Accuracy: The Fundamental Requirement for Voting Systems

Tim Storer and Russell Lock
School of Computer Science
University of St Andrews
St Andrews, Fife Scotland.
Email: tws@cs.st-andrews.ac.uk

***Abstract*—There have been several attempts to develop a comprehensive account of the requirements for voting systems, particularly for public elections. Typically, these approaches identify a number of "high level" principals which are then refined either into more detailed statements or more formal constructs. Unfortunately, these approaches do not acknowledge the complexity and diversity of the contexts in which voting takes place.**

This paper takes a different approach by arguing that the only requirement for a voting system is that it is accurate. More detailed requirements can then be derived from this high level requirement for the particular context in which the system is implemented and deployed.

A general, formal high level model for voting systems and their context is proposed. Several related definitions of accuracy for voting systems are then developed, illustrating how the term "accuracy" is in interpreted in different contexts. Finally, a context based requirement for voting system privacy is investigated as an example of deriving a subsidiary requirement from the high level requirement for accuracy.

I. Introduction

A large number of attempts have been made to catalogue the requirements for voting systems, some by computer scientists (e.g. [1]–[4]) and some as part of legislative frameworks or standards for the deployment of voting systems in public elections (e.g. [5]–[7]). Typically, these approaches identify "top-level" requirements for voting systems (secrecy, privacy, equality, integrity, usability and so on.), and then proceed to successively refine these categories with further sub-categories and natural language statements of requirements. These approaches suffer from the usual limitations of natural language requirements documents:

- Conflation of requirements with implementations. Tjøstheim, for example, provides a model for requirements for voting systems based on a particular procedural and technological environment for the system (paper based polling station voting with some form of encrypted receipt) [8]. Similarly, Rivest has recently argued for a definition of a "software independence" requirement for voting systems, something which is only relevant to voting systems which are computer based [9]. The problem which arises in such situations is to decide which requirements are applicable to different voting systems.
- Conflicts between requirements. The Voluntary Voting System Guidelines (VVSG), for example, require voting systems to ensure voting privacy, whilst also permitting the implementation of Closed Audio Loop devices, which broadcast the results of interactions with a voting system over unencrypted radio frequencies for detection by hearing aids [6].
- Incompleteness and requirements evolution. Assessment of whether the requirements set covers all aspects of the voting context for the voting system is difficult. Even very extensive requirements approaches such as the VVSG are expected to be extended for new types of voting systems [6]. This is typically because existing requirements approaches attempt to prepare a catalogue of requirements applicable across all voting contexts, with accompanying notes of exemptions for individual cases.

Academic approaches have attempted to develop rigorous formal definitions of particular properties commonly thought to be desirable for voting systems. Such definitions are usually used to formally evaluate cryptographic voting schemes rather than full voting systems. Ryan and Peacock, for example, adopt the notion of system indistinguishability as a means of defining voting privacy [10]. Informally, this approach defines a voting system as providing privacy if an observer cannot distinguish between any two pairs of runs of the system in which two voters swap votes. This approach accepts that a voting system cannot provide privacy where all voters cast the same vote and also assumes that all voters cast the same form of vote. Alternatively, Juels and Jakobsson provide a definition of strong coercion resistance (voter anonymity), in which an observer cannot determine whether a voter even participated in an election [11].

These two definitions illustrate an important objection to existing requirements approaches: there is a substantial lack of agreement as to what is actually required. Some authors require voting privacy, others require voter anonymity. Some requirements approaches explicitly assume that the list of voters who participated in an election will be published in order to provide for verification of votes cast [12]. The plethora of voting contexts has lead to a plethora of apparently conflicting requirements documentation for voting systems. Pieters has similarly noted the simultaneous success and failure of deployments of similar voting systems in diverse cultural and legal settings [13].

It would seem that the approach adopted by many computer scientists in attempting to specify and develop a single perfect voting system, is doomed to failure, due to the diversity of requirements in different contexts. Whilst this statement may appear somewhat obvious, particularly in the context of socio-technical system research, it is not evident that such a view is accepted in the academic cryptographic or security formal methods communities. Voting systems are implemented as a result of compromises between various factors, such as the desired electoral system, the cultural practices associated with voting and the perceived threats in a particular electoral context.

