Mathematical Problems of Computer Science 57, 39–46, 2022.
doi: 10.51408/1963-0085

UDC 004.05

Electronic Voting System Essentials and Problems

Arman A. Avetisyan

Russian-Armenian University
e-mail: armanavetisyan1997@gmail.com

Abstract

The development of reliable and safe e-voting systems is relevant because of the wide range of applications. This paper provides an analysis of modern electronic voting systems based on security criteria. An analysis was conducted based on the most popular modern e-voting system architectures. The analysis provides a baseline for developing a secure e-voting system.
Keywords: Electronic voting, Internet voting, Information security, Elections, System architecture, Voting systems.
Article info: Received 18 February 2022; received in revised form 16 September 2022; accepted 15 November 2022.
Acknowledgement: The work was supported by the Science Committee of RA, within the framework of the research project 21T-1B151.

1. Introduction

Electronic voting (e-voting) is a term that encompasses several different types of voting methods and electronic means of counting votes. E-voting systems include punched cards, optical voting systems and specialized voting kiosks (including stand-alone electronic systems for direct voting), as well as means for the transmission of ballots and votes by telephone, via a private computer network or via the Internet [1]. Such systems would speed up the counting of votes and make voting more accessible and transparent. However, weak e-voting systems could encourage electoral fraud. The advantages and disadvantages of modern e-voting solutions and technologies should be explored in order to create a secure system. This study focuses on the electronic systems through which the entire electoral process (voter registration, voting and counting votes) is conducted. The study distinguishes the standard functionality of e-voting systems.

Standard e-voting systems include the following modules [2]:

- electronic voter lists and a method of voter identification,
- interface for polling station staff,
- interface for voters,

- system for sending votes to count,
- interface to show results.

The e-voting system should correspond to a series of criteria, which can be divided into two important groups: primary - based on the security and safety of the system, and secondary - based on the user friendliness and accessibility.

System safety requirements are:

- **integrity of elections** (ensuring the accuracy of the elections, all the ballots should be accounted for and no changes must be made to them),
- **privacy of the vote** (make ballots indistinguishable from one another, as well as protect any information about the voter),
- **authenticity of the voters** (only eligable voters can take part in elections),
- **verifiability of the votes** (a person should be able to verify that his vote has been cast and counted),
- **protection against attacks** (the system should be secure against attacks in any phase of the elections, and the voters should be able to alert the committee if any fraud has been detected),
- **ensuring the confidentiality of personal data** (no voter should be able to prove to a third party that he voted for a particular person).

At the international level, the systems developed and tested today have some security problems. A great deal of scientific literature has been devoted to this study [2] - [5], but a number of questions still remain. Even the best e-voting systems today have some drawbacks.

In [6], the author reviewed electoral systems in some countries, where e-voting was used during elections. The comparative analysis was carried out on the basis of the main safety criteria of the most popular modern e-voting systems used in several countries. The study showed that the systems used nowadays are insecure against external attacks and thus raise questions about the integrity of elections they are used in. Most of the systems were implemented more than a decade ago, and the security protocols used have gone obsolete since then. Even the best systems that are steadily replacing paper voting, have been criticized by third-party studies due to massive vulnerabilities. The need for secure and reliable e-voting systems remains a relevant problem nowadays. This paper proposes a model based on the most popular practices in modern e-voting systems.

2. E-voting System Architecture

In the last twenty years there has been active research into the creation of secure voting systems. These systems are based on public-key cryptography and on the approach that the voter's vote is encrypted with a public key that corresponds to it. The private key is distributed among the members of the electoral commission, so the members of the electoral commission will be able to decrypt and count the votes together. In addition, special methods are used to ensure the secrecy of the ballots (MIX network, additive homomorphic encryption systems...). This study proposes a baseline system architecture based on e-voting systems and protocols used nowadays, as well as their known vulnerabilities.

First, we outline the basic voting procedure, divided into 5 key phases:

- **setup phase** - setting up the election system architecture,
- **e-ballot filling phase** - filling out an e-ballot on a device and casting the vote,
- **e-ballot registration phase** - checking if the e-ballot is eligible and storing it on a server,
- **anonymity phase** - making sure all the voter info is stripped away from the e-ballot,
- **counting phase** - counting all the anonymous ballots and providing the results to public.

