Electronic Voting Systems: Security Implications of the Administrative Workflow*

Costas LAMBRINOUDAKIS[1], Spyros KOKOLAKIS[1], Maria KARYDA[2], Vasilis TSOUMAS[2], Dimitris GRITZALIS[2], Sokratis KATSIKAS[1]

[1] *Dept. of Information and Communication Systems Engineering*
University of the Aegean, Samos GR-83200, Greece
e-mail: {clam,sak}@aegean.gr

[2] *Dept. of Informatics, Athens University of Economics and Business*
76 Patission St., Athens GR-10434, Greece
e-mail: {mka,bts,dgrit}@aueb.gr

Abstract

With the rapid growth of the Internet, online voting appears to be a reasonable alternative to conventional elections and other opinion expressing processes. Current research focuses on designing and building "voting protocols" that can support the voting process, while implementing the security mechanisms required for preventing fraud and protecting voter's privacy. However, not much attention has been paid to the administrative part of an electronic voting system that supports the actors of the system. Possible "security gaps" in the administrative workflow may result in deteriorating the overall security level of the system, even if the voting protocol implemented by the system succeeds to fully comply with the security requirements set for voting. To this direction, this paper describes the responsibilities and privileges of the actors involved in the electronic voting process. The description of the role of each actor, together with the clear indication of what each actor is expected - and thus allowed - to do with the system, formulate an operational framework that complements the technological security features of the system and allows us to talk about "secure electronic voting systems".

1. Introduction

The main contribution of electronic voting and more specifically of internet-based voting systems is the support they offer for "voter mobility", allowing them to participate in an election from any location that provides Internet access.

It has been demonstrated [6] that the design of a voting protocol that protects the integrity, generality, equality, freedom, secrecy and fairness of the election process is feasible, facilitating the development of an electronic voting system that complies with the requirements of transparency and verifiability. However, the security features implemented in the voting protocol do not "*cover*" the tasks for organising the voting process. This is known as the administrative part of the election system, through which authorised actors can set-up the election characteristics, the list of eligible voters, the list of parties and candidates, the available ballots and several other parameters that must be specified before instructing the system to conduct the voting process.

This known inefficiency may become even more dangerous in systems that are highly customised, in terms of alterations in the administrative workflow and modifications in the level of the security mechanisms implemented, to support different types of voting processes like general elections, polls, referendums etc; each one exhibiting slight differentiations in terms of the functional and security requirements that must be supported.

To this direction, this paper describes the responsibilities and privileges of the actors identified to have a need to interact with an electronic voting system, namely: the Election Organisers, the Election Personnel, the Party Representatives, the Judicial Officers and the Trusted Third Parties. The description of the *role* of each actor, together with the clear indication of what each actor is expected - and thus allowed - to do with the system, for-

* This work has been supported in part by the European Commission, IST Programme, Project e-vote (An Internet-based electronic voting system; IST-2000-29518)

mulate an operational framework that complements the technological security features of the system and allows us to talk about "secure electronic voting systems".

Section 2 provides an overview of the electronic voting systems objectives together with a brief descryption of the functional, security and legal/constitutional requirements that must be fulfilled. Furthermore, section 2 describes the system actors (*roles*), as far as their involvement in the operation of the system and their privileges is concerned, and also the sequence of use cases for organizing and conducting the voting process. Section 3 proposes an extension to the traditional authentication/authorization scheme, introducing the *Validate Action* function. It demonstrates the necessity for validating administrative operations, in an e-vote environment, and shows how it should be integrated in the administrative workflow of the system. Finally, in Section 4 we summarize the work presented in the paper stressing out some of the conclusions.

2. Electronic voting systems

An *electronic voting (e-voting) system* is a voting system in which the election data is recorded, stored and processed primarily as digital information [9]. More specifically, the most common objectives of an e-voting system are to:

- Provide the entire set of required services for organizing and conducting a voting process.
- Support, in accordance to a well-defined operational framework, all 'actors' that have a need to interact with the system.
- Support different 'types' of voting processes like polls, plebiscites, inter-organizational elections, general elections etc.
- Be customisable in respect to the geographical coverage of the voting process, the number of voting precincts, the number of voters, and other specific characteristics of the process like starting date and time, number of candidates etc.
- Ensure that [5]:
  - Only eligible persons can vote.
  - No person can vote more than once.
  - The vote is secret.
  - Each vote is counted in the final tally.
  - The voters trust that their vote is counted.

2.1. Functional and security requirements

Electronic voting systems should fulfil a rather long list of legal, societal and technological requirements. The majority of these requirements, apart from the functionality that the system should exhibit in order to support the voting process, have been also influenced from a) the set of guidelines that must be adopted in order to ensure conformance to the legislation (the *election organizer's point of view*), and b) the problems associated with the provision of the adequate level of security; like anonymity, authentication, tractability etc (the *engineer's point of view*).

