UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

A Model for Direct Recording Electronic Voting Systems

Mini-dissertation by

NELLY SOLEDAD MEDINA MEZA

(24310523)

Submitted in partial fulfillment of the requirements for the degree

MASTER OF INFORMATION TECHNOLOGY

in the

SCHOOL OF INFORMATION TECHNOLOGY

of the

FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

University of Pretoria

Supervisor: Prof. Martin S. Olivier **August 2008**

Abstract

The automation of the election process has been experimented in many countries during recent years, to demonstrate that it accelerates the election process and that it offers many advantages; however, such automation also needs to satisfy many security requirements to guarantee a transparent process. In this dissertation, a model for an electronic voting system is proposed. This model focuses on the security risks and the vulnerabilities associated to these processes.

As in any election process, electronic voting needs to meet the appropriate standards regarding the basic principles and attributes of a good democratic election. In this study, the principles considered as the basic requirements for electronic voting, are analyzed and included in the proposed model.

This dissertation discusses the Brazilian case for being the first country in the world where a 100% of the citizens voted electronically. It also presents other experiences related to Direct Recording Electronic voting in other countries in order to compare and critically analyze the different models. The best features of each model are taken and examined in order to propose secure electronic elections that maintain the selected principles as key requirements.

Acknowledgement

I would like to use this opportunity to express my gratitude to:

- My supervisor, Professor Martin Olivier, for his guidance and valuable support.
- John Endres and David Gauna for reading and editing the draft chapters, and giving valuable recommendations and advice.
- My husband, César, and my daughters, Xidikarí and Nicole, for their understanding, patience and support throughout my studies. They are my inspiration.
- Finally my greatest appreciation to my mother, Carmen.

Table of Contents

Chapter I

Chapter II

Chapter III

Chapter IV

Chapter V

Chapter VI

Chapter VII

Chapter I

Introduction

1. Introduction

Since communication technology has become an important part of modern society, it brings a security problem inherent to the interchange of information through the networks. The economic and social benefit of Information Technology (IT) embraces dependence on systems and networks but unwittingly also their susceptibilities to failure (Lindsay, 1993).

In a country's general election, the process of casting votes is one of the most important processes. It needs to be automated with a high level of security criteria such as integrity, confidentiality, availability, reliability and assurance (Neumann, 1993). In addition it is a process that needs to be executed in the shortest possible time without compromising the integrity of the information.

According to Carracedo (2002), in the last few years different governments have experimented with electronic voting and argued that further development is still required. He attributes this to basic factors such as, the technical difficulties to satisfy the security requirements in all the stages of the process as well as, the requirement to guarantee the right to vote for all the citizens. However, he said that the basic problem is the cultural change which implies that the society must trust the new system that not only requires skills to use the system, but the confidence on a technology that is not well-known, and that seems to be more vulnerable to external manipulation than paper voting.

Despite the view that electronic voting requires further development and trials, it must be conceded that it is an important advantage for a country to use information technology to

collect and tabulate the votes. McGaley and Gibson (2003) stated in their research, that there are several advantages over the manual system, such as a quicker tallying process, the elimination of human error that sometimes occurs in manual vote tabulation, and the expansion of voting to those with disabilities.

In this sense, Brazil is one of the countries that have made enormous advances in the electoral process since 1996, when 33 percent of the voters used electronic ballot boxes, distributed in 57 municipalities (Riebeek, 2002). Later, in 1998, seventy five million of electors voted through electronic devices and, in 2000, one hundred per cent of the population (more than 108 million electors) participated in the biggest automated electoral process of the world, delivering the results in a few hours (Guimaraes, et al, 2001; Pezzuol, et al, 2001). Despite the progressive advancements in the Brazilian case, its success evoked criticism from the technical and political sectors, that alledged flaws in the process (Oliveira, 2001).

The United States is another country that has been using computer based voting since 1970. There is no uniform voting procedure in the country because every State has the autonomy to adapt the voting method that they consider best. In October 2002 the US Federal Government allocated $3.9 billion to upgrade old election equipment in the entire country (Riera, 2003).

The most popular technology to cast electronic votes is the Direct Recording Electronic technology It is based on the usage of computerized voting machines that allow voters to register their votes by touching the screen, a keyboard or a panel with buttons (Ruttledge, 2002).

Other technologies that have been used to perform electronic voting are optical readers, punched cards and internet voting. Internet voting is a good alternative in the flexibility that it offers to the voters, as the vote can be registered from almost everywhere, simply by being connected to the internet, but there are many security gaps that have not been resolved yet.

Given that the future of a nation is determined by a national election, in almost all of the countries that have conducted elections electronically, the process has been questioned, despite the advantages that it offers over the conventional methods of voting, such as greater speed and accuracy of ballot tabulation (Riera, 2003).

As IT professionals we defend the use of technology for electoral processes but at what cost to the integrity and confidentiality of the data? Bechtold (2003) said: "*technology enables, shapes, and limits social, legal, and political relationships among citizens, businesses, and the state."* But on the other hand Oliveira (2001) questioned upto which point should democracy be placed at risk by the fact that certain processes are being automated.