2.1 3-Server Architecture

The proposed e-voting system architecture consists of 3 main servers (see Fig. 1):

- **Vote forwarding server** is the only publicly accessible server. It verifies the eligibility of the voter and acts as an intermediary to the backend vote storage server.
- **Vote storage server** is a backend server that stores signed, encrypted votes during the online voting period. Upon receiving a vote from the forwarding server, it confirms that the vote is formatted correctly and verifies the voter's digital signature.
- **Vote counting server** is never connected to a network and is only used during the final stage of the election to count the votes received from the storage server.

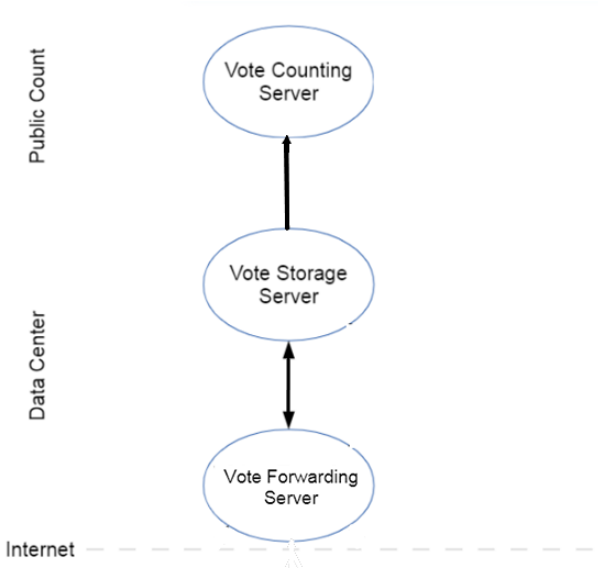

Fig. 1. 3-Server architecture.

2.2 Voting Process

During the initial voting stage, the voter uses client software to cast a vote. The software has a connection with a forwarding server, which is used to authenticate the voter and check their eligibility. All communication with elections servers is done via the vote forwarding server which is the only server accessible from the voter's device. The vote forwarding server is an intermediary between the client device and the storage server. After the voter is authenticated, the client receives a package with a set of candidates. When the voter picks a candidate, the software encrypts the information about the candidate and signs the data with the unique key of the voter.The software then sends the encrypted data package to the forwarding server which returns an ID of the package meaning the vote has been successfully casted. It is important to note that no information about the voter is sent to the election server other than their unique signature which can only be used to check the eligibility of the vote and not the identity of the voter.
The transfer of this data between the forwarding server and storage server remains a huge issue even nowadays because each part of the system trusts the channels through which the vote data is transferred. The transfer from client to storage is done via the Internet using secure protocols (see Fig. 2).

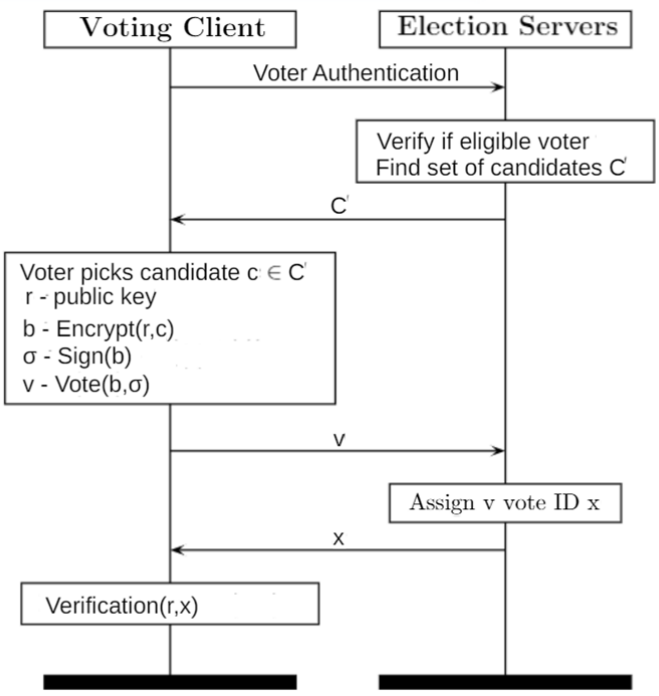

Fig. 2. Casting Vote.

When the vote data arrives at the vote storage server, it is once again checked and verified. Then the sensitive data like the unique signature is stripped from the votes to make them completely anonymous before sending to the counting server where the data (which contains only information about who the vote is for) is decrypted and tabulated (see Fig. 3).

Counting server then writes all the data into an accessible database from which the final results can be gathered.

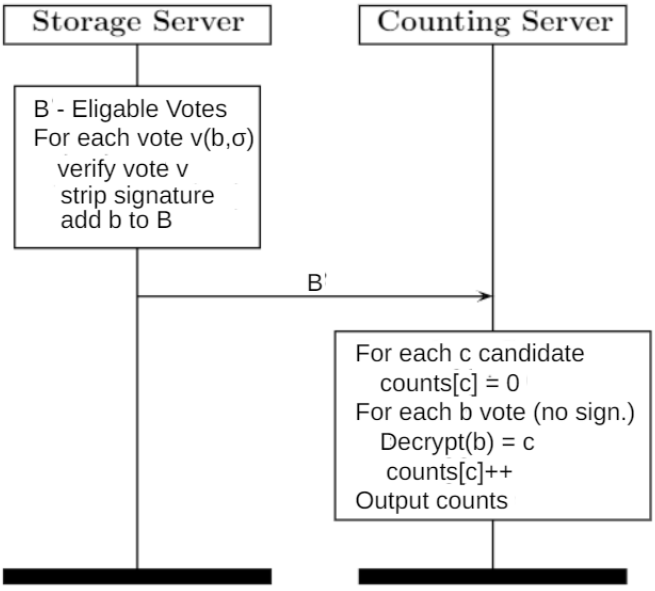

Fig. 3. Vote Counting.

The discussed system is a basic model of e-voting systems being used nowadays [7] - [10], but there are vulnerabilities and areas for improvement.

3. Discussion About Vulnerabilities

Although the system may seem straightforward and secure, its current implementations have raised serious concerns [11] - [13]. The main concern is the secure transfer of the vote data. Usage of client-side software is essential in e-voting systems so the process of transferring votes from the client device to the election server should be handled carefully. The inclusion of transfer server as a buffer between the client and the storage server is integral. We can differentiate two types of attacks: client-side and server-side.

Client-side attacks target the client device and exploit its vulnerabilities. The client software needs to be as secure as possible against this kind of attacks by not having any unwarranted communication with the device.

Server-side attacks target server architecture. The system must be minimally dependent on the person or people controlling it to be secure. The human factor plays a huge role in exploiting the election systems. Another major vulnerability is the code vulnerability. Due to the complex nature of the system, current implementations have been proven to have significant oversight in security against attacks like denial of service or shell injection.

Attacks target client software or server architecture and try to achieve the following:

- find out confidential information about voters like the candidate they voted for,
- try to alter the results of the election by changing or adding fake votes,
- altering/destroying enough votes to create mistrust in the election results.

To find out information about voters, the attack needs to take place before the anonymity phase, so client-side attacks mainly take place for this purpose. If the channel between the

client software and the transfer server is not secure, the data may be intercepted and even altered. Modern cryptography methods help to encrypt data, so it is hard to decode, but adding noise to an insecure channel to alter or ruin the vote is easy if someone already has access. These attacks are generally low-scale as user devices need to be exploited one by one, even with techniques like botnets it is unlikely to cause too much harm to the overall security of elections.

The main damage to elections is caused by attacking storage and counting servers and the channel between them. As all the important vote databases are in those servers, if access is received by an attacker, the damage to elections will be massive. Having a good and secure architecture is the key to preventing that from happening. Currently, the systems use physical data transfer from one server to another, as well as a physical decryption device that holds the key. This relies too much on actual human beings to securely transfer a lot of essential data from one point to another, and the whole point of implementing e-voting is to get rid of the human factor. This also means that the storage server must be easily accessible for humans to put in data, which is not ideal.

We see that modern systems in use still use "hybrid" systems partly run by people to make up for software vulnerabilities that need to be addressed in the future works when it comes to developing better e-voting systems.

4. Conclusion and Future Work

The paper discussed the basic architecture of the e-voting system, which is the baseline of systems used nowadays. Understanding the potential problems and vulnerabilities is essential to creating a secure e-voting system. The 3-server architecture is a good starting point to build a new system. It is evident that the physical transportation of data in modern systems is the key problem that has to be addressed first. The use of various steganographic models can help to reduce the risks of data corruption and tampering. More specifically, the steganography models with active adversary are very close to imitating attacks that can happen during elections. One of the main focus points of more secure systems will be the testability, it is essential to have an ability to quantify the level of security of the model. To achieve this goal, research has to be conducted in various fields of security, specifically steganography and differential privacy.