This paper is a first attempt at providing a methodology for deriving context dependent voting system requirements. We begin with an abstract model for a voting system and its context at its most abstract. We use this model to define a single high-level requirement for the voting system in terms of the system's ability to accurately record and then tally the intentions of legitimate voters at an election. We argue that this requirement is *the* fundamental requirement for voting systems. Tjøstheim et al and Schneier have made similar remarks in their own approach to voting system requirements [8], [14]. We argue that all other requirements for a voting system can then be derived from this single high level requirement for a particular context. The refinements chosen are part of the specification and design process for the voting system for a particular context. For example:

- system integrity is directly related to accuracy, with the intention that a system is not violated and subsequently produce an inaccurate result;
- requirements for voter equality are intended to ensure that particular groups of voters are not disadvantaged when using a system, potentially biasing the final result produced during an election;
- requirements which specify the usability of a system are intended to prevent voters accidentally recording votes other than their true intentions;
- the common requirement for voting privacy is specified when it is desirable to prevent voters casting votes other than their true intention even if someone should attempt to coerce them.

Although requirements for voting systems will inevitably be different for different contexts (as well as changing over time), our intention is that using a uniform methodology for deriving requirements allows comparisons to be made between contexts and similarities to be discovered. We argue that this approach has the additional benefit of easing the transfer of voting systems between contexts by making explicit the change in requirements.

This paper is structured as follows. Section II gives an abstract definition of a voting system and its context. Formal definitions of both the voting context and voting system are provided using the Z specification language [15] with some syntax from the CADiZ extended toolkit [16]. We have chosen to formalise the definition of electoral context and voting system model in this way in order to provide a precise definition of the concepts discussed. In addition, we believe the work described in this paper is a useful example of research spanning the fields of formal methods and socio-technical systems. Section III presents some alternative specifications of accuracy for a voting system. Section IV extends the context model by adding the possibility of voter coercion, and thus the means of defining what a system must achieve to thwart this attack. The purpose here is to demonstrate that a requirement for privacy specified in some voting context is in fact derived from the need for a voting system to be accurate with respect to voters' intentions. Section V summarises the work and identifies some future extensions.

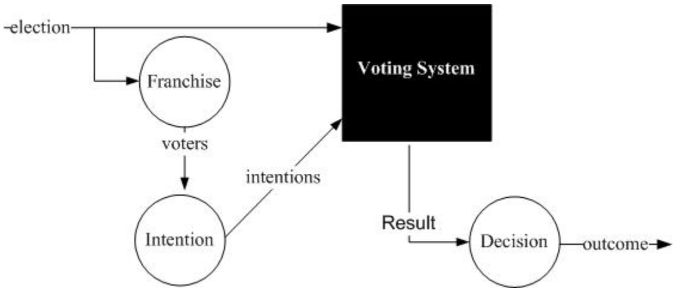

Fig. 1. Model of voting system and context.

II. Voting System Model

First, we need to give a definition of the context in which a voting system operates. In doing so, we limit the scope of our concern to the operation of the voting system, rather than wider aspects of election regulation:

> An *election* is a device by which a number of autonomous parties (*voters*) make a collective decision based on individual preferences (*votes*), according to a set of rules for aggregating preferences (*electoral system*). The set of voters eligible to participate in an election is termed the *electorate*. Membership of the electorate for an election is defined by a set of rules describing eligibility criteria called the *franchise*. The translation between votes cast and the aggregated *result* is computed in accordance with an implementation of the electoral system. The purpose of a voting system is to accurately collect and aggregate the *legitimate intended vote*s of some *voters* for a number of *elections*. The result produced by a voting system is used to decide the *outcome* for an election, i.e. the consequences of the result.

Figure 1 gives a visual presentation of this definition as an information flow diagram. The voting system is a 'black box' process which maps voting intentions for a single election to a result. The result is then used as input to a decision process which determines an outcome. The definition of intention here is limited to what is considered a legitimate construction of a vote in a given context. A legitimate intention may include a voter's decision to abstain or cast a non-vote, depending on the context. At this stage, we are concerned with providing a model for a voting system's context and operation, rather than specifying requirements on it. Thus, the model will not incorporate explicit requirements concerning the accuracy of the voting system.

To begin the Z specification, we introduce the basic types for the entities in the schema, drawn from the definition given above:

$$[VOTER, ELECTION, VOTE, RESULT, OUTCOME]$$

The definition of an electoral context can now be formalised as a schema:

$$\begin{array}{|l}
\textit{ElectoralContext} \\
\hline
franchise : ELECTION \rightarrow \mathbb{P}\, VOTER \\
intention : VOTER \times ELECTION \rightarrow VOTE \\
electoralSystem : \mathrm{bag}\, VOTE \rightarrow RESULT \\
decision : RESULT \rightarrow OUTCOME \\
\hline
\forall\, voter : VOTER;\ election : ELECTION \bullet \\
\quad (voter, election) \in \mathrm{dom}\, intention \\
\qquad \Leftrightarrow voter \in franchise(election) \\
\hline
\end{array}$$

The franchise for the voting context (line 1) is a function giving the set of voters eligible to participate in an election. The franchise will vary for each election as some voters become eligible, and others are disqualified. A voter's intention (line 2) is a function which maps from a voter and an election to a vote. The electoral system (line 3) is a function which translate a collection of votes (a bag in Z) into a result. A result for an election will translate into an outcome (line 4). The expression (line 5,6,7) sets the domain of the intention function to be all pairings of elections and their corresponding electorates. That is, voters only express legitimate intentions for elections in which they are eligible to participate.

The definition of electoral context given above includes an implicit definition of a voting system. To restate: the purpose of a voting system is to collect and aggregate the legitimate intended votes of a set of voters for an election into a result. Typically, a voting system can be considered as two separate concerns (Figure 2): the recording of voters' intended votes (vote collection); and the translation of recorded votes into a result (tallying). The figure illustrates that vote collection sub-process takes the current election and voting intentions as input. The votes collection process produces a collection of votes which are derived from the voter's intentions (possibly inaccurately). The Z schema for the collection of votes is given below:

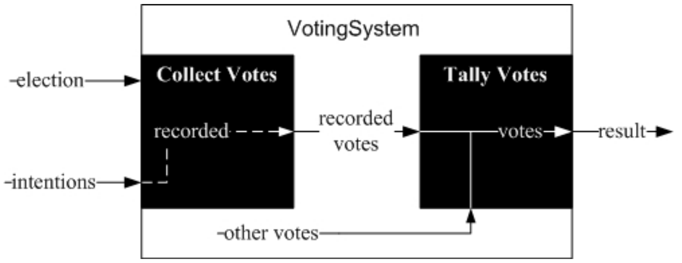

Fig. 2. Model of voting system refined into collecting and tallying operations.

$$\begin{array}{|l}
\textit{CollectVotes} \\
\hline
ElectoralContext \\
election? : ELECTION \\
intentions? : \mathbb{P}(VOTER \times ELECTION \times VOTE) \\
recorded : \mathbb{P}(VOTER \times ELECTION \times VOTE) \\
\hline
\forall\, voter : VOTER;\ election : ELECTION; \\
\quad vote : VOTE \bullet \\
\qquad (voter, election, vote) \in intentions? \Leftrightarrow \\
\qquad\quad election = election? \wedge \\
\qquad\quad intention(voter, election) = vote \\
\hline
\end{array}$$

The schema includes the previous definition of electoral context given above (line 1). The schema defines an election and a set of voting intentions for the election as inputs to the voting system (lines 2,3). The expression (lines 5-9) restricts the set *intentions?* which are input to the voting system to those of voters for the current election. An additional internal variable *recorded* is introduced (line 4) which refers to the voting intentions as recorded by the voting system.

Figure 2 also illustrates the process of translating votes held by the voting system into a result. This process of tallying votes takes votes from (a) the votes recorded as voting intentions from voters and (b) other votes potentially introduced into the voting system, for example through some nefarious activity. The Z schema for tallying of votes is:

$$\begin{array}{|l}
\textit{TallyVotes} \\
\hline
CollectVotes \\
result! : RESULT \\
recorded\_votes : \mathrm{bag}\, VOTE \\
other\_votes : \mathrm{bag}\, VOTE \\
votes : \mathrm{bag}\, VOTE \\
\hline
recorded\_votes = \{ \\
voter : VOTER;\ election : ELECTION; \\
vote : VOTE;\ n : \mathbb{N} \mid \\
(voter, election, vote) \in recorded \wedge \\
n = \#\{voter2 : VOTER; \\
\quad election2 : ELECTION; \\
\quad vote2 : VOTE \mid \\
\quad (voter2, election2, vote2) \in \\
\qquad recorded \wedge vote2 = vote\} \bullet vote \mapsto n\} \\
votes = recorded\_votes \uplus other\_votes \\
\hline
\end{array}$$

The schema defines an output *result!* (line 2). The *recorded_votes* variable (line 3,6-14) denotes the collection of votes derived from recorded voting intentions (*recorded*). The votes used by a voting machine for tallying are those votes which were recorded as the intentions of voters, as well as possibly other extra errant votes that were introduced prior to tallying (lines 4,5,15).

So we can now define a voting system:

$$\mathit{VotingSystem} == \mathit{CollectVotes} \land \mathit{TallyVotes}$$

At this stage of refinement, no attempt has been made to specify the relationship between the intended votes and the recorded intentions, nor between the votes collected and the aggregated result.

III. Voting System Accuracy

The previous section provided a basic model for a voting system and context (VotingSystem). In this section, several interpretations of an accuracy requirement are proposed. In an ideal world, it might be nice to require a perfectly accurate voting system to be implemented:

$$\begin{array}{|l}
\mathit{PerfectVotingSystem} \\
\mathit{VotingSystem} \\
\hline
\mathit{recorded} = \mathit{intentions}? \\
\mathit{other\_votes} = \varnothing \\
\mathit{electoralSystem}(\mathit{votes}) = \mathit{result}!
\end{array}$$

That is, the voting system exactly records the intentions of all the voters (line 2), no extra votes are introduced (line 3), and the result produced at the end is correct with respect to the relevant electoral system (line 4). However, practical voting systems are not generally implemented to provide perfect accuracy, but accuracy that is "good enough". One possible interpretation of "good enough" for a voting system, is that the difference between the correct result and the result provided by the voting system does not alter the outcome of an election:

$$\begin{array}{|l}
\mathit{OutcomeAccurateVotingSystem} \\
\mathit{VotingSystem} \\
\mathit{intended\_votes} : \mathrm{bag}\ \mathit{VOTE} \\
\hline
\mathit{intended\_votes} = \{ \\
\mathit{voter} : \mathit{VOTER};\ \mathit{election} : \mathit{ELECTION}; \\
\mathit{vote} : \mathit{VOTE};\ n : \mathbb{N} \mid \\
(\mathit{voter}, \mathit{election}, \mathit{vote}) \in \mathit{intentions}? \land \\
n = \#\{\mathit{voter}2 : \mathit{VOTER};\ \mathit{election}2 : \mathit{ELECTION}; \\
\quad \mathit{vote}2 : \mathit{VOTE} \mid \\
\qquad (\mathit{voter}2, \mathit{election}2, \mathit{vote}2) \in \mathit{intentions}? \\
\qquad\quad \land\ \mathit{vote}2 = \mathit{vote}\} \bullet \mathit{vote} \mapsto n\} \\
\mathit{decision}(\mathit{result}!) = \\
\quad \mathit{decision}(\mathit{electoralSystem}(\mathit{intended\_votes}))
\end{array}$$

The schema introduces a new collection of votes which are intended to be cast by eligible voters in the election (line 2). The expression in lines 11-12 requires that the result (*result!*) produced by the voting system (however it is obtained) gives the same outcome as the application of the electoral system specification to the collection of votes intended by the voters in the election. A voting system which implements the simple plurality electoral system, for example, would be satisfactory if it always accurately identified the candidate with the most number of votes.

However, such a definition is often politically unacceptable if, for example, the distribution of funding at subsequent elections is dependent on a candidates share of votes. The schema below gives a measured definition of accuracy:

$$\begin{array}{|l}
\mathit{MeasuredVotingSystem} \\
\mathit{VotingSystem} \\
\mathit{collAcy} : \mathbb{R} \\
\mathit{resultOrder} : \mathit{order}\ \mathit{RESULT} \\
\mathit{devianceInterval} : \mathbb{P}\,\mathit{RESULT} \\
\mathit{talAcy} : \mathbb{R} \\
\hline
\mathit{collAcy} = \\
\quad \#(\mathit{recorded} \cap \mathit{intentions}?)\ \mathrm{div}\ \mathit{bagsize}\ \mathit{votes} \\
\mathit{devianceInterval} = \{r : \mathit{RESULT} \mid \\
\quad ((\mathit{result}!, r) \in \mathit{resultOrder} \land \\
\qquad (r, \mathit{electoralSystem}(\mathit{intended\_votes})) \in \\
\qquad\quad \mathit{resultOrder}) \lor \\
\quad ((r, \mathit{result}!) \in \mathit{resultOrder} \land \\
\qquad (\mathit{electoralSystem}(\mathit{intended\_votes}), r) \in \\
\qquad\quad \mathit{resultOrder})\} \\
\mathit{talAcy} = 1 - \#\mathit{devianceInterval}\ \mathrm{div}\ \#\mathit{RESULT}
\end{array}$$

Lines 2,6 and 7 define collection accuracy to be the normalised (number of intended votes and additional votes) difference between the set of recorded votes and the set of intended votes. One consequence of this definition means that the swapping of the intentions of two voters reduces the accuracy of the voting system.

The accuracy of the tally is measured by assuming a partial ordering on the set of possible results (line 4). Line 5 and 8-14 define the interval between the result computed by the voting system and the true result as computed by the electoral system on the set of intended votes within the set of all possible results. The tally accuracy (lines 5 and 15) is then the normalised size of the interval between the actual result produced by the voting system and the ideal result that would be produced by a perfect implementation of the electoral system on the set of actual votes.

IV. Defining Voting Privacy in Terms of Accuracy

Given the definitions above, we can now investigate a definition of voting privacy requirements in order to support our argument that accuracy is the primary requirement of voting systems. The initial step is to define a voting system in the context of an attacker who wishes to coerce voters into changing their votes (a coercer). A coercer will seek to induce voters to record votes which are different from their true intentions in order to achieve a particular outcome for the election. The coercer may also wish to observe recorded intentions to satisfy themselves that their objective has been achieved. The Z schema for the coercible context is given below:

$$\begin{array}{|l}
\textit{CoercionContextVS} \\
\hline
\textit{VotingSystem} \\
\textit{desired}? : \mathbb{P}(\textit{ELECTION} \times \textit{VOTER} \times \textit{VOTE}) \\
\textit{coerced} : \mathbb{P}(\textit{ELECTION} \times \textit{VOTER} \times \textit{VOTE}) \\
\textit{observedC}! : \mathbb{P}(\textit{ELECTION} \times \textit{VOTER} \times \textit{VOTE}) \\
\textit{observedU}! : \mathbb{P}(\textit{ELECTION} \times \textit{VOTER} \times \textit{VOTE}) \\
\hline
\textit{desired}? \cap \textit{intentions}? = \varnothing \\
\textit{coerced} = \textit{recorded\_votes} \cap \textit{desired}? \\
\textit{observedC}! \subset \textit{coerced} \\
\textit{observedU}! \subset \textit{desired}? \setminus \textit{coerced} \\
\hline
\end{array}$$

The extension to the model specifies the voting intentions which a coercer wishes to change as an input to the schema (line 2). The coercer may not be able to successfully coerce all the votes they desire, so the set of coerced votes represents the occurrence of desired coerced intentions in the recorded set of votes (lines 3, 7). For simplicity, the definition excludes from consideration any of the coercer's desired voting intentions which are the same as the voter's true intention (line 6). This is acceptable because such intentions are not violated by an attacker's attempted coercion and so do not have an influence on the accuracy of the election. The definition also excludes any voters who willingly collude with the coercer, for tactical voting purposes, for example. The outputs from the schema define the two subsets of recorded votes observed by the coercer (lines 4,5,8,9). The attacker may be able to observe some of the successfully coerced votes as well as some of the recorded votes which do not match their desired intentions.

Typically, the various definitions of coercion resistance in the cryptographic voting scheme literature (e.g. [11], [17]), seek to limit the recorded intentions of voters which are observable by a coercer. In such circumstances, it is argued, a coercer cannot effectively induce voters to change their votes, because they cannot be sure that the voter followed their instructions:

$$\begin{array}{|l}
\textit{CryptoCoercionResistantVotingSystem} \\
\hline
\textit{CoercionContextVS} \\
\hline
\textit{observedC}! = \varnothing \land \textit{observedU}! = \varnothing \\
\hline
\end{array}$$

It may be noted that ensuring that no recorded intentions are observable by the coercer does not limit the size of the set of coerced votes. The model reflects this by separating votes that are coerced from those that are observable as such by a coercer. The coercer may instead attempt to convince a voter that their recorded intention is observable by them, whether this is true or not. One study which investigated the prospects of introducing computer based voting systems to UK elections found that some voters believed that their votes were observable by candidates [18] - because the successful candidate had thanked them for their support after the election!

A voting system vulnerable to this form of coercion may be modelled as one in which, for some voters, the true set of recorded votes observable by the coercer is indistinguishable from the set of observable votes claimed by the coercer. When presented with a set of claimed observations of voters for an election, the voter will believe that some voters' interactions with the voting system will be observable. In such circumstances, the voter may be coerced into changing their recorded vote from their true intention if they believe that their own interaction with the voting system will be observable by an coercer. This can be described as follows:

$$\begin{array}{|l}
\textit{CoercionContextVS}2 \\
\hline
\textit{CoercionContextVS} \\
\textit{claimedObs}? : \textit{ELECTION} \times \textit{VOTER} \\
\textit{voterBel} : \textit{VOTER} \times \mathbb{P}(\textit{ELECTION} \times \textit{VOTER}) \rightarrow \\
\qquad \mathbb{P}(\textit{ELECTION} \times \textit{VOTER}) \\
\textit{convincedCoerced} : \\
\qquad \mathbb{P}(\textit{ELECTION} \times \textit{VOTER} \times \textit{VOTE}) \\
\hline
\textit{claimedObs}? \subseteq \operatorname{dom} \textit{intention}? \\
\textit{convincedCoerced} = \{ \\
\forall\, \textit{election} : \textit{ELECTION}, \textit{voter} : \textit{VOTER}, \\
\textit{vote} : \textit{VOTE} \mid (\textit{election}, \textit{voter}, \textit{vote}) \in \textit{coerced} \land \\
\qquad\qquad (\textit{election}, \textit{voter}) \in \\
\qquad\qquad\qquad \textit{voterBel}(\textit{voter}, \textit{claimedObs}?)\} \\
\hline
\end{array}$$

The schema defines a subset of voter's intentions that the coercer claims to be able to observe (lines 2, 7). In addition the schema defines for each voter in the election, those claims regarding observations made by the coercer they will believe (line 3). The subset of coerced intentions resulting from the attack (lines 5,8-12) will be the intersection between the claims made by the attacker and the set of observations that the voter believes are observable by the attacker.

The possibility is a particular problem for both cryptographic and non-cryptographic voter-verifiable schemes alike, (e.g. [19]–[22]). Several studies have indicated that voters in public elections are disinclined to utilise verification mechanisms, or struggle to comprehend them [23], [24]. Storer and Little's study suggested that people eligible to participate in UK public elections had limited confidence in explanations of why their vote would be kept secret by a relatively simple internet based voting system [25].

There are several alternative approaches that may be specified for countering the threat of coercion of this form, for example, it may be desirable to require that a voting system is *understandable*, i.e. that is each voter understands why their vote is not observable by a coercer. For the definition given above, this would mean that a voter does not believe the coercer can observe any voter's interactions with the voting system. Alternatively, require that the coercer is restricted in the claims regarding observability of the voting system they can make to voters. This requirement might be satisfied by legislation which threatens severe penalties for claiming the ability to observe voting intentions with the intent to coerce voters, for example. In either case, the requirement can be directly associated to the accuracy of the voting system.

V. Conclusions

This paper has presented an abstract model of voting systems as the basis for developing requirements in different voting contexts in a consistent manner. The paper proposed a single high level requirement for voting systems (accuracy) from which all other requirements are derived, contingent on the system's context. Several related interpretations of voting system accuracy are also discussed, highlighting in particular the distinction between the result of an election and the outcome. To illustrate the approach to voting system requirements, the commonly cited requirement for voting privacy was investigated in terms of its relationship to accuracy. It was argued that the requirement for voting privacy (in contexts where it is specified) is based on the desire to prevent voters from being inappropriately influenced into recording a vote which is different from their true intention and thus reducing the accuracy of system.

Several extensions to the work described are possible. In particular, the development of requirements for particular contexts would provide a more comprehensive evaluation of the proposed framework. A more severe limitation of the work presented here is that it does not incorporate a requirement for the timely production of an election result. The elections in Scotland in 2007, for example, caused consternation because of the extended delay in extracting records of votes from the counting system [26]. We could therefore extend our definition of voting context and system to require a result to be produced within some specified time period. Although we leave further investigation of this limitation to future work.

The approach described in this paper was predicated on the need to avoid producing "yet another" list of desiderata proposed as being generally applicable as the requirements for voting systems. Rather, the paper presents a framework for developing requirements in different contexts. Requirements for voting systems are not universal; they are based on social, historical and cultural factors, as well as the perceived threat environment.

References

[1] R. Anane, R. Freeland, and G. Theodoropoulos, "e-voting requirements and implementation," in *9th IEEE International Conference on E-Commerce Technology and (CEC 2007) / 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (EEE 2007)*. Tokyo, Japan: IEEE Computer Society, July 2007, pp. 382–392.

[2] E. Gerck, "Voting system requirements," *The Bell(Safevote Newsletter)*, vol. 1, no. 7, pp. 3–16, 11 2000. [Online]. Available: http://www.thebell.net/papers/vote-req.pdf

[3] L. M. D. Gritzalis and S. Katsikas, "Revisiting legal and regulatory requirements for secure e-voting," in *Security in the Information Society: Visions and Perspectives, IFIP TC11 17th International Conference on Information Security (SEC2002)*, ser. IFIP Conference Proceedings, A. Ghonaimy, M. T. El-Hadidi, and H. K. Aslan, Eds., vol. 214, IFIP. Cairo,Egypt: Kluwer, May 2002, pp. 469–480.

[4] R. Mercuri, "Electronic vote tabulation: Checks and balances," Ph.D. dissertation, University of Pennsylvannia, 2001.

[5] "e-voting security study," Communications and Electronic Security Group (CESG), July 2002. [Online]. Available: http://www.edemocracy.gov.uk/library/papers/study.pdf

[6] *Voluntary Voting System Guidelines*, Draft ed., Election Assistance Commission, 1225 New York Ave., NW, Suite 1100, Washington, D.C. 20005, July 2005.

[7] *Voting Systems Standards*, Federal Election Commission, 999 E Street, NW, Washington, DC 20463, January 1990.

[8] T. Tjøstheim, T. Peacock, and P. Y. Ryan, "A model for systematic analysis of voting systems," School of Computing Science, University of Newcastle, Claremont Tower, Claremont Road, Newcastle upon Tyne, NE1 7RU, Tech. Rep. 1001, January 2007.

[9] R. L. Rivest and J. P. Wack, "On the notion of "software independence" in voting systems," NIST, Draft White Paper proposals for VVSG 2007, July 2006.

[10] T. Peacock and P. Y. Ryan, "Coercion-resistance as opacity in voting systems," School of Computing Science, University of Newcastle, Claremont Tower, Claremont Road, Newcastle upon Tyne, NE1 7RU, Tech. Rep. CS-TR-959, April 2006.

[11] A. Juels and M. Jakobsson, "Coercion resistant electronic elections," 2002, eprint.iacr.org/2002/165.pdf. [Online]. Available: eprint.iacr.org/2002/165.pdf

[12] "Representation of the People Act," 1983, ch. 2.

[13] W. Pieters, "La volonté machinale - understanding the electronic voting controversy," Ph.D. dissertation, Raboud University Nijmegen, 2008.

[14] B. Schneier, "Voting security and technology," *IEEE Security and Privacy*, vol. 2, no. 1, p. 84, January 2004.

[15] J. Spivey, *The Z Notation: A Reference Manual*, 2nd ed., Programming Research Group, University of Oxford, Oriel College, Oxford, OX1 4EW, England, 1998, http://spivey.oriel.ox.ac.uk/mike/zrm/index.html.

[16] I. Toyn and J. A. McDermid, "CADiZ: An architecture for Z tools and its implementation," *Software Practice and Experience*, vol. 25, no. 3, pp. 305–330, March 1995.

[17] M. R. Clarkson and A. C. Myers, "Coercion-resistant remote voting using decryption mixes," in *Frontiers in Electronic Elections (FEE 2005)*, Milan, Italy, September 2005.

[18] "e-democracy report of research findings," COI Communications/Office of the e-Envoy, December 2002. [Online]. Available: http://www.edemocracy.gov.uk/downloads/Full_Report.pdf

[19] D. Chaum, P. Y. Ryan, and S. Schneider, "A practical, voter-verifiable election scheme," in *Computer Security - ESORICS 2005, 10th European Symposium on Research in Computer Security*, ser. Lecture Notes in Computer Science, S. D. C. di Vimercati, P. F. Syverson, and D. Gollmann, Eds., vol. 3679. Milan, Italy: Springer Verlag, September 2005, pp. 118–139.

[20] P. Y. Ryan, "Prêt à voter with a human-readable, paper audit trail," in *Frontiers of Electronic Voting*, Schloss Dagstuhl, Germany, July 2007.

[21] R. L. Rivest and W. D. Smith, "Three voting protocols: ThreeBallot, VAV, and Twin," in *EVT'07 Electronic Voting Technology Workshop*. Boston, MA: USENIX/ACCURATE, August 2007.

[22] T. W. Storer, "Practical pollsterless remote electronic voting," Ph.D. dissertation, University of St Andrews, St Andrews, Fife, Scotland., June 2007.

[23] A.-M. Oostveen and P. van den Besselaar, "Ask no questions and be told no lies security of computer based voting systems; user's trust and perceptions," in *EICAR 2004 Annual Conference CD-ROM*, U. E. Gattiker, Ed. Grand-Duché de Luxembourg: European Institute for Computer Anti-Virus Research, May 2004.

[24] T. Selker and J. Goler, "Security vulnerabilities and problems with VVPT," Caltech/MIT Voting Technology Project, Pasadena, California 91125/ Cambridge, Massachusetts 02139, VTP Working Paper 13, April 2004.

[25] T. Storer, L. Little, and I. Duncan, "An exploratory study of voter attitudes towards a pollsterless remote voting system," in *IaVoSS Workshop on Trustworthy Elections (WOTE 06) Pre-Proceedings*, D. Chaum, R. Rivest, and P. Ryan, Eds., Robinson College, University of Cambridge, England, June 2006, pp. 77–86. [Online]. Available: research/papers/storer06exploratory.pdf

[26] R. Gould, "Independent review of the Scottish Parliamentary and local government elections 3 may 2007," The Electoral Commission, Trevelyan House, Great Peter Street, London, SW1P, October 2007.