ \frac{0,015}{A_1}, \frac{0.02}{A_2}, \frac{0.008}{A_3}, \frac{0.038}{A_4} \right\}$$

As it is seen, threats are ranked by the importance of criteria in the following sequence A_4, A_2, A_1 and A_3.

Conclusion

E-voting is distinguished from any other electronic transaction for its significance. Violation of the right to secret ballot in e-voting can lead to political conflicts and social disorder. From this point of view, e-voting is a real threat to the confidentiality of personal data. The problem of phishing, viruses, and spy programs still remain a serious threat to voters and e-voting system. The article examined the approaches to e-voting system and factors that make the system more relevant, and its security threats. Based on the multi-criteria assessment method, the weights of all alternatives were calculated using the worst-case method for solving the issue of empirical assessment of security threats to e-voting system. The threats were ranked based on Belman-Zadeh's principle.

Based on the analysis of extant practices in the field of e-voting, it can be concluded that security threats to e-voting system at the local level should be assessed and empirical research should be preferred. This issue is particularly urgent and important for developing countries. E-voting mechanisms to be developed, given the security features of e-voting system will allow solving numerous problems.

References

1. Abu-Shanab E., Knight M. and Refai H. E-voting systems: a tool for e-democracy management research and practice // Management research and practice, 2010, vol. 2 (3), pp. 264-274.
2. Mursi M., Assassa G. and et al. On the Development of Electronic Voting: A Survey // International Journal of Computer Applications, 2013, vol. 61(16), pp. 1-13.
3. Musial-Karg M., The use of e-voting as a new tool of e-participation in modern democracies, 2014, http://www.pressto.amu.edu.pl
4. Schryen G. Security Aspects of Internet Voting / Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04), 2004, https://www.ssrn.com
5. Li X.Sh., Lee H.R., Lee M. and Choi J.-Y. A Study of Vulnerabilities in E-Voting System // Advanced Science and Technology Letters, 2015, vol. 95, pp.136-139.
6. Van der Meer T. G.L.A, Gelders D. and Rotthier S. E-democracy: exploring the current stage of e-government // Journal of Information Policy, Penn State University Press, 2014, vol. 4, pp. 489-506.
7. Stoica M., Ghilic-Micu B. E-Voting Solutions for Digital Democracy in Knowledge Society // Informatica Economică, 2016, vol. 20 (3), pp. 55-65.
8. Al-Ameen A. and Talab S. The Technical Feasibility and Security of E-Voting // The International Arab Journal of Information Technology, 2013, vol. 10(4), pp. 397-404.
9. Ssekibuule R. Security Analysis of Remote E-Voting // Advances in Systems Modelling and ICT Applications, 2007, http://www.cit.mak.ac.ug
10. Javaid M.A. Electronic Voting System Security, 2014, https://www.papers.ssrn.com
11. Lauer T. W. The Risk of e-Voting // The electronic journal of e-government, 2004, vol. 2 (3), pp.147-218.
12. Kang B. Cryptanalysis on an e-voting scheme over computer network / International conference on computer science and software engineering, 2008, pp. 826-29.
13. Cetinkaya O. and Cetinkaya D. Verification and Validation Issues in Electronic Voting // The electronic journal of e-government, 2007, vol. 5 (2), pp.117-126, http://www.ejeg.com
14. Wang K.-H., Mondal S.K., Chan K. and Xie X. A Review of Contemporary E-voting: Requirements, Technology, Systems and Usability // Data Science and Pattern Recognition, 2017, vol. 1 (1), pp. 31-47.
15. Dhillon K., Challenges for LargeScale Internet Voting Implementations, 2015, http://www.cs.princeton.edu
16. Qadah G.Z., Electronic voting systems: Requirements, design, and implementation // Computer standards and interfaces, 2007, vol. 29 (3), pp. 376-386.
17. Okediran O.O., Omidiora E.O., A Framework for A Multifaceted Electronic Voting System // International Journal of Applied Science and Technology, 2011, vol. 1 (4), pp. 135-142.
18. Saaty T.L. Decision making with the analytic hierarchy process // International Journal of Services Sciences, 2008, vol.1 (1), pp. 83–98.
19. Rotshtein A.P. Fuzzy multicriteria choice among alternatives: Worst-case approach // Journal of Computer and Systems Sciences International, 2009, vol. 48 (3), pp. 379-383.
20. Alguliyev R.M., Aliguliyev R.M., Mahmudova R.M. A Fuzzy TOPSIS+Worst-Case Model for Personnel Evaluation Using Information Culture Criteria // International Journal of Operations Research and Information Systems, 2016, vol. 7 (4), pp. 38-66.
21. Zadeh L.A. A Very Simple Formula for Aggregation and Multicriteria Optimization // International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2016, vol. 24 (6), pp. 961–962.