In this research the Brazilian elections and other electronic voting experiences in America and Europe are analyzed. The whole process and the security methods used in the different stages of the voting process are discussed. It also covers the difficulties encountered as well as technical problems and detected risks. Finally,a model that seeks to overcome the authentication and security problems encountered in these voting processes is proposed.

2. Problem Statement

This research will propose a model, based on the lessons learnt of the mentioned cases that will be analyzed. The model will present the requirements that should be considered in a process for electronic voting, to improve the security, and it will identify the sub-processes where security is important to maintain the integrity, confidentiality and reliability of the information.

In order to design this model it is necessary to analyze, evaluate and compare the most critical aspects of electronic voting. The study will examine the performance in all the phases of these voting processes as well as, the critical vulnerabilities, giving special attention to the authentication and the counting process. The best of each process will be taken to design a refined model.

3. Limitations

Due to time constraints, this study will be limited to one type of voting technique, the Direct Electronic Voting or kiosk voting, not covering other methods like internet voting. However there will be a chapter dedicated to analyze the different kinds of electronic voting systems in order to present the whole spectrum of this important way to vote.

4. Structure of the research

The first chapter of this dissertation introduces electronic voting and identifies the problem statement.

Chapter two introduces the different voting systems. It starts by describing the paper based voting systems and concludes by presenting the two main electronic voting systems, Direct Recording Electronic (DRE) and Remote voting system or Electronic Distance Voting (EDV). This chapter ends with a list of the advantages of electronic voting.

The third chapter is dedicated to the security in electronic voting systems as a key requirement in all the voting processes. This chapter is divided into two parts; the first one defines some of the criteria that applies to all voting processes like authentication, confidentiality, uniqueness, integrity, availability, reliability, flexibility, verifiability and convenience. The second part presents the common threats to computer systems and how these threats can affect electronic voting.

Chapter four discusses the electronic voting processes in Brazil. It starts with a short summary of the Brazilian national elections from the time that they implemented electronic voting. It follows with a description of the electronic voting process in Brazil and the main risks identified in the process.

The next chapter presents experiences with DRE voting in other countries. The selected processes are from Belgium, the Netherlands, Germany, Australia, United States and Venezuela.

Chapter six starts with a section dedicated to the influence of social engineering on electronic voting, as a main security concern. It continues with the model proposed for DRE voting processes, which highlights the different phases and their identified risks and how these risks can be mitigated.

Finally, chapter seven sets out the recommendations and the conclusion to this mini-dissertation.

Chapter II

Electronic Voting Methods

1. Electronic voting

The term "electronic voting" refers to the incorporation of information technology at one or more stages of the electoral process. It is generally used to describe any type of voting that involves electronic means (IPI, 2001, cited by Connolly, 2004). However, there are some differences in the definition of electronic voting in terms of the inclusion of the electronic apparatus in the recording of the vote (known as the "front-end" of the election) or in the counting process or "back-end". According to Riera & Brown (2003), electronic voting refers to the incorporation of information and communication technologies (ICT) at the front-end of the election system; it therefore implies the use of an electronic device to record the votes directly in a digital format. Contrary to conventional, paper-based ballots, the voter has to interact with some kind of machine to vote. After the voting process has concluded, the votes are tallied electronically. Riera & Brown (2003) also state that the inclusion of ICT at the "back-end" of elections is a common practice in almost all developed countries, which means that even when the voters place their votes on paper ballots, and these are collected in voting urns, the electoral board counts the votes electronically to speed up the counting process, for instance by using optical scanning machines (Riera & Brown, 2003).

Other authors consider that the term e-voting includes any kind of electronic system used at any stage of the electoral process, such as in the counting phase. This is the case, for instance, for mark sense ballots, which consist in a paper ballot that is read with a computer

scanner or with mark-sense reader devices attached directly to each ballot box, allowing even paper ballot votes to be counted electronically (Jones, 2001).

In any case, there is a common opinion about three levels of voting systems according to the automation included in the process: the first level is the Paper-Based Voting System or Conventional Voting System, the second level is the Direct Recording Electronic Voting (DRE) and the third is the Remote Voting System. The first level is not really considered as electronic voting but will be included in the classification to provide a complete view of the different kind of systematic voting methods (as opposed to earlier systems such as a show of hands or voice approbation or *viva voce*) (Reynolds and Steenbergen, 2006). The second level or Direct Recording Electronic Voting (DRE) includes ICT at the "front-end" of the voting process and is usually PC-based, with computers being used as voting machines and no paper involved in the voting act (IPI, 2001); the third level, also known as Internet Voting, use DRE devices to record the votes, but employs the internet as the channel to transmit the votes.