References

[1] M. Stenbro, *"Survey of Modern Electronic Voting Technologies"*, The Norwegian University of Science and Technology, Master Thesis, 2010.

[2] International IDEA *"Introducing Electronic Voting: Essential Considerations"*, https://www.corteidh.or.cr/tablas/28047, 2011.

[3] K. Sanjay and E. Walia, "Analysis of electronic voting system in various countries", *International Journal on Computer Science and Engineering*, vol. 3, no. 5, pp. 1825–1830, May 2011.

[4] V. Martin, "Evaluation of internet voting systems based on requirements satisfaction", *International Review of Social Sciences and Humanities*, vol. 6, no.1 , pp. 41-52, 2013.

[5] A. T. Sherman, R. A. Fink, R. Carback and D. Chaum, "Scantegrity III: Automatic trustworthy receipts, highlighting over/under votes, and full voter verifiability", *In Proceedings of the Electronic Voting Technology/Workshop on Trustworthy Elections, EVT/WOTE*, 2011.

[6] A. Avetisyan, "Comparative analysis of modern E-voting systems based on security criteria",*Proceedings of International Conference CSIT 2021*, Yerevan, Armenia, pp. 81-84, 2021.

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

[8] L. Loeber, "E-Voting in the Netherlands: from general acceptance to general doubt in two years, *3rd International Conference on Electronic Voting*, pp. 2130, 2008.

[9] D. F. Aranha and J. van de Graaf, "The Good, the Bad, and the Ugly: Two decades of E-voting in Brazil", *IEEE Security and Privacy*, vol. 16, no. 6, pp. 22-30, Nov.-Dec. 2018.

[10] M. Hapsara, A. Imran and T. Turner, "E-Voting in developing countries", *Electronic Voting. E-Vote-ID 2016. Lecture Notes in Computer Science*, vol. 10141, pp. 3655, 2017.

[11] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine and J. Halderman, "Security analysis of the estonian internet voting system", *Proceedings of the 21st ACM Conference on Computer and Communications Security*, pp. 703-715, 2014.

[12] T. Haines, S. J. Lewis, O. Pereira and V. Teague, "How not to prove your election outcome," *IEEE Symposium on Security and Privacy (SP)*, pp. 644-660, 2020.

[13] M. A. Specter, J. Koppel and D. Weitzner, "The ballot is busted before the blockchain: a security analysis of voatz, the first internet voting application used in U.S. federal elections", *Proceedings of the 29th USENIX Conference on Security Symposium. USENIX Association*, pp. 1535-1552, 2020.

Էլեկտրոնային քվեարկության հիմունքները և խնդիրները

Արման Ա. Ավետիսյան

Ռուս-հայկական համալսարան, Երևան, Հայաստան
e-mail: armanavetisyan1997@gmail.com

Ամփոփում

Հուսալի և անվտանգ էլեկտրոնային քվեարկության համակարգերի մշակումն արդիական է կիրառությունների լայն շրջանակի պատճառով: Աշխատանքում ներկայացվում է ժամանակակից էլեկտրոնային քվեարկության համակարգերի վերլուծություն՝ հիմնված անվտանգության չափանիշների վրա: Վերլուծությունն իրականացվել է՝ հիմնվելով էլեկտրոնային քվեարկության ամենահայտնի ժամանակակից համակարգերի վրա: Վերլուծությունը հիմք է հանդիսանում անվտանգ էլեկտրոնային քվեարկության համակարգերի մշակման համար:

Բանալի բառեր՝ էլեկտրոնային քվեարկություն, ինտերնետ քվեարկություն, տեղեկատվական անվտանգություն, ընտրություններ, համակարգի ճարտարապետություն, քվեարկության համակարգեր:

Основы и проблемы электронного голосования

Арман А. Аветисян

Российско-Армянский университет, Ереван, Армения
e-mail: armanavetisyan1997@gmail.com

Аннотация

Разработка надежных и безопасных систем электронного голосования актуальна из-за широкого спектра применений. В данной работе был проведен анализ современных систем электронного голосования на основе критериев безопасности. Анализ проводился на основе наиболее популярных современных архитектур систем электронного голосования. Данный анализ является основой для разработки безопасной системы электронного голосования.

Ключевые слова: электронное голосование, интернет-голосование, информационная безопасность, выборы, архитектура системы, системы голосования.