Validation and Verification Issues in E-Voting

Orhan Cetinkaya[1], Deniz Cetinkaya[2]
[1]Institute of Applied Mathematics, METU, Ankara, Turkey
[2]Computer Engineering (M.Sc.), METU, Ankara, Turkey
[1]e113754@metu.edu.tr
[2]e131263@ceng.metu.edu.tr

Abstract: Electronic democracy (e-democracy) is a necessity in this era of computers and information technology. Electronic election (e-election) is one of the most important applications of e-democracy, because of the importance of the voters' privacy and the possibility of frauds. Electronic voting (e-voting) is the most significant part of e-election, which refers to the use of computers or computerised voting equipment to cast ballots in an election. 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 the political area.
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 the literature, many e-voting requirements are defined. However, the researchers started to discuss the verification in e-voting recently. Unfortunately the definitions for verifiability are inadequate and unclear; and it is categorised as individual verifiability and universal verifiability, where they are generally misused in the literature. Moreover, validation is not discussed yet.
This paper focuses on the importance of the validation and verification in e-voting, gives proper definitions for validity and verifiability in e-voting and describes their relation to accuracy and robustness of the e-voting system. This paper also states some problems to design and develop secure and verifiable e-voting systems and provides basic requirements that any e-voting system should satisfy.

Keywords: e-voting, e-voting requirements, validation, verification, verifiability.

1. Introduction

Electronic voting (e-voting) has been an applicable alternative for many non-governmental elections in the last decades. However, it is not easy to say that e-voting is likely to become viable soon for governmental elections. One of the reasons for this is the security needs of e-voting. E-voting is a security-critical application of electronic democracy (e-democracy).

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. The challenge arises primarily from the need to achieve voter anonymity, in other words to remove voter's identity from his cast ballot in order to ensure voter privacy whereas ensuring the e-voting has been done correctly without any violation and ensuring only eligible voter's votes have been counted. Therefore, e-voting has been intensively studied in the last decades.

When paper based voting is applied, voter can be easily persuaded that his vote is counted in the final tally since observers participate to the voting process which can be summarised as following: 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. 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 publicised. Voter casts his vote by himself without any influence and nobody can see voter's vote except himself. Voter cannot cast more than one vote. Vote collecting, counting and tabulating are done in front of observers publicly. 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.

When voting takes place in an electronic environment, possibility of fraud is unavoidable since ensuring the trust is not an easy task. At any step in the e-voting process, e-voting results can be manipulated if there is lack of validation and verification. The e-voting experience in Ohio in 2004 is

a well-known example which caused many discussions about vote miscount and modification where its expected candidate did not match the official winner of the election.

Majority of people may accept and use e-voting, but people have some doubts about the privacy, security and accuracy of the e-voting. They cannot easily trust the e-voting system unless validation and verification of the system is achieved. If validation and verification (V&V) processes are applied on e-voting systems, then the trust level will be increased and more voter participation can easily be achieved.

In e-voting, V&V processes should be performed to assure the security and reliability of the e-voting protocols and systems. Since an e-voting system usually depends on an e-voting protocol, the V&V of the e-voting system typically covers V&V of the e-voting system and its underlying e-voting protocol. In practice, V&V activities should occur both during, as well as at the end of the development life cycle to ensure that all requirements have been fulfilled and the system works properly. The quality of the requirements can be improved and costs and risks can be controlled by performing V&V early in the development process.

Verifiability and verification in e-voting is started to be discussed recently. Unfortunately the definitions for verifiability are inadequate and unclear. Moreover, verifiability is categorised as individual verifiability and universal verifiability, where they are generally misused in the literature.

This paper states the importance of the V&V in e-voting and gives proper definitions for validation and verification of e-voting protocols and systems. It also describes the relation between V&V and major e-voting requirements. The remainder of the paper is organised as follows. The next section provides an overview of e-voting and its requirements. Then related work is discussed. In Section 4, validation and verification in e-voting is explained. Finally, conclusions are drawn and future work is suggested.

2. Overview of e-Voting

Voting is regarded as one of the most effective methods for individuals to express their opinions on a given topic. E-voting refers to the use of computers or computerised voting equipment to cast ballots in an election. Chaum pioneered the notion of e-voting and then many protocols were proposed (Chaum 1981). The first practical e-voting protocol for large scale elections is of Fujioka *et al*. (Fujioka 1992). Verifiability was firstly introduced in this protocol however it requires more voter involvement and accuracy can be violated that the malicious authority can add votes if any voter abstains from voting in the counting stage.