1.1. Paper-based voting system

The Paper-based voting system is the classical voting process used in the past in many countries. Votes are registered on paper, punch-cards or mark-sense cards, and the results are generated on paper. It is also known as Manual Vote Collection (McGaley & Gibson, 2003). In some cases the voter uses an electronic device to register the vote but the votes are not stored or saved in any kind of register or database (Tuesta, 2004). The different kinds of voting system in this category are Paper Ballot, Lever Voting Machines, Punched Card Voting, Mark-sense ballots and some other alternative processes such as vote by mail. A brief explanation of this voting system is given below.

1.1.1. The **Paper Ballot** system is the classical voting process, first introduced in Australia in 1858 (Jones, 2001), by the British Colony of South Australia as a way to introduce a secret vote while protecting voters from manipulation or intimidation. This way of voting was called the "Australian Ballot" and was

adopted in Britain under the 1872 ballot act. (Reynolds and Steenbergen, 2006). The paper ballot has been improved through the years and is still used today. Candidates' names are printed on paper ballots and the voters mark boxes next to the name of their candidate using a writing tool. The paper ballots are collected in ballot boxes and are counted manually by election officials (Fisher, 2001). This voting process has the problem that counting is laborious and subject to human error (IPI, 2001).

1.1.2. Lever Voting Machines were first used in New York, United States, in 1892. They consist in rectangular array of levers that may be arranged with candidates from right-to-left and parties from top-to-bottom, or viceversa. Voters pull down the desired lever to make their choice; when the voter exits the private room the levers return to their original positions and a connected wheel turns one-tenth of a full rotation to count the vote. At the end of the voting process the counters indicate the number of votes that were cast on each lever (Saltman, 1988). There is no paper ballot involved because the lever machines count the votes as they are cast, simply accumulating votes; therefore there is no possibility to recount (Jones, 2001). The Internet Policy Institute (IPI) states in its Report of the National Workshop on Internet Voting (2001), that this voting method prevents voting for more than one candidate and that some versions produce an audit trail. It is still used in some counties of the United States but lever machines are no longer manufactured (IPI, 2001).

1.1.3. Punched Card Voting was first used for voting purposes in 1964 in the United States. Even though punched cards were developed for data processing in the 1890's, only in the middle 1960s were they used as a voting tool. This voting method is based on pre-scored cards, which require voters to record their vote by punching holes in the card in a specific location depending on their choice. The cards are counted at a central counting center using a punched card reader attached to a computer system (Jones, 2001). Some

systems use hole punch type devices while others provide the voter with pins to punch out the holes. These methods of punching the cards have been subject to incomplete punches resulting in errors reading the cards (IPI, 2001). The system has the benefit that the punched cards can be manually recounted and audited (Fisher, 2001), as is the case for paper ballots. It implies an advantage over the lever voting machines, because the votes are stored, for the first time, in a computer or memory storage.

1.1.4. **Mark-sense ballots** are based on optical mark sensing technology first used in 1955 by the University of Iowa (United States) for educational tests. It consists in a physical paper ballot where the voter marks the selected choice by filling in an oval, a circle or a box with a writing tool. The ballots are read in a machine which uses light as a sensor. Ballots can be counted in a central-count setting with only one high speed counter serving an entire county or with mark-sense readers attached directly to each ballot box (Jones, 2001). The first generations of mark-sense readers allowed only a standardized ink or pencil lead and it was difficult to prevent voters from using their own pens or pencils, which invalidated the vote. Newer versions are based on scanners that can read marks made from almost anything. The problem is that if the ballot paper has a defect or a smudge darker than the paper it can be taken as a vote, which results in an overvote (Jones, 2001). An advantage of this kind of voting method is that it allows manual recounting of the votes, and the votes are stored in a computer memory as in the case of punched cards.

1.1.5. The traditional poll site voting or paper-based voting has been enhanced with **Alternative Processes** or alternative ways to cast the votes. The aim of these alternative voting processes is to increase the voting participation and give access to people with disabilities or those that are unable to attend the election in the polling places. One of the most used alternative processes is the **Vote by Mail** or **Absentee Ballot**. In this process the voter receives the ballot by mail before the election and has to return the completed ballot by mail. To be

admitted to vote by mail the registered voter has to certify his impediment to getting to the polling place on the election day (IPI, 2001).

1.2. Direct Recording Electronic Voting System (DRE)

The Direct Recording Electronic (DRE) voting system is based on electronic machines that use microprocessor technology to record the vote electronically and process it by software. Therefore it is the first voting method that uses computers at the front-end of the electoral process, such as a specialized voting machine or a voter-choice entry station in a voting booth, with touch screens, push buttons or a keyboard. The voting machines are connected to a stand-alone Personal Computer (PC) to store the votes in a digital format and to tally the votes electronically. It has the advantage that more than one voter can simultaneously record his or her vote with the entry device and all of the votes are summarized in a single computer (Saltman, 1988). In this voting system there is no need to have a paper ballot involved in the process: once the voter has entered and confirmed his or her vote it is stored in the computer's memory and any recount or audit trail should be done electronically, unless a proof of the vote is printed, which the voter can place in a ballot. This alternative will be analysed later in this study. The DRE was conceived originally with no printed proof of the vote.

