Verification and Validation Issues in Electronic Voting

Orhan Cetinkaya[1], and Deniz Cetinkaya[2]
[1]Institute of Applied Mathematics, METU, Ankara, Turkey
[2]Computer Engineering, METU, Ankara, Turkey
e113754@metu.edu.tr
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 arena.

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 a correct and complete set of requirements. In this manner all e-voting studies mention e-voting requirements somewhere, and different sets of requirements are defined. Almost all researchers state verifiability as an e-voting requirement by narrowing the definition of verification. 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. Nowadays the researchers have started to discuss deeply the verification in e-voting. However there is no obvious consensus about the definitions. Moreover, validation has not been discussed properly yet.

This paper focuses on the importance of the verification and validation (V&V) in e-voting and gives proper definitions for verifiability and validity. Then it describes some V&V activities and explains the relationship between V&V and core requirements that any e-voting system should satisfy. This paper also states some problems for designing and developing secure e-voting systems.

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

1. Introduction

Electronic voting (e-voting) is a security-critical application of electronic democracy (e-democracy). E-voting has become an applicable alternative for many non-governmental elections recently. There are a number of e-voting experiments currently being employed by various countries in political area as well. However many discussions, controversies and irregularities have been raised about them (VVF 2003), (Kiayias 2007). The e-voting experience in Ohio in 2004 (Wikipedia 2007) is one of the well-known examples which caused many discussions about vote miscount and modification. Therefore, it is not easy to say that an accurate and faultless 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. 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 voters' votes have been counted. Thus, 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.

Reference this paper as:
Cetinkaya, O. and Cetinkaya, D. (2007) "Verification and Validation Issues in Electronic Voting" *The Electronic Journal of e-Government* Volume 5 Issue 2, pp 117 - 126, available online at www.ejeg.com

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 verification and validation. 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 verification and validation of the system is achieved. If verification and validation (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. Besides, validation has not been discussed properly yet and there is no obvious consensus about the definitions.

This paper states the importance of the V&V in e-voting and gives proper definitions for verification and validation 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 3. V&V in e-voting is explained in Section 4. 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 he 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. Registration authorities may be registrar, authenticator, authoriser, ballot distributor and/or key generator.
- Tallying Authority(ies): The tallying authorities collect the cast votes and tally the results of the election. Tallying authorities may be counter, collector and/or tallier.

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).

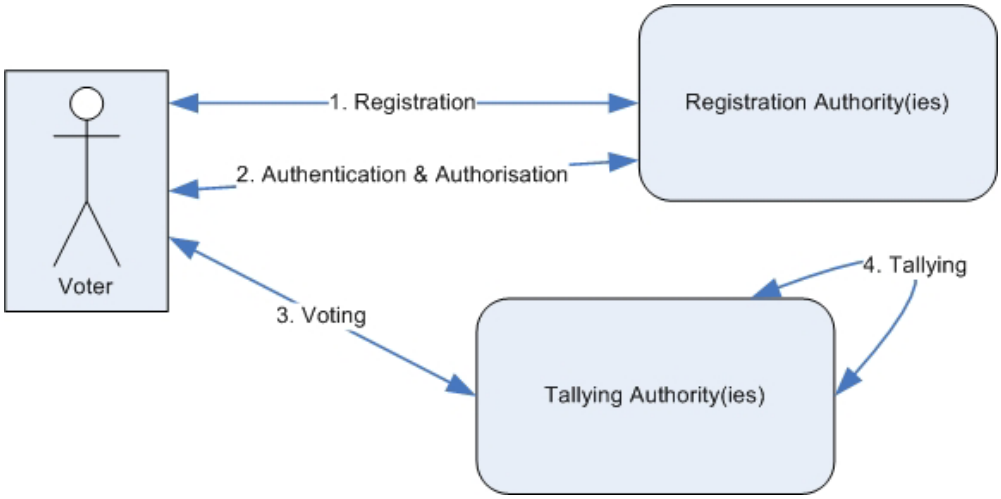

Figure 1: A general e-voting process

In the literature, numerous e-voting protocols have been proposed (Sampigethaya 2006). 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 various e-voting requirements mentioned in e-voting protocols. We will briefly describe major ones (Cetinkaya 2007), (Cranor 1997), (Fujioka 1992). We will analyse the relation between V&V and these requirements in Section 4.3.

- *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.
- *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 is 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*. defines 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.

He *et al.* (He 1998) and Riera *et al.* (Riera 1998) give a variant of the aforementioned definitions for verifiability. He *et al.* handles verifiability as "Every voter can make sure that his vote has been taken into account in the final tabulation"; and Riera *et al.* handles verifiability as "A system is verifiable if voters can independently verify that their votes have been counted correctly".

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 verification and validation; 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), (He 1998), (Riera 1998), (Karlof 2005).

The aforementioned e-voting studies take V&V into consideration partially in different e-voting phases. Table 1 illustrates how some well known e-voting protocols figure out verifiability with respect to their verifiability definitions and protocol details. The data in the table show that verification is generally handled in voting and tallying phases. Furthermore it states that the definitions in Fujioka *et al.* and Sako *et al.* are more comprehensive than the latter ones.

The table does not show that whether these protocols achieve verifiability or not in the specified phase. It only illustrates that the verifiability definition is intended for that phase and handled in some degree whereas the definition probably does not cover whole phase.

Table 1: Verifiability definitions do not cover all e-voting phases

	Registration	Authentication & Authorisation	Voting	Tallying
Fujioka *et al*. (1992)	N/A	Yes	Yes	Yes
Sako *et al.* (1995)	N/A	Yes	Yes	Yes
Cranor *et al.* (1997)	No	No	No	Yes
He *et al.* (1998)	No	No	Yes	Yes
Riera *et al.* (1998)	No	No	No	Yes
Karlof *et al.* (2005)	No	Yes	Yes	Yes

Delaune *et al.* (Delaune 2006) formalises some of the e-voting requirements and then verifies whether the requirements hold on particular e-voting protocols. Specifically 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 case studies and has been partially automated using the ProVerif tool (Blanchet 2001). Delaune *et al*. brings the formal verification on some of the e-voting requirements; however, they do not mention anything about the validation issues. 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. This research seems important for future studies since it meets formal verification with e-voting. As well as, a recent study of Cansell *et al.* (Cansell 2007) recommends application of formal methods for guaranteeing tamper evident storage of votes.

Another well known study is the concept of Voter Verified Paper Audit Trail (VVPAT), introduced by Mercuri (Mercuri 2000). VVPAT refers to a kind of "vote receipt" printed by an electronic voting machine. The VVPAT is kept by the election official, as the record of votes cast, for audit and recount purposes. Although VVPAT is commonly accepted in U.S., it can be easily seen that VVPAT does not guarantee the accuracy of the system. In other words looking at a piece of paper does not mean verification and voter does not actually verify his vote with VVPAT.

In addition to these theoretical studies, there are also a few implementations which focus on verifiability, in the context of above definitions. VoteHere VHTi (VoteHere 2007) is commercial software which is an independent verification and validation technology that works with any electronic voting system and based on Neff's cryptographic algorithm (Neff 2001). However it has some integration and usage drawbacks which make it unpractical (Sherman 2006).

Next section explains the importance of V&V in e-voting and gives proper definitions for verification, validation, verifiability, and validity. It describes some V&V activities and analyses the relationship between V&V and core e-voting requirements.

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

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.

4.1 V&V definitions in e-voting

In e-voting, *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; and *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. Verification also includes the review of interim work steps and interim

outputs during the e-voting process to ensure they are acceptable. Therefore, verification tries to answer the question: “Do we apply the protocol and build the system right?” and validation tries to answer the question: “Do we apply the right protocol and build the right system?” Verification and validation in e-voting is illustrated in Figure 2.

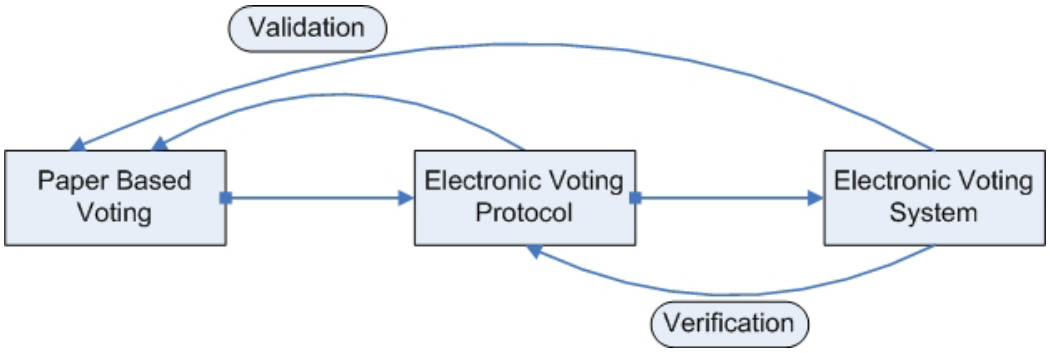

Figure 2: V&V in e-voting

According to these definitions we can state that individual verifiability used in the literature can be treated as a part of the validation process since 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 an ideal case, V&V 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, this is not currently achievable in practice and therefore there are many studies which define verifiability as a requirement. Thus, within the mentioned e-voting context we give the definitions of validity and verifiability in order to cover previous studies. *Verifiability* is the ability of performing the verification process of the e-voting protocol or the e-voting system; and *validity* is the ability of performing the validation 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. However, one should notice that people cannot make individual vote check (individual verifiability) directly even in paper based voting. Figure 3 summarises the definitions in e-voting.

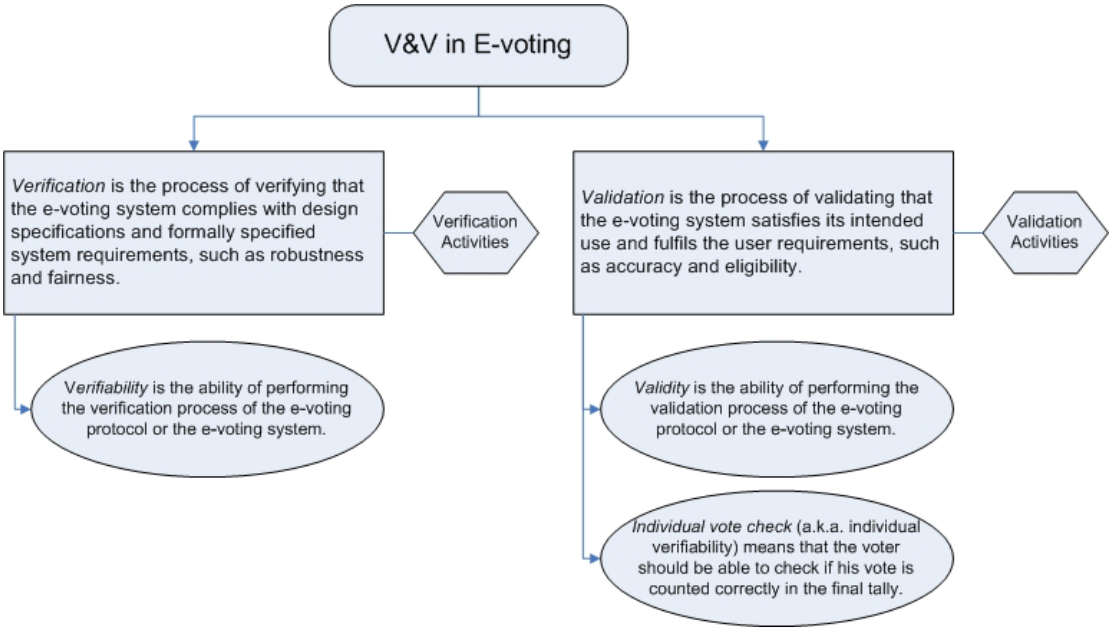

Figure 3: V&V definitions in e-voting

In literature, the verification is misused since it represents control or check mechanisms instead of verification process. Mostly, verifiability is used as verification and validation 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.

4.2 V&V activities

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. 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 are defined (for the voter, the authorities, or independent parties) for validating the e-voting protocol or the e-voting 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 and completeness for all of the e-voting steps,
- ballot testing, … etc.

In order to fully perform 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 the e-voting system completely voter should involve in V&V processes during or at the end of the election. Allowing passive observers to monitor the election can be a reasonable approach to achieve some V&V activities.

4.3 V&V and e-voting requirements

We briefly described major e-voting requirements in Section 2.1. In this section we will illustrate the relation between V&V and the e-voting requirements. Because of the characteristic of e-voting, some of the requirements may contradict each other. For example, individual vote check may contradict with receipt-freeness and uncoercibility requirements. If individual vote check is fully satisfied, achievement of receipt-freeness can fail. So, verification and validation of some requirements could be performed partially or conditionally.

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. However, accuracy and robustness may contradict with privacy.

In the context of the given definitions in Section 4.1, verifiability and validity is strongly related to transparency. The e-voting system should be able to allow verification and validation. The relation between V&V and the e-voting requirements is shown in Table 2. The relation describes whether the requirements can be verified or validated. 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: V&V can be applied on e-voting requirements in some degree

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

5. Conclusion and future work

In this paper we first gave an overview of e-voting and its requirements. Then we stated that verification and validation have not been discussed properly in e-voting by pointing out the inadequate and unclear definitions. After that, we explained V&V in e-voting systems. We defined verification, validation, verifiability and validity terms in e-voting. We also suggested an alternative naming for individual verifiability requirement, which is commonly used in the literature, as individual vote check. We also described V&V activities and made some suggestions to perform V&V in e-voting. Besides, we stated that the former definitions related to V&V can be treated as some activities of the V&V processes.

When proposing an e-voting protocol or implementing an e-voting system, it is necessary to perform the election in a secure manner. Any e-voting protocol or application may be accepted as secure and reliable if, and only if, it satisfies core e-voting requirements. Thus, we analysed the applicability of V&V on major e-voting requirements. This analysis shows that V&V could be applied partially or conditionally for some requirements. It makes V&V difficult in e-voting since it is hard to know how much confidence is enough. V&V introduces a matter of developing a level of confidence and so the level of V&V effort needed. Briefly, requirements should be defined clearly, the level of confidence for each requirement should be defined well and V&V processes should be applied on e-voting systems.

As a future work, a common framework for V&V processes will be established and e-voting V&V plan with all V&V activities will be defined. Furthermore, 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.

In comparison to paper-based voting, e-voting may provide more verifiability as it uses cryptographic primitives which can be formally verified. Thus, e-voting requirements may be formalised and formal verification may be performed in the future.

References

Benaloh, J. and Tuinstra, D. (1994) "Receipt-free Secret-Ballot Elections", *In Proceedings of the 26th ACM Symposium on Theory of Computing (STOC'94)*, Montreal, Canada, pp. 544-553.

Blanchet, B. (2001) "An Efficient Cryptographic Protocol Verifier Based on Prolog Rules", *In Proceedings of the 14th IEEE Workshop on Computer Security Foundations (CSFW)*, Canada, pp. 82-96.

Cansell, D., Gibson, J. P. and Mery, D. (2007) "Formal verification of tamper-evident storage for e-voting", *In Proceedings of the 5th IEEE International Conference on Software Engineering and Formal Methods (SEFM'07)*, London, UK, pp. 329-338.

Cetinkaya, O. and Cetinkaya, D. (2007) "Towards Secure E-Elections in Turkey: Requirements and Principles", *International Workshop on Dependability and Security in e-Government (DeSeGov'07) - In Proceedings of ARES'07*, Vienna, Austria, pp. 903-907.

Chaum, D. (1981) "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM*, Vol. 24-2, pp. 84-90.

Chaum, D. (1982) "Blind Signatures for Untraceable Payments", *In Proceedings of Advances in Cryptology CRYPTO'82*, pp. 199-203.

Cranor, L. and Cytron, R. (1997) "Sensus: A Security-Conscious Electronic Polling System for the Internet", *In Proceedings of the 30th Annual Hawaii International Conference on System Sciences*, Wailea, Hawaii.

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

Fujioka, A., Okamoto, T. and Ohta, K. (1992) "A Practical Secret Voting Scheme for Large Scale Elections", *Workshop on the Theory and Application of Cryptographic Techniques - In Proceedings of Auscrypt'92*, Gold Coast , Australia, pp. 244-251.

He, Q. and Su, Z. (1998) "A New Practical Secure e-Voting Scheme", *In Proceedings of the 14th International Information Security Conference (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", *IEEE*, USA.

Karlof, C., Sastry, N. and Wagner, D. (2005) "Cryptographic Voting Protocols: A Systems Perspective", *In Proceedings of the 14th Conference on USENIX Security Symposium*, Baltimore, MD.

Kiayias, A., Michel, L., Russell, A., Sashidar, N., See, A. and Shvartsman, A. A. (2007) "An Authentication and Ballot Layout Attack against an Optical Scan Voting Terminal", *In Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop EVT '07,* Boston, MA.

Mercuri, R. (2000) "Rebecca Mercuri's Statement on Electronic Voting", [Online], Available: http://www.notablesoftware.com/RMstatement.html [25 Oct 2007].

Neff, C. A. (2001) "A verifiable secret shuffle and its application to e-voting", *In Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS'01)*, Philadelphia, PA, pp. 116-125.

Riera, A., Borrell, J. and Rifa, J. (1998) "An Uncoercible Verifiable Electronic Voting Protocol", *In Proceedings of the 14th International Information Security Conference (IFIP/SEC'98)*, Austrian Computer Society, Austria, pp. 206-215.

Sako, K. and Kilian J. (1995) "Receipt-Free Mix-Type Voting Scheme: A Practical Solution to the Implementation of A Voting Booth", *In Proceedings of Advances in Cryptology EUROCRYPT'95*, Malo, France, pp. 393-403.

Sampigethaya, K. and Poovendran, R. (2006) "A framework and taxonomy for comparison of electronic voting schemes", *Elsevier Computers & Security*, Vol. 25-2, pp. 137-153.

Sherman, A. T., Gangopadhyay, A., Holden, S. H., Karabatis, G., Koru, A. G., Law, C. M., Norris, D. F., Pinkston, J., Sears, A. and Zhang, D. (2006) "An examination of vote verification technologies: findings and experiences from the Maryland study", *In Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop EVT '06*, Canada.

VoteHere (2007) *VoteHere VHTi technology*, [Online], Available: http://www.votehere.com/vhti.php [26 Oct 2007].

VVF (2003) *Verified Voting Foundation*, [Online], Available: http://www.verifiedvotingfoundation.org/ [21 Oct 2007].

Wikipedia (2007) "US presidential election controversy and irregularities", [Online], Available: http://en.wikipedia.org/wiki/2004_U.S._presidential_election_controversy_and_irregularities [20 Oct 2007].