The basic process of any e-election is almost standard although a wide variety of e-voting systems and protocols exist. Any e-voting system should include these actors:

- 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.

Any e-voting system should also involve these four phases:

- Registration: Voters register themselves to registration authorities and the list of eligible voters is compiled before the election day.
- Authentication and Authorisation: 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.

A general e-voting process and the actors involved can be summarised as in Figure 1 (Cetinkaya 2007), (Cranor 1997), (Fujioka 1992).

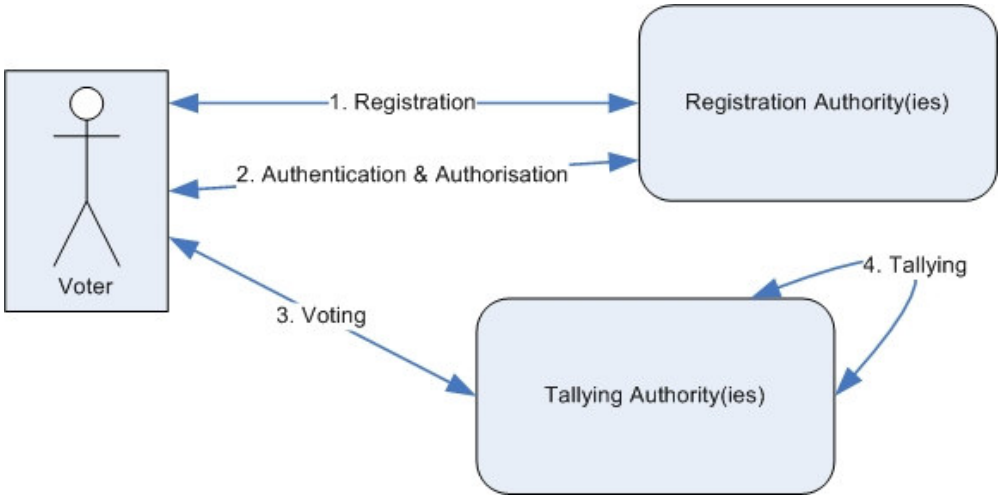

Figure 1: A general e-voting process

In literature, many e-voting protocols have been proposed. In those protocols, different requirement sets are defined, and whereas fulfilling these requirements different cryptographic tools and primitives are used. These underlying primitives are mainly blind signatures (Chaum 1982), mix-nets (Chaum 1981) and homomorphic encryption (Benaloh 1994). Before proceeding to the related work about V&V in e-voting protocols, we will briefly describe e-voting requirements.

2.1 E-Voting requirements

There are many e-voting requirements mentioned in e-voting protocols. We will briefly describe major ones (Cetinkaya 2007), (Cranor 1997), (Fujioka 1992). For further reading on e-voting requirements we refer the interested readers to the recent work of (Cetinkaya 2007). We will describe the relation between V&V and these requirements in Section 4.1.

- *Privacy*: It is the inability to link a voter to a vote. 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. They should register before the election day and only registered eligible voters can cast votes.
- *Uniqueness*: Only one vote for a voter should be counted. It is important to notice that uniqueness does not mean un-reusability, where voters should not vote more than once. Only one vote for a voter is counted.
- *Uncoercibility*: Any coercer, even authorities, should not be able to extract the value of the vote and should not be able to coerce a voter to cast his vote in a particular way. Voter must be able to vote freely.
- *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 both during the election and after the election ends. This is to prevent vote buying or selling.
- *Fairness*: No partial tally is revealed before the end of the voting period to ensure that all candidates are given a fair decision. Even the counter authority should not be able to have any idea about the results.
- *Transparency*: The whole voting process must be transparent. Bulletin boards may be used to publicise the election process. The security and reliability of the system must not rely on the secrecy of the network which cannot be guaranteed.
- *Accuracy*: All cast votes should be counted. Any vote cannot be altered, deleted, invalidated or copied. Any attack on the votes should be detected. Uniqueness should also be satisfied for accuracy.

- *Robustness*: Any number of parties or authorities cannot disrupt or influence the election and final tally. 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.