Direct Recording Electronic machines (DRE) were first introduced in the 1970s as a computerized version of the mechanical lever machine (Saltman, 1988), and are currently used in many countries.

DRE systems may be classified in two main groups depending on where the casting of the votes takes place. These groups are Electronic Ballot Voting and Electronic Kiosk Voting, which are explained below.

1.2.1. Electronic Ballot Voting refers to the casting of ballots at public sites. The entire process is controlled by election officials, from the authentication of the voter to the storage and transmission or physical movement of the summarized

votes to the central center. It involves ICT systems controlled by election officials. The voting choices are displayed on a computer screen or on a ballot posted on the machine; voters make their choice by touching the screen, using a keyboard or pushing a button (Connolly, 2004). The votes are stored in databases to be tallied at the end of the voting period. These systems can be connected through virtual private networks (VPN) to the central processing center for tabulation of all the results; alternatively, they can be stored digitally at the place where the vote takes place and then sent to the central tabulation center via telephone lines or manually in removable data storage devices. (Saltman, 1988).

1.2.2. In the case of **Electronic Kiosk Voting,** the terminals are located in convenient places like shopping centers, post offices, libraries, hospitals, embassies or schools. The whole voting platform remains under the control of supervisors, and the environment can be modified in order to monitor the terminals. Supervisors may include election officials, observers, volunteers and cameras, which address security and privacy to prevent coercion and guarantee the secrecy of the vote (IPI, 2001). The main characteristic of this kind of voting system is that results are not accumulated or counted at the polling place, like in Electronic Ballot Voting, but are instead sent via VPN to the central tabulation center. The votes can also be stored digitally on removable data storage devices to be physically transported to the central center where they are summarized.

1.3. Electronic Distance or Remote Voting System

The Electronic Distance or Remote Voting System is one step behind DRE voting in the sense that the votes are transmitted via the public internet using web servers. In this model the electronic registration, recording and counting of votes is done from different locations at private or public sites such as home, schools, office, libraries, post offices, malls or shopping centers. The results are not accumulated or counted in the polling places but at

the tabulation center. It is an ideal voting system because it allows users to use a more generic technology to cast their votes, such as interactive digital TV, telephone, Short Message Service (SMS) or the internet (Connolly, 2004).

The implementation of Remote Voting Systems was conceived in the United States to enable military personnel or US citizens outside of the country to vote from embassies, hospitals, offices or home, given that people can virtually vote from anywhere at anytime. The problems with this kind of voting system are the risks associated with the security and integrity of the data, which will be discussed later in this research.

According to Tuesta (2004), the remote voting or network voting system can be attended or unattended. These two different alternatives are briefly defined below.

1.3.1. In the case of the **Attended Network Voting System,** the voter has to move physically to a polling center to cast his or her vote. There, he or she will be authenticated by the administrator and assigned a computer or a terminal to register the vote using a keyboard, touch screen or push buttons. The voting place can be a polling place totally controlled by election officials or a public place, such as the kiosk voting method, also controlled by election officials, observers or cameras, but located in more convenient places such as libraries, shopping centers, post offices, etc. The data is transmitted to the central counting center by internet or via a public network. (Tuesta, 2004).

1.3.2. With the **Unattended Network Voting System** the voter is allowed to vote from virtually anywhere, using the internet as a platform to transmit the data. It is a non-assisted voting system because the voter does not have to displace to a polling center and can use a more generic technology like interactive digital TV, telephone or internet, to cast the vote from any preferred place (Connolly, 2004). This type of voting system is also called Electronic Distance Voting (EDV) and has been used in many countries. Some of the modalities for EDV, as defined below, are Internet Voting, Short Message Service (SMS) Voting, Telephone Voting and Digital Television Voting.

1.3.2.1. Internet Voting refers to the use of the internet to register the vote, in any private place such as at home, at the office, at school, or any other place where the voter or a third party controls the voting client (IPI, 2003, cited by Connolly, 2004). This is an ideal form of voting which gives voters maximum flexibility for casting their vote. Internet voting has received intense scrutiny because of the risks associated with the security and integrity of the data transmitted versus the flexibility of voting. Internet Voting will be analyzed later in this mini-dissertation.

1.3.2.2. Short Message Service (SMS) Voting is a method that has been used in some countries and allows the voter to register the vote by sending a short text message to the polling station. It is an application that reaches more voters due to the fact that more people have mobile phones than internet, so for governments it is also a way to overcome the "digital divide". It allows greater parts of the population to vote without the fear of having to use a computer, which may be a factor for voters who have never used them before (Connolly, 2004).

1.3.2.3. Telephone Voting is not widely used, in spite of the advantages it offers. It is used mostly for disabled people and consists of an interaction with the electronic voting system through a phone call. The voter calls a number and has to authenticate with a secret code to gain access to the voting system. If he or she is a registered voter, he or she is given access to the system and follows the instructions to cast the vote. The first time this voting system was officially used was in the Liberal Party of the State of Novia Scotia in Canada, where about 7000 members participated in the election of party leaders by telephone (Slaton, 2000, cited by Connolly, 2004).