The outcome was a "User Requirements Specification Document" that describes a *Generic Voting Model*, which consolidates the European Union Legislation, the organizational details of a conventional election process and the issues raised by the opportunities offered and the constraints imposed by state-of-the-art technologies. Therefore, such a specification document can assist developers to set the Design Criteria by equally considering the set of functional, security (non-functional) and constitutional/legal requirements for an e-voting system. A detailed description of them can be found in [4], [6] and [7], [9] respectively and will therefore not be repeated in this paper. However, in order to facilitate the discussion about the administrative part of the system as well as about the *role* of each actor who interacts with the system, the use-case model [3] of an electronic voting system is presented through a brief description of the identified system use-cases.

Table 1. System use cases for an e-voting system

System Use Case	***Description***
Provide Authentication Means	Create and distribute authentication means to all actors
Authenticate Actor	Provide access to the system functions in accordance with the authorization level (privileges) of the actor
Validate Action (refer to Section 3)	Ensure that an action that affects the integrity of the system will not be committed unless validated by a predetermined group of actors.
Manage System Users	Add, modify, delete and view the e-vote System Users (i.e. election organizers, election personnel, judicial officers, party representatives, independent third parties).
Modify System State	Perform the system transition from one operational state to a new one. The states of the system are "Election set-up", "Election in progress" and "Election concluded".
Manage Election Districts	Create, view and modify different sets of election districts for one or more election processes.
Manage Voters	Import, insert, view, modify and export voters for an election process.
Manage Candidates	Insert, modify or delete the candidates of a party for a specific election district.
Provide Election System Parameters	Set-up the election system parameters required for organizing and conducting a specific election process.
Preview Ballots	Examine the content and format of the ballots that will be used during the election process

Cast Vote	Facilitate electronic voting
Tally Votes	Calculate the voting result
Verify Result Integrity	Verify that system use cases have performed the required actions as expected and in a timely manner

2.2. System actors and administrative workflow

The different *roles* that have been identified by examining the various categories of system actors participating in the system use cases are listed next, together with a brief description of their participation characteristics and privileges.

- ***Election Organisers*** are the people responsible for organising the election process as well as for ensuring that it is properly conducted. For the General Elections case, they are normally people appointed by the state. In most use cases their role is to validate the work performed by the E*lection Personnel*, in order for the modifications made during the use case to be committed.
- ***Election Personnel*** are the people actually performing the system use cases, under the supervision of *Election Organisers* (who validate the actions performed).
- ***Judicial Officers*** are responsible for monitoring the election process and ensuring that *Election Organisers* perform their duties in a proper and legal way. In certain use cases they explicitly participate in the validation of the use case actions.
- ***Party Representatives*** are appointed by parties to monitor the election. They have the right to be present during all election phases although they don't directly interact with the system. Their consensus may be required (according to the election system) for the initiation of the tallying process.
- ***Independent Third Parties*** are responsible for monitoring the election process and providing reasonable assurance with respect to the integrity of the election process. Independent third parties are typically neutral from participating parties and their role is to strengthen the public trust. They explicitly participate in several use cases in order to ensure that everything is conducted in a legitimate way and according to the regulations of the specific election. Their role is to audit the system operation and the functions performed by the system actors, utilizing any tools they may wish at any given time. Assuming that they do not identify any problems they facilitate the operation of the system by explicitly participating in the validation process of "system critical" use cases.
- ***Voters:*** The persons eligible to participate in the election process

The way that system use cases have been implemented facilitates the realisation of a simple access control mechanism based on the different roles. The general concept is that each use case can be only performed by some authorised actors (*roles*). Depending on the criticality of the specific use case a *validation phase* may be requested by the system, prior to the commitment of the use case results. This validation phase is implemented through the *Validate Action* use case and it is described in the next section. For instance, the work involved in a use case can be performed by an authorised actor (e.g. Election Personnel) but the resulting changes can not be committed until they have been validated, through the successful operation of the *Validate Action* use case by some other authorised, for this specific use case, actor of the system (e.g. Election Organiser).

In addition to this rather elementary *Role Based Access* Control (RBAC) [2] mechanism, it is extremely important to ensure that the system use cases can be only triggered in a predetermined sequence (workflow), thus ensuring that the steps for organising and conducting the election process are conforming to the conventional process while facilitating easier audit mechanisms. The suggested workflow is depicted in Figure 1.

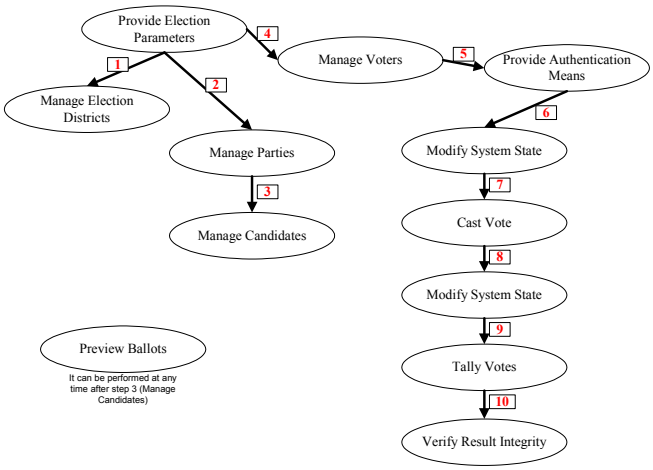

Figure 1. Use case sequence for organising and conducting a voting process

The "Election Set-up" state includes steps 1 to 6, as shown in the above Figure, the "Election in Progress" state steps 7 and 8, while the "Election Concluded" state steps 9 and 10. Most of the research effort nowadays has been focussed in the design and implementation of *Voting Protocols* that exhibit the required characteristics for fulfilling the security requirements of the "Election in Progress" state. However, it is evident that possible security incidents in the other two states, with emphasis in the "Election Set-up" state, can compromise the overall security of the e-voting system. For instance consider if, prior to step 7, some non-authorised person manages to modify the list of voters or candidates or even achieves to produce authentication means for non-eligible voters. Having identified this risk/vulnerability of e-voting systems, the

contribution of the RBAC mechanism together with action validation has been judged essentially critical.

3. The security framework of the administrative workflow

Trust is a critical success factor for election processes, whether electronic, or based on conventional means. In conventional elections, trust is enabled through the participation (active or observatory) of people representing different interest groups, stakes and authorities. For example, in most countries vote tallying is conducted with the participation of judicial officers, citizens and party representatives.

In electronic elections, in order for people to trust the system, it should be assured that no single actor or authority could manipulate the system. This can be achieved by means of enforcing the participation of several actors, in critical system operations, and by implementing the *separation of duties* principle [8], [1]. Within this context, the access control scheme is based on the principle that (a) each use case (e.g. "Provide Election Parameters") can only be performed by some authorized actors (i.e. users that have been assigned a *role*, e.g. "Election Personnel") and (b) the actions performed by this actor have to be *validated* by other actors.

3.1. The "Validate Action" principle

Based on the above observations, we argue that traditional authentication and authorization mechanisms cannot fully cover the needs of electronic voting systems. In the proposed *security framework for e-voting systems* a third phase, namely the *Validate Action*, has been added. Depending on the criticality of each use case, as well as on the overall impact of its results, the system requests validation from a predefined set of actors (e.g. "Election Organizer" and "Judicial Officer") prior to the commitment of the use case results. This extra validation phase is implemented through the *Validate Action* use case. Therefore, in order for an actor to perform a critical system operation, the following steps should be followed:

- **Step 1:** The user who intends to perform an administrative operation is authenticated, by means of providing his/her credentials to the voting system.
- **Step 2:** The authenticated user is assigned to a specific role and authorization is performed on the basis of the user's role. After the actor has been authorized, following the RBAC model, he/she performs the authorized operations. However, for use cases that perform critical administrative operations to the system, the authenticcation - authorization phase does not end at this point. Changes to the e-voting system resulting from those operations are not actually implemented; they are postponed until the next step is concluded. For the remaining use cases, not considered to be of critical importance for the system, operations are normally committed following successful authorization (see Table 2).
- **Step 3**: For critical use cases, a validation phase is performed: A predetermined set of actors validates the actions performed by the authorized users, thus committing resulting changes to the e-voting system.

Table 2. The "Validate Action" use case

		Roles					
System Use Cases	Activation *of* "Validate Action" Use Case	***Election Organisers***	***Election Personnel***	***Judicial Officers***	***Party Representatives***	***Independent Third Parties***	***Voters***
Authenticate Actor	**-**	A	A	A	A	A	A
Manage System Users	+	A		**V**			
Validate Action	**N/A**	A		A	A	A	
Modify System State	+	A		**V**			
Manage Election Districts	+	**V**	A				
Provide Election System Parameters	+	**V**	A	**V**			
Manage Voters	+	**V**	A				
Provide Authenticati on Means	+	**V**	A				
Manage Candidates	+	**V**	A				
Preview Ballots	**-**	A	A		A		
Cast Vote	**-**						A
Tally Votes	+	A		**V**	**V**	**V**	
Verify Result Integrity	+	A		**V**		**V**	

The actors participating in the realization of each use case, alongside with the corresponding validating *roles*, are listed in Table 2. More specifically the symbol "**A**" indicates the *roles* authorized to perform the use case tasks, while the symbol "**V**" is used to indicate the *roles* performing the validation of the specific actions. More-

over, the symbol "**+**" highlights the use cases requiring a validation phase, in order for their results to be committed, whereas the symbol **"–"** is used for the opposite case.It is demonstrated that the *Validate Action* is a distinct use case performed with the purpose of extending the traditional authentication - authorisation scheme that will meet the augmented security needs of an e-voting system.

The implementation of this validation-based scheme presupposes that the administrative use cases have been clearly defined (see Section 2) and the set of actors that participate in the validation of each use case is pre-defined.

3.2. Differentiations according to the election type

Our discussion, so far, has focused on an e-voting system that supports a generic type of election, that of 'General Elections'. The authors have considered in detail the cases of different types of election and decision-making processes, such as, for example *polls*, *referenda*, *internal* or *local elections*, comparing the requirements each of those pose to the system. It has been concluded that no substantial differentiation in terms of the functional requirements (use case model) and the respective workflow exist. We therefore argue that the functionality of an e-voting system, as described with the use case model presented in Section 2, can support most types of election processes. For example, in order to organize and conduct a *Poll*, use cases like *Manage Election Districts* and *Manage Parties* are not essentially differentiated in terms of their functionality, since we can assume that only a single district and a single party (ballot) are employed.

Concluding, we argue that by modifying the actors who are authorized to perform the *Validate Action* use case (in other words the actors who can commit the result of a use case) or/and by altering the "Election Set-up" sequence of use cases - utilizing tools that support the customization of the system - (i.e. not performing specific use cases; for instance the *Manage Election Districts* one if there are no Election Districts), it is possible to differentiate both the functionality and the security level that the system exhibits. In this way, it is possible to support different type of election process like polls, internal elections etc.

4. Concussions

In this paper we have addressed the issue of security in the administrative operations that are performed through an electronic voting system prior to the actual election process. The conclusions resulting from our research include the following:

- Traditional authentication and authorization mechanisms cannot fully cover the security requirements of the administrative workflow in an electronic election system.
- An extension of the authentication-authorization scheme is necessary, which can be provided by a mechanism that requires validation of user actions before actually enforcing any changes to the system.
- Such a mechanism presupposes a clear specification of administrative use-cases and a precise determination of the set of actors expected to participate in the validation of each use case.

Furthermore, we have presented a comprehensive security framework, based on the *Validate Action* concept, which has been developed specifically for an electronic voting system.

References

[1] Clark, D., Wilson, D., "*A comparison of commercial and military computer security policies*", in *Proc. of the Symposium on Security and Privacy*, IEEE Press, USA, pg. 184-194, 1987.

[2] D. Ferraiolo, R. Sandhu, S. Gavrila, D. Kuhn, R. Chandramouli, "Proposed NIST Standard for Role-Based Access Control", *ACM Transactions on Information and System Security*, Vol. 4, No. 3, August 2001.

[3] G. Booch, I. Jacobson, J. Rumbaugh, *The Unified Modeling Language User Guide*. Addison-Wesley, 1999.

[4] Ikonomopoulos S., Lambrinoudakis C., Gritzalis D., Kokolakis S. and Vassiliou K., "Functional Requirements for a Secure Electronic Voting System", in *Proc. of the 17th IFIP International Conference on Information Security*, pg. 507-520, Egypt, Kluwer Academic Publishers 2002.

[5] Internet Policy Institute, *Report of the National Workshop on Internet Voting*, March 2001.

[6] Lambrinoudakis C., Tsoumas V., Karyda M., Ikonomopoulos S., "Secure e-Voting: The Current Landscape", in *Secure Electronic Voting: Trends and Perspectives, Capabilities and Limitations*, D. Gritzalis (Ed.), Kluwer Academic Publishers, 2002.

[7] Mitrou L., Gritzalis D., Katsikas S., "Revisiting Legal and Regulatory Requirements for Secure e-Voting", in *Proc. of the 17th IFIP International Conference on Information Security*, pg. 469-480, Egypt, Kluwer Academic Publishers, 2002.

[8] Sandhu, R., "Transaction control expressions for separation of duties". In *Proc. of the 4th Aerospace Computer Security Applications Conference*. IEEE Computer, Society Press, USA, pg. 282–286, 1988.

[9] The Swedish Government, *Internet Voting – Final Report from the Election Technique Commission*, 2000, available at http://www.justitie.regeringen.se/propositionermm/sou/pdf/sou2000_125.pdf

[10] VoteHere Inc., *Network Voting Systems Standards*, April 2002.