3. Related work

Fujioka *et al.* (Fujioka 1992) pioneered the verifiability in e-voting protocols by forcing voters to involve more than one round. Voter has to participate in the counting stage by checking that his vote is listed correctly in the tallying list, and then sending a part of the vote in order to complete voting. In this protocol, verifiability defined as "No one can falsify the result of the voting".

Later, Sako *et al.* (Sako 1995) introduces the concept of universal verifiability to emphasise the importance of auditing of overall election by categorising the verifiability as individual variability and universal verifiability. Further e-voting studies apply this categorisation. Sako *et al*. defined individual and universal verifiability respectively as "A sender can verify whether or not his message has reached its destination, but cannot determine if this is true for the other voters" and "In the course of the protocol the participants broadcast information that allows any voter or interested third party to at a later time verify that the election was performed properly".

Cranor *et al.* (Cranor 1997) makes the definition of universal verifiability narrow by limiting it as just counting the votes and defines verifiability as "Anyone can independently verify that all votes have been counted correctly". Most of the later studies use this definition since it is much more specific and measurable.

Karlof *et al.* (Karlof 2005) combines the verifiability definition without distinguishing universal or individual as follows: "Verifiably *cast-as-intended* means each voter should be able to verify his ballot accurately represents the vote he cast. Verifiably *counted-as-cast* means everyone should be able to verify that the final tally is an accurate count of the ballots."

It is obvious that the definitions are not unique and comprehensive. However when they are examined in detail, it is understood that they all imply the same meaning. They use verifiability in the sense of the validation of the final tally by the actors of the e-voting system, which can be the voters, authorities, passive observers or trusted third parties. Unfortunately this explanation is not adequate. "Validating the final tally", "verifying that all votes have been counted correctly", and "assuring the result of the voting" …etc can be treated as some activities of the V&V processes. So, comprehensive definitions should be stated for verifiability requirement. Moreover, validation should be taken into consideration; it should be pointed out the difference between validation and verification; and validity requirement should be introduced in e-voting.

We can summarise the individual verifiability and universal verifiability definitions used in the literature respectively as following "every voter can check if his vote has been properly counted" and "anyone can check that the calculated result is correct and election is performed correctly" (Fujioka 1992), (Sako 1995), (Cranor 1997), (Riera 1998), (He 1998), (Karlof 2005), (Chaum 2005).

Delaune *et al.* (Delaune 2006) formalises some of the e-voting requirements and then verifies whether the requirements hold on particular e-voting protocols. In particular, they use the formalism of the applied pi calculus which is a formal language similar to the pi calculus but with useful extensions for modelling cryptographic protocols and has been used to analyse a variety of security protocols in other domains. Verification of the requirements is illustrated on two cases studies and has been partially automated using the Blanchet's ProVerif tool. Delaune *et al*. brings the formal verification on some of the e-voting requirements; however, they do not mention anything about the validation issues.

The aforementioned e-voting protocols take into consideration V&V in different e-voting phases. Table 1 illustrates this relation according to the definitions of verifiability and the protocol details. The data in the table show that verification is generally handled in voting and tallying phases.

Table 1: Related work

	Registration	Authentication & Authorisation	Voting	Tallying
Fujioka *et al.*	N/A	Yes	Yes	Yes
Sako *et al.*	N/A	Yes	Yes	Yes
Cranor *et al.*	No	No	No	Yes
He *et al.*	No	No	Yes	Yes
Riera *et al.*	No	No	No	Yes
Karlof *et al.*	No	Yes	Yes	Yes

4. Validation & Verification (V&V) in E-Voting

Many e-voting protocols have been proposed from both theoretical and practical perspectives in the literature. However, to the best of our knowledge, no complete solution has been found because of the importance of security requirements in voting systems such as privacy, accuracy, fairness and robustness.

E-voting protocols have an anonymity requirement, which means the unlinkability between the voter and his cast vote. Anonymity is the primary requirement of the e-voting protocols in order to satisfy voter privacy. Fraud and system violations can be done without being detected in anonymous environments. This characteristic of e-voting forces the researchers to find a way to persuade the voter that his vote is really counted and the voting is done properly. This requirement is named as verifiability and used many years in the literature.

In software engineering, validation is the process of validating that the system satisfies the intended use and fulfils the user requirements; and verification is the process of verifying that the system complies with design specifications and formally specified properties, such as consistency and redundancy (IEEE 1996). In other words, validation is building the right system and verification is building the system right.

In an ideal world, a verified system would be naturally validated, but this is far from what is currently possible in practice. Even if it is possible to specify formally all of the user requirements, and then to verify that a system conforms to this specification, there would still be no guarantee that the requirements were correct. Verification can be viewed as a part of validation, it is unlikely that a system that is not "built right" to be the "right system". However, verification is unlikely to be the whole of validation, due to the difficulty of specifying user requirements. Therefore, it seems that validation should be more than verification.

In e-voting, *validation* is the process of validating that the e-voting system satisfies its intended use and fulfils the user requirements, such as accuracy and eligibility; and *verification* is the process of verifying that the e-voting system complies with design specifications and formally specified system requirements, such as robustness and fairness. Verification also includes the review of interim work steps and interim outputs during the e-voting process to ensure they are acceptable. Therefore, validation tries to answer the question: “Do we apply the right protocol and build the right system?” and verification tries to answer the question: “Do we apply the protocol and build the system right?”

According to these definitions we can state that individual verifiability used in the literature can be treated as a part of the validation process because voter checks whether his vote is really counted in the final tally. As well as, universal verifiability can be a part of the verification process as it is employed to check dishonest authorities and some internal processes.

While V&V are parts of the overall system development process, they are extremely important because they are the only way to produce a right system in a right manner. The V&V of e-voting protocol or e-voting system are parts of the overall design and development processes. So in ideal case V&V issues should not be handled as e-voting requirements such as verifiability or validity, since it is expected that V&V should be performed by default. However, there are many studies which use verifiability as a requirement. Thus, within the mentioned e-voting context we give the definitions of validity and verifiability in order to cover those studies. *Validity* is the ability of

performing the validation process of the e-voting protocol or the e-voting system; and v*erifiability* is the ability of performing the verification process of the e-voting protocol or the e-voting system.

Besides, in order to cover individual verifiability as an e-voting requirement we offer an alternative naming for that requirement to prevent misunderstanding: *individual vote check*. It means that the voter should be able to check that his vote is counted correctly in the final tally.

In literature, the verification is misused since it represents control or check mechanisms instead of verification process. Mostly, verifiability is used as validation and verification of any subset of the e-voting requirements especially accuracy and robustness. However, when V&V are used in an e-voting system, they should be applied to all requirements instead of a subset of requirements as the V&V processes cover all steps in an e-voting system.

V&V are interrelated and complementary processes that use each other's process results. In order to perform V&V, some activities are specified and these activities are described in system V&V plans. Validation activities are defined (for the voter, the authorities, or independent parties) for validating the e-voting protocol or the e-voting system. Verification activities are defined (for the voter, the authorities, or independent parties) for verifying the e-voting protocol or the e-voting system in varying depth depending on the system.

Validation activities may be:

- validating if the e-voting system complies with the user requirements,
- checking if the e-voting system performs functions for which it is intended
- checking if the e-voting system meets the specified goals,
- tally validation,
- ballot validation,
- authentication, …etc.

Verification activities may be:

- verifying if the e-voting system is consistent,
- checking if the e-voting system adheres to standards,
- verifying if the e-voting system uses reliable techniques and sensible practices
- verifying if the e-voting system performs the selected functions in the correct manner,
- checking the compatibility between the e-voting protocol and the e-voting system,
- verifying if the e-voting system conforms to requirements such as correctness, completeness, accuracy for all of the e-voting steps,
- ballot testing, … etc.

In order to fully satisfy validation in e-voting protocols and e-voting systems, voter should be an active participant. The reason is that nobody can know the voter's cast vote except voter himself. Thus, to validate e-voting system completely voter should involve in V&V processes during the election.

4.1 V&V and E-Voting Requirements

Verification is aimed at eliminating errors in the system, and is typically a low level task. Verification is related to robustness. Validation is more concerned with the quality of the system and is typically a high level task. Validation is related to accuracy, and the observed robustness.

Validity and verifiability is strongly related to transparency. The e-voting system should be able to allow validation and verification. However, validity and verifiability may contradict with receipt-freeness and uncoercibility requirements, since individual vote check requirement is clearly conflicting with them. Moreover, accuracy and robustness may contradict with privacy.

The relation between V&V and the e-voting requirements is shown in Table 2. The relation describes whether the requirements can be validated or verified. For example privacy can be verified by monitoring the election; however it cannot be validated without the help of voter. Besides, eligibility can be both verified and validated, since it does not require voter. In the table "conditionally" refers to the dependency to the voter and "partially" refers to the possibility of contradiction with other requirements.

Table 2: Relation between V&V and the e-voting requirements

	Validation	Verification
Privacy	Conditionally	Yes
Eligibility	Yes	Yes
Uniqueness	Yes	Yes
Uncoercibility	Partially	Yes
Receipt-freeness	Conditionally	Partially
Fairness	Yes	Yes
Transparency	Yes	Yes
Accuracy	Conditionally	Partially
Robustness	Partially	Yes
Individual vote check	Conditionally	Partially

In comparison to paper-based voting, e-voting may provide more verifiability as it uses cryptographic primitives which can be formally verified. In the context of software systems, formal verification is the act of proving or disproving the correctness of intended algorithms underlying a system with respect to a certain formal specification or property, using formal methods of mathematics. E-voting requirements may be formalised and formal verification may be performed.

5. Conclusion and Future Work

In this paper we first gave an overview of e-voting and its requirements and then explained the V&V in e-voting systems. We defined validation, verification, validity and verifiability terms in e-voting and described their relation to e-voting requirements. We also suggested an alternative naming for individual verifiability used in the literature as individual vote check.

V&V are difficult because it is hard to know how much confidence is enough. V&V is a matter of developing a level of confidence and so the level of V&V effort needed. Thus, requirements should be defined clearly and the level of confidence for each requirement should be defined well.

As a future work, a common framework for V&V processes can be established and e-voting V&V plan with all V&V activities can be defined. Moreover, V&V techniques, which can be used in e-voting V&V processes, can be explained and research on V&V tools can be done.

References

Benaloh J., Tuinstra D. (1994) "Receipt-free Secret-Ballot Elections", *Proc. of the 26th ACM Symposium on Theory of Computing*, Montreal, Canada, pp. 544-553.

Cetinkaya, O., Cetinkaya, D. (2007) "Towards Secure E-Elections in Turkey: Requirements and Principles", *Int. Workshop on Dependability and Security in e-Government*, Vienna, Austria.

Chaum D. (1981) "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM*, Vol. 24-2, pp. 84-88.

Chaum D. (1982) "Blind Signatures for Untraceable Payments", *CRYPTO '82*, pp. 199-203.

Chaum D., Ryan P. Y. A., Schneider S. (2005) "A Practical, Voter-Verifiable Election Scheme", *ESORICS'05*, Milan, Italy, pp. 118-139.

Cranor L., Cytron, R. (1997) "Sensus: A Security-Conscious Electronic Polling System for the Internet", *Proc. of the 30th Annual Hawaii Int. Conf. on System Sciences*, Wailea, Hawaii.

Delaune S., Kremer S., Ryan M. D. (2006) "Verifying Properties of Electronic Voting Protocols", *IAVoSS Workshop On Trustworthy Elections (WOTE'06)*, Cambridge, UK, pp. 45-52.

Fujioka A., Okamoto T., Ohta K. (1992) "A Practical Secret Voting Scheme for Large Scale Elections", *In Advances in Cryptology Auscrypt'92*, Gold Coast , Australia, pp. 244-251.

He Q., Su Z. (1998) “A New Practical Secure e-Voting Scheme”, *IFIP/SEC’98, Austrian Computer Society*, Austria, pp. 196-205.
IEEE/EIA (1996) “12207 Industry Implementation of International Standard ISO/IEC 12207 Standard for Information Technology - Software life cycle processes”, USA.
Karlof C., Sastry N., Wagner D. (2005) “Cryptographic Voting Protocols: A Systems Perspective”, *14th USENIX Security Symposium*, USA.
Riera A., Borrell J., Rifa J. (1998) “An Uncoercible Verifiable Electronic Voting Protocol”, *IFIP/SEC’98, Austrian Computer Society*, Austria, pp. 206-215.
Sako K., Kilian J. (1995) “Receipt-Free Mix-Type Voting Scheme: A Practical Solution to the Implementation of A Voting Booth”, *EUROCRYPT’95*, Malo, France, pp. 393-403.