1.3.2.4. Digital Television Voting is also an electronic voting system, where the link consists of digital television, allowing users to interact with the system through their television sets. The data is transmitted using

telephone technology. It has not been widely used in official elections, but has been employed for TV shows (Connolly, 2004).

This concludes the overview of different voting methods; some authors have other classifications but essentially they describe the same voting systems. Independent of the different modalities of voting, we can state that the voting process is considered electronic when the voter has to interact with some kind of electronic device to record his or her vote in a digital form before it is transmitted by some ICT system to a repository, where the counting process takes place.

Figure 1 shows the different kind of voting systems described in this study.

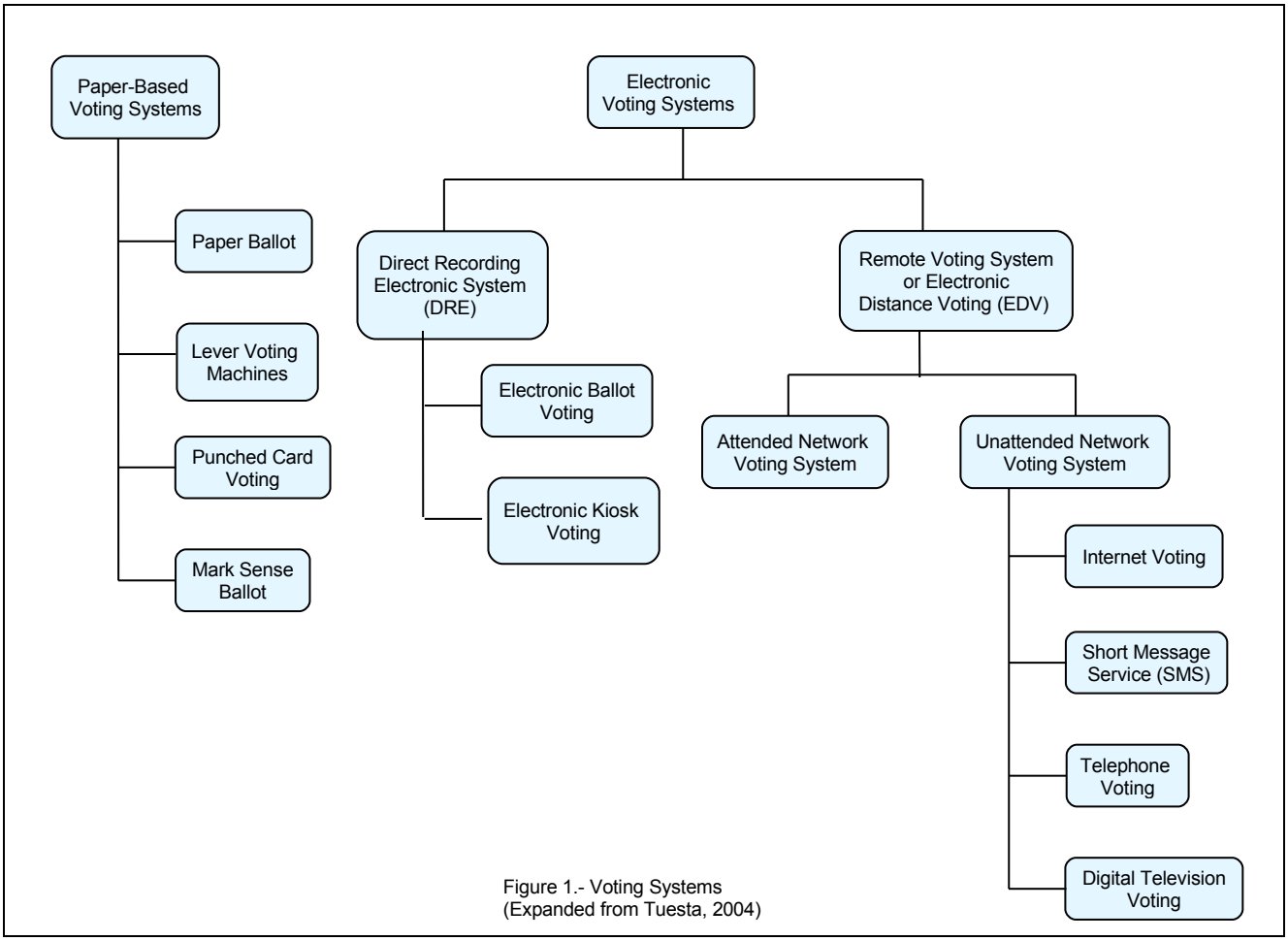

Figure 1.- Voting Systems
(Expanded from Tuesta, 2004)

2. Advantages of Electronic Voting Systems

Electronic voting systems are characterised by the fact that they incorporate ICT into the system, which introduces many advantages but also many risks. In the following section some important advantages of the electronic voting systems are described and analyzed.

One of the greatest potential benefits is the increase in speed of the ballot tabulation process. As the votes are stored digitally and the counting process is automatic, the waiting time for the results is reduced significantly.

The increase in accuracy of the results is another advantage, but it depends on the kind of system used and the design and conditions of the hardware and software, as well as human behaviour (Fisher, 2001). The accuracy of the results is threatened by security risks that in some cases are more devastating than the security risks involved in the traditional paper-based voting systems.

One important issue that has to be highlighted is the cost associated with electronic voting. The first investment that the government has to make is the acquisition of hardware and software, which involves high costs. But it brings economies of scale as the increase of the size of the electoral roll does not increase the cost linearly (Riera & Brown, 2003). It also brings savings in future elections as the hardware and software are reusable and because the ballots no longer have to be printed, but can now be shown on a computer or terminal screen.

Accessibility is another added value for electronic voting systems, as it allows alternative ways to access the ballots. It decreases rates of abstention, especially when the remote voting method allows widespread technologies to be used, such as cellphones (for SMS voting) or the internet. The fact that voters do not have to move physically to a voting centre to cast their vote provides geographic independence and better accessibility for people with disabilities, increasing electoral participation (Riera & Brown, 2003).

Given that the ballots are designed through computer systems, multiple language options can be provided on the ballot. If the system is user-friendly it will also offer more information about each candidate to help the voters in their selection.

Electronic voting systems can help prevent common errors as undervoting (voting for less than the allowed number of candidates) or overvoting (voting for more than the allowed number of candidates). In case of an error, the system will display an error message to the voter and ask him or her to repeat the vote.

These are the most important advantages of the electronic voting systems; the disadvantages involve many security issues that we should analyze before highlighting these disadvantages. Therefore the next chapter consists of a review of the security risks contained in the electronic voting systems.

Chapter III

Security Issues

---

1. Security in Electronic Voting Systems

After the overview of different types of voting system, we can say that electronic voting is fundamentally more flexible than paper-based voting, due to the accessibility and possibility to vote from convenient places as shopping centers, post offices, libraries, hospitals, embassies or schools. Remote Voting especially allows the voter to exercise his or her right in a very convenient way in terms of voting time and location (Lauer, 2004). It also has the benefit of increasing voter participation, especially among youths, business and holiday travelers, people with incapacities, and overseas personnel, thereby reducing voter apathy. The proponents of internet voting also suggest that it may reduce the cost of elections in the future (IPI, 2001) as the technology can be reused. This issue will be analyzed later in this study as it has also been suggested that because the internet and some remote voting technology transfers some election costs to the voter, governments may have to compensate voters for some expenses such as those incurred in SMS voting, voting using telephony technology, or internet voting. However, in spite of all the advantages of electronic voting, it is widely considered to be the most controversial voting system because there are vulnerabilities and risks involved with the use of ICT technologies. These vulnerabilities include incidents such as intentional attacks on the system or the unavailability of the services, which must be analyzed and controlled in order to guarantee the right of the citizens to express their vote in a transparent process.

There are many contrary positions on electronic voting. For instance, Mercuri (2001) author of a doctoral dissertation on electronic voting, analyzed the security criteria for electronic voting and concluded in her thesis that current measures are insufficient. After a decade of research in this area, she considers that voters will have to wait a long time

before they can rely 100 percent on electronic devices for voting. She states that in every case, the vote should be supported by a printout to be verified by the voter and deposited in a ballot box, which would allow a future manual audit in case of problems.

On the other hand, there are experts who defend pure electronic voting and compare it with the sophisticated computers used in the aerospace industry, which rely on highly complex software but are tested extensively and continuously and are considered reliable (Gerck, 2001, and Shamos, 1993, cited by Brunazo, 2001).

Electronic voting is associated with several security risks relating to reliability, user proficiency and system security (Leenes et al, 2003 cited by Connolly, 2004). Any election system must meet standards with regard to security, secrecy, equity, and many other criteria that make electronic voting more challenging to implement than other electronic government applications (IPI, 2001).

To analyze security in electronic voting systems we should start by defining the main voting principles or criteria that apply to all voting processes and are considered basic characteristics and attributes of a good democratic election. For the purpose of this research, were selected the principles related to security and manipulation of data as **authentication**, **accuracy**, **reliability, availability** and **integrity** as well as those that relate to the right of the citizens to vote in secrecy and in a simple and accessible way, as **confidentiality**, **flexibility** and **convenience.** Finally **uniqueness** and **verifiability** were considered important because all the voting systems should have the possibility to verify the votes and to detect any intent to overvote.

Authentication is the process by which a voter is identified and validated on the system in order to ensure that only authorized users are allowed to vote. "*Authentication is a process by which one satisfies another about one's claim of identity"* (Gong, 1993). In traditional voting systems it is ID cards or passports that confirm the identity of the voter, thus problems with authentication are eliminated through face-to-face communication.

Conversely, in electronic, ICT-based voting the identity of the parties involved in the information exchange or communication has to be confirmed by a secure protocol; both the sender and the receiver should be able to identify the other party reliably (Connolly, 2004). The challenge here is to guarantee that unauthorized individuals are not permitted to vote, or, even worse, to modify the content of a vote (as malicious hackers or corrupted administrators might be inclined to do) and commit a criminal fraud. Authentication includes the registration process, which is completed before the election day. During registration, the voter has to identify him or herself to be registered in a database that will be used to establish the identity of the voter. On the day of the election, each voter has to be authenticated through some secure protocol used to communicate with the server that contains the information of all the valid voters and confirms their identity. In DRE systems such as electronic kiosk voting, the voter would conventionally have a polling card that is given to the voters before the election, once they have expressed their intention to vote. The polling card has a unique number and shows the voter's ID or passport number to identify him or her. In the case of remote voting procedures such as internet voting, the technique used to authenticate the users should be a more sophisticated mechanism such as digital signatures or biometric identification systems.

The principle of **Confidentiality** relates to the democratic right of all citizens to vote in secrecy and anonymously. In order to avoid vote selling or coercion, nobody except for the voter himself/herself should be able to determine how he or she votes (IPI, 2001). This means that authentication and registration have to be separated from the actual voting process, assuring that the votes are validated separately and independently from the voter authentication (Ikonomopoulos, et al., 2002). This is a technical problem that has to be solved in order to fulfill the requirement of the secrecy of the vote, because how can an individual be registered and identified in the same system and yet be able to cast an anonymous vote? (Kofler, et al., 2003). This problem has been addressed with the encryption of data using private key cryptography.

Another principle is **Uniqueness,** which refers to the fact that voters should not be able to vote more than once. The system should reject the voter in the authentication process if it detects that he/she has already voted.

The next principle is **Integrity,** which is commonly referenced in ICT and alludes to the reliability and accuracy of the data. Once the data is stored on a system it should not be possible to modify or destroy it in an unauthorized way or without detection. In a voting system integrity refers to the assurance that the vote will remain the same after the voter has cast it into the ballot box. *"An electronic voting system using ICT would have to ensure the integrity of all data communicated within an ICT voting system"* (Connolly, 2004). This principle points to the accuracy and quality of the information to ensure trust in the voting process. There are hashing algorithms that can be used to maintain the integrity of the data but it is also important not to allow modifications to the code once it has been certified; no configuration information should be changed, nor should the initial parameters. It means that any systems change has to be prohibited throughout the election process (Neumann, 1993).

The voting system must have high **Availability** to all users during the election day or when it is expected to be operational; it has to be protected from any hardware faults or denials of service (DoS), which refers to a refusal from a server to respond to a request. A secure ICT system has to enable communication when it is needed and prevent DoS attacks, or any other kind of attacks, that can compromise the access of a legitimate user to the system (Connolly, 2004). There should be proper verification-based access control to allow only legitimate users to vote or access the system and refuse all non-legitimated persons, but communication for authorized users has to be available at all times.

The system's **Reliability** is an important condition of the election, required to ensure participation and a transparent process. No votes should be lost by means of software or hardware failure or by network or internet communication faults. It refers to the robustness of the whole voting system (IPI, 2001). The software has to be tested through high-assurance methods to ensure minimum bugs in the system (Neumann, 1993). At the same

time, the communication path has to be secure to guarantee that the data transmitted is the same at the sending point as at the receiving point.

Accuracy refers to the correctness of the vote. The system must register the correct vote selected by the voter and it should not be possible to alter or eliminate it from the final tally. Invalid votes may not be altered or taken into account for the final tally (Connolly, 2004).

The **Flexibility** of a voting system alludes to the compatibility of the system with different standard platforms, technologies or operating systems. It should accept different kinds of format for registering votes (e.g., multiple languages or even adapted for people unable to read or write). It also should be accessible to people with disabilities (IPI, 2001). In this sense the participation will increase as the voting system will have the possibility to adapt external devices to accept blind people to vote, or people unable to read and write. In countries like South Africa, for example, is important that the system includes the options to translate all the systems menus to any of the official languages, which will result in voters more confident to record their votes.

The principle of **Verifiability** invokes the possibility to audit all the votes and verify that they have been correctly accounted for with a demonstrable election record of the votes (IPI, 2001). The whole process must be transparent and reproducible at any stage (Kofler, et al., 2003).

Convenience refers to the simplicity with which the vote can be cast; the voter should be able to cast the vote in a short and easy session without needing special skills, and with minimal equipment (IPI, 2001). The system should be friendly and easy to use.

All these criteria are considered universal principles for traditional or paper ballot voting systems and for electronic voting systems. Many of them are interrelated and the compromise of one can affect others. The administrators of the election have to dedicate special attention to ensuring that all these requirements are met in order to guarantee a democratic and trustworthy election system.

2. Threats to Electronic Voting Systems

All ICT systems or computer based systems have to be protected from external threats that attack the normal functioning of the system and that, in the case of electronic voting, may compromise the security of the election and lead to an untrustworthy process.

At the technical level, there are three vulnerable points under threat of attack: the server, the client (the machine of the end user or voter) and the communication path (IPI, 2001). The server and the client can be attacked by viruses, worms or Trojans that are delivered to the computer and, after being loaded, can start malicious attacks. The communication path can be threatened by Denial of Service (DoS) attacks, which interrupt the transmission of data and can bring down a server from the network.

To enable a better understanding of possible attacks and the way they compromise the electronic voting system, some of the most common threats to all the computer systems will be described. The threats selected are Denial of Service (DoS), Viruses, Worms, Trojans, Spoofing and Phishing. It is important to mention that these threats affect the voting systems as they affect any other computer based system.

2.1. Denial of Service (DoS) consists in attacks performed during a communication between a client and the host server (where the votes are tallied). When a DoS is executed the communication between the client and the server is interrupted by flooding the target with more requests that it can handle. In many cases only a reboot or a shutting down of the network will reactivate the connection. In the case of remote electronic voting the availability of the internet service is vital, and diagnosis and reactivation of the service can take hours once it has been stopped. The consequences can be devastating, as data or votes may be lost (IPI, 2001).

Some of the most common techniques or methods used to perform DoS attacks are ping of death, packet flooding and distributed DoS, which are briefly explained below:

2.1.1. The **ping of death** is a type of attack that consists in a flaw in the transmission protocol that controls how IP packets are transmitted over the internet (TCP/IP). These packets have a maximum size allowed by the protocol, but for ping requests larger than this size, the packets are fragmented into smaller segments that are reassembled at the receiving host. The hackers take advantage of this fragmentation, and when the target computer assembles the fragments, the result is a message larger than the allowed size, overloading the buffer and causing the operating system to crash (Rubin, 2001).

2.1.2. Packet flooding is another type of attack performed during the transmission of data through a TCP protocol. In a connection via the TCP protocol, an acknowledgment should be sent from the sender host to the receiving server after the packets have been transmitted. In the case of a packet flooding attack, the attacking host sends many packets but does not send any acknowledgment, causing the overflow of the buffer of the target host as it receives more and more packets while waiting for the acknowledgment (Connolly, 2004).

2.1.3. The **Distributed Denial of Service (DDoS)** is a massive attack launched from many computers simultaneously against a target server. It works through two programs called the *master* and the *daemon:* the master is installed on one computer and the daemon on many machines. Master and daemon are distributed through the internet to the different computers and lie dormant until the strike is to be launched. At the moment of the attack the hacker sends a signal to the *master* indicating that a specific target should be attacked; the master conveys this information to all the *daemons,* which flood the target system with more internet traffic than it can handle, causing the operating system to crash, freeze or reboot (Rubin, 2001).

2.2. The second threat considered are the **Viruses**, which are computer codes that recursively replicates a possibly evolved copy of itself causing malicious effects in the machines when they are activated. They are loaded without the knowledge of the end user, during a program download from websites or via a diskette or a CD. Once the virus has been downloaded it can infect a host file or system area, or simply modify a reference to objects to take control and then multiply to form new generations of the virus (Szor, 2005).

2.3. The **Worms** are similar to viruses but with the difference that whereas viruses need to be activated by the user through the execution of a specific file, worms spread autonomously without the action of a user. Worms are network viruses, primarily replicating itself on remote machines without any help of a user (Szor, 2005). Worms simply make copies of them and can become very destructive causing irreparable damage. In a voting system they could change the results of the votes, if programmed to do so, threatening the integrity of the votes (Connolly, 2004).

2.4. Other malicious threats to computer systems are **Trojan Horses**, which Szor (2005) defined as malicious programs that try to interest the user with some useful functionality to make them run the program. These attacks are very dangerous because they can delete or modify files in the attacked computer or retrace their steps to the compromised system, creating an "open door" from the computer to the hacker. Once this "door" is open any unauthorized individual can have access to confidential information such as passwords or, in the case of electronic voting, to votes. These kinds of attacks are a huge threat to the confidentiality and integrity of the information of ICT-based voting systems (Connolly, 2004).

2.5. **Spoofing** attacks are another type of risk to electronic voting. There is more than one way to spoof a legitimate voting site. For instance, an attacker may send an e-mail to the voter asking him or her to click on a link to access the voting site, but instead send him/her to a fake web page that simulates the voting site. The hacker may use the user's credentials to access the real voting site and vote for the attacked voter (Rubin, 2001).

2.6. The **Phishing** attacks use computer worms to steal information. A common practice is when the attacker uses social engineering to get private information as credit card information and PIN numbers, simply by asking the target person to disclose the information by using fraudulent web sites or spoofed e-mails (Szor, 2005). In a voting system these attacks can compromise the confidentiality of the votes if the attacker discloses sensitive information, as passwords and personal information, to get access to the votes.

The threats described above are some of the most common attacks that can be performