Towards Secure E-Elections in Turkey: Requirements and Principles

Orhan Cetinkaya
Institute of Applied Mathematics,
METU, Ankara, Turkey
e113754@metu.edu.tr

Deniz Cetinkaya
Department of Computer Engineering,
METU, Ankara, Turkey
e131263@ceng.metu.edu.tr

Abstract

E-democracy is a necessity in this era of computers and information technology. E-voting is one of the most significant parts of e-democracy, which refers to the use of computers or computerized voting equipment to cast ballots in an election.

This is a study on e-voting requirements specifically pointing out its implementation in Turkey. Nowadays, the Turkish Government has begun to test an e-voting system, which has been developed by a private company for Turkish electoral needs. Since there is neither technical nor academic comprehensive documentation available regarding the system, we are not sure about that it may or may not be a satisfactory solution to Turkish electoral needs.

The aim of this paper is to define an extensive set of requirements that any e-voting system, which is planned to be used instead of paper-based voting system in the countries that have representative democracy so as in Turkey, should satisfy.

1. Introduction

Electronic election (e-election) is a security-critical application of electronic democracy (e-democracy). Since electronic voting (e-voting) is the most significant part of the e-election, they are generally used with the same meaning. Due to the rapid growth of computer technologies and advances in cryptographic techniques, e-voting is now an applicable alternative for many non-governmental elections. However, security demands become higher when voting takes place in political range. Hence, it is not easy to say that e-voting is likely to become viable soon for governmental elections.

E-voting is an inter-disciplinary subject and should be studied together with the experts of different domains, such as software engineering, cryptography, politics, law, economics and social sciences. Although many people have worked on this subject, mostly e-voting is known as a challenging topic in cryptography.

Up to now, many e-voting protocols have been proposed; some of them have been implemented and tested in different countries [2]. Mainly, we can talk about two different approaches. In the first one e-voting is done at voting booths or in voting pools. In the other one e-voting is done over the Internet which is also called as I-voting. I-voting is mostly studied in the countries where postal voting is legally used. However, in Turkey postal voting is not allowed.

Belgium, the Netherlands, the USA, Russia, Azerbaijan, Brazil, Paraguay, and India offer e-voting at polling stations at a large scale. Furthermore Japan, Germany, Canada, Portugal, Denmark, Venezuela and Australia perform e-voting tests at a mid-scale. Remote I-voting at real elections and referenda are used at pilots in England, Switzerland, France, Spain, the Netherlands and Estonia. Italy, Denmark, Portugal, Germany, Austria, and some others also accomplish I-voting tests. Also, there are different e-voting studies in Ireland, Slovenia, Hungary, Malaysia, Korea, New Zealand, Finland and Bulgaria [3].

In Turkey, e-voting studies started more than 20 years ago. Nowadays, the Turkish Government has begun to test the Electoral Roll Information System (SECSIS) which was started in 1986 and lastly developed by a private company in order for Turkish electoral needs. Unfortunately, there is no technical or academic comprehensive documentation available regarding the system. So, we are not sure about that it may or may not be a satisfactory solution to Turkish electoral needs. It should be discussed by academicians whether SECSIS meets e-voting requirements or not. Otherwise, it is hard to trust it.

In all proposed e-voting protocols and implementations, different sets of requirements are defined and almost all academic studies focus on a subset of the requirements. The requirements are generally well defined in some big projects where the implementation issues have more importance.

Requirement analysis is an important part of the system design process and it is impossible to develop the right system in the right way without correct and complete set of requirements.

In some countries, where e-voting is studied not only commercially but also academically, there are several studies about e-voting requirement analysis and/or implementation issues. In [6], basic requirements for any voting system are defined and the e-voting system bought by the Irish Government is examined to see whether it can meet those requirements. In [7], a structural security framework for e-voting systems is presented. [8] deals with the legal requirements for e-voting in Austria. [10] addresses the democracy-oriented legal and constitutional requirements for any e-voting system.

The aim of this paper is to define an extensive set of requirements that any e-voting system, which is planned to be used instead of paper-based voting system in the countries that have representative democracy so as in Turkey, should satisfy. This paper has importance since it can be base reference for new studies on e-election or e-voting, and it can be useful on evaluation and test phases of already started studies.

The remainder of the paper is organized as follows. The next section provides overview of the paper-based voting system in Turkey. Next, the basic procedure for an e-election is described and the e-voting requirements are explained in Section 3. Finally, conclusions are drawn and future work is suggested.

2. Paper-Based Voting in Turkey

In this section we shortly describe the traditional paper-based voting system in Turkey, which is in fact a well-known application of representative democracy.

We, in Turkey, live in a representative democracy. This means that Turkish citizens govern themselves by electing representatives to make decisions on behalf of them. Paper-based voting system in Turkey is almost as similar as voting system in other countries which have paper-based voting and representative democracy. After the announcement of the election day, registration of the voters and political parties' propagandas take place during the pre-voting period. In this period, election environment is prepared, i.e. everything is made ready to vote on the election day.

On the election day, the voter, after being authenticated by an authority, receives a blank ballot, makes his choice in a polling-booth and casts it into a ballot box in front of the authority. The anonymity is achieved by using the polling-booth and the ballot box. Then voter signs the record list to indicate that he has voted.

After the voting period is completed, the ballot box is opened and the ballots are counted by the authorities. The counting result is announced. After all counting results are combined, election result is publicized.

Voter casts his vote by himself without any influence and nobody can see voter's cast except himself. Voter cannot cast more than one vote. Vote collecting, counting and tabulating are done in front of observers and public. Meanwhile, representatives of political parties, observers of independent non-governmental organizations and international organizations are welcome to be present and can observe the election process. The voter is alone while he is casting his vote; nobody can see or coerce him. Voter is not allowed to stay in voting booth more than reasonable duration. [11]

Although paper-based voting system has been widely used for many years and it has been fulfilling almost all voting requirements, it has some problems and drawbacks. Registered voters may be impersonated at the polls. Ballot boxes and ballots may be compromised. Counting is laborious and subject to human error. Even so, election fraud has been prevented through the use of physical security measures, audit trails, and observers, representative of all parties involved. These security measures generally work well enough that the possibility of widespread fraud is small and people have confidence that election results are accurate. Any proposed e-voting system should satisfy at least the requirements which paper-based voting systems achieve.

Moreover, more people involvement should be encouraged to be a part of governing process by using multiple ways. E-election and e-referendum are ideal means to achieve this goal.

3. E-Voting in Turkey: Requirements and Principles

Although a wide variety of e-voting systems and protocols exist, the basic procedure for an e-election is almost standard [1].

Any e-voting system should include these elements:

- Voter: Voter has the right for voting, and votes in the election.
- Registration Authority(ies): Registration authority or authorities register eligible voters before the election day. These authorities ensure that only registered voters can vote and they vote only once on the election day.
- Tallying Authority(ies): The tallying authorities collect the cast votes and tally the results of the election.

Registration authorities may be registrar, authenticator, authorizer, ballot distributor, key generator and/or validator. Tallying authorities may be tallier, counter and/or verifier.

Any e-voting system should also involve these four phases [12], [13]:

- Registration: Voters register themselves to registration authorities and the list of eligible voters is compiled before the election day.
- Authentication and Authorization: On the election day registered voters request ballot or voting privilege from the registration authorities. Registration authorities check the credentials of those attempting to vote and only allow those who are eligible and registered before.
- Voting: Voter casts his vote.
- Tallying: The tallying authorities count the votes and announce the election results.

When proposing an e-voting protocol or implementing an e-voting system, it is necessary to perform these phases in a secure manner. Any e-voting protocol or application may be accepted as secure and reliable if and only if it satisfies core requirements and has basic properties. In general, the requirements for traditional paper-based voting can also be applied to e-voting. However, there are more requirements people should take into consideration in e-voting.

A widespread assumption in e-voting is using trusted components like trusted third parties, trusted authorities, trusted channels …etc. However, in any electronic application, the security and reliability of the system should be achieved without any trust on any component. The basic requirements should be assured even if everything fails and/or everyone colludes including authorities. Thus, as a general requirement, the security and reliability of the system would be provable from the cryptographic point of view.

We reviewed several sets of secure election system characteristics found in the literature [1], [13], [14], [15] and proposed an extensive requirements set. These requirements are categorized as core requirements and additional requirements based on their applicability as a result of detailed evaluation of the e-voting protocols and requirements. In the following sections these requirements are described.

3.1. Core Requirements

These requirements are mandatory for any electronic system, which is planned to be used instead of paper-based voting system. A secure system should meet these requirements. Otherwise it will not be an adequate solution to electoral needs.

- *Voter Privacy*: It is the inability to link a voter to a vote [14]. Voter privacy must be preserved during the election as well as after the election for a long time.
- *Eligibility*: Only eligible voters participate in the election [13], [15]. They should register before the election day and only registered eligible voters can cast votes.
- *Fairness*: No partial tally is revealed before the end of the voting period to ensure that all candidates are given a fair decision [16]. Even the counter authority should not be able to have any idea about the results.
- *Uniqueness*: Only one vote for a voter should be counted [15]. It is important to notice that uniqueness does not mean unreusability, where voters should not vote more than once.
- *Uncoercibility*: Any coercer, even authorities, should not be able to extract the value of the vote [13] and should not be able to coerce a voter to cast his vote in a particular way. Voter must be able to vote freely.
- *Accuracy*: All cast votes should be counted. Any vote cannot be altered, deleted, invalidated or copied. Any attack on the votes should be detected [4]. Uniqueness should also be satisfied for accuracy.
- *Robustness*: Any number of parties or authorities cannot disrupt or influence the election and final tally [4]. To have confidence in the election results, robustness should be assured. However, there are numerous ways for corruption. For example; registration authorities may cheat by allowing ineligible voters to register; ineligible voters may register under the name of someone else; ballot boxes, ballots and vote counting machines may be compromised [1].

In order to satisfy robustness, system should be protected against any kind of active and passive attacks [13], [9]. Empty Ballot, Null Ballot, Abstaining Voter requirements should also be satisfied for robustness.

- *Efficiency*: In all phases, registration, authentication and authorization, voting and tallying, the processes should be done efficiently in a very short time. It is desired to get the results as soon as possible after the voting phase ends.
- *Abstaining Voter*: Voters may not vote for some reasons. For instance, it is allowed in Turkey not to vote, but in the past Turkey held some elections where voting was mandatory. Anyway, the system should represent abstaining voters. Abstaining voters may be recorded or not. In either case, nobody could vote instead of them.
- *Null Ballot*: The system should represent null voting, which means voter started voting process but not completed. Voters may decide not to vote at any time before casting the ballot. Null votes should also

be counted as null ballots and they cannot be filled, altered, deleted, invalidated or copied.

- *Empty Ballot*: The system should represent blank votes, which means none of the candidates is selected. Voters may change choices from 'vote' to 'blank vote' and vice-versa before casting the ballot [14]. Blank votes should also be counted as empty ballots and they cannot be filled, altered, deleted, invalidated or copied.
- *Validability*: It is the provability that the final tally is correct.
- *Universal Verifiability*: It is the provability that the election is accurate and that the published tally is correctly computed from correctly cast votes. [13]
- *Individual Verifiability*: The voter should be able to check that his encrypted vote was counted [15]. In traditional paper-based voting system in Turkey, people cannot make individual verifiability directly. But the voter casts his vote into the ballot box by himself. Since the security of the ballot box is guaranteed, individual verifiability is assured indirectly.
- *Convenience*: A convenient system allows voters to cast their votes quickly, in one session, without any extra equipment or special skills. No particular computer knowledge should be necessary to cast a vote [15]. User interfaces should be clear and easy to use. System should not involve any misunderstood or ambiguous information.
- *Equality of candidates*: The e-voting system should give equal opportunity to the candidates. [10]
- *Open Source*: All source code should be allowed to be publicly known and verified. The security and reliability of the system must not rely on secrecy of its source code which cannot be guaranteed. Only keys must be considered secret. [14]
- *Manifold of Links*: The e-voting system should be backed up and use a manifold [14] of important components against the failures and attacks.
- *Transparency*: The whole voting process must be transparent. Bulletin boards may be used to publicize the election process. The security and reliability of the system must not rely on the secrecy of the network which cannot be guaranteed.
- *Physical Recounting and Auditing*: The election data and results should be saved in both electronic and physical environments. Recounting and auditing should be able to done off-line in both electronic and physical environments after the election ends, without compromising election integrity or voter privacy. [14]
- *Technical Adequacy*: Technical infrastructure and hardware should be adequate. Cryptographic techniques should be effective not only for today but also for the future.
- *Announcement of Results*: The tally and election results and other information which may be known publicly should be announced after the election.

3.2. Additional Requirements

These requirements are not mandatory; however, they are desirable.

- *Receipt-freeness*: It is the inability to know what the vote is. Voters must neither be able to obtain nor construct a receipt which can prove the content of their vote to a third party [4] both during the election and after the election ends. This is to prevent vote buying or selling. Receipt-freeness must not depend only on communication protocol and cryptographic assumptions. It must be assured even if all ballots and decryption keys are known by collusion, attacks or faults. [14]
- *Mobility*: An e-voting system is mobile if there are no restrictions on the location from which a voter can cast a vote. [1]
- *Cheap Elections*: The cost of the e-voting should be less than the cost of the paper-based voting.
- *Flexibility*: A system is flexible if it allows a variety of ballot question formats including write-in ballots and some survey questions. [1]
- *Design Independence*: The e-voting system design should not depend on the programming language, operating system, development environment and technology.
- *Authenticated Ballot Styles*: The ballot style to be used by each voter may be authenticated or ballots may be signed to prevent invalid votes.
- *Scalability*: An e-voting system is scalable if it supports small, mid and large scale elections without any extra effort.

Some of the requirements contradict each other. For example, individual verifiability contradicts with receipt-freeness [5]. If individual verifiability is fully satisfied, achievement of receipt-freeness can fail.

4. Conclusion

In this paper, we explained fundamental parts and properties of e-elections and defined an extensive set of requirements that any e-voting system, which is planned to be used instead of paper-based voting system in the countries that have representative democracy so as in Turkey, should satisfy. Ideally, any e-voting system, which is planned to replace paper-based system, should fulfill all requirements. In fact, it should fulfill core requirements in practice.

Majority of people may accept and use e-elections since people consuming technology incredibly

nowadays. However, people may have some doubts about the privacy, security and accuracy of the e-elections. They cannot easily trust their governments, unknown individuals or commercial companies. If the e-voting systems achieve proposed requirements, then people could trust the system and use it without any hesitation. Therefore, it is not possible to accept an e-voting system for the Turkish electoral needs, without satisfying the core requirements defined in this paper.

This paper has importance since it can be base reference for new studies on e-voting. Moreover, evaluation forms can be prepared by using the defined requirements and these forms can be used in testing of already started studies.

As a future work, the applicability of proposed e-voting systems and protocols in Turkey will be evaluated against the given requirements.

5. References

[1] L. Cranor, and R. Cytron, "Sensus: A security-conscious electronic polling system for the Internet," *Proceedings of the Hawaii International Conference on System Sciences*, Wailea, Hawaii, 1997.

[2] CESG (Communications-Electronics Security Group), *e-voting security study issue 1.2*. Crown Copyright, 2002.

[3] T. M. Buchsbaum, "E-voting: lessons learnt from recent pilots," *International Conference on Electronic Voting and Electronic Democracy: Present and the Future*, Korea, 2005.

[4] J. Benaloh, and D. Tuinstra, "Receipt-free secret-ballot elections," *Proceedings of the 26th ACM Symposium on Theory of Computing*, 1994, pp. 544-553.

[5] B. Chevallier-Mames, P. A. Fouque, J. Stern, D. Pointcheval, and J. Traore, "On some incompatible properties of voting schemes," *IAVoSS Workshop On Trustworthy Elections*, Cambridge, UK, 2006.

[6] M. McGaley, and J. P. Gibson, "Electronic voting: a safety critical system," *National University of Ireland, Dept. of Computer Science*, Technical Report: NUIM-CS-TR2003-02, Ireland, 2003.

[7] G. Schryen, "Security aspects of internet voting," *Proceedings of the 37th Hawaii. International Conference on System Sciences*, Big Island, Hawaii, 2004.

[8] P. Heindl, "E-Voting in Austria legal requirements and first steps," *Workshop on Electronic Voting in Europe*, Bregenz/Austria, 2004, pp. 165-170.

[9] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, Alexandria, VA, 2005, pp. 61-70.

[10] L. Mitroud, D. Gritzalis, and S. Katsikas, "Revisiting legal and regulatory requirements for secure e-voting," *Proceedings of the 16th IFIP International Information Security Conference*, Egypt, 2002.

[11] The Grand National Assembly of Turkey, *The constitution of the Republic of Turkey: Law 298*, Ankara, Turkey, 2006.

[12] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale elections," *Advances in Cryptology - AUSCRYPT'92*, Springer, 1992.

[13] M. Burmester, andE. Magkos, "Towards secure and practical e-elections in the new era," *Information Security - Secure Electronic Voting*, Kluwer Academic Publishers, 2003, pp. 63-76.

[14] Safevote, "Voting system requirements," *The Bell Newsletter*, ISSN 1530-048X, 2001.

[15] O. Forsgren, U. Tucholke, S. Levy, and S. Brunessaux, "Report on electronic democracy projects, legal issues of ınternet voting and users (i.e. voters and authorities representatives) Requirements Analysis," *European Commission CYBERVOTE Project*, D4 Volume 3, 2001.

[16] R. Aditya, B. Lee, C. Boyd, and E. Dawson, "Implementation issues in secure e-voting schemes," *The 5th Asia-Pacific Industrial Engineering and Management Systems Conference*, Goldcoast, Australia, 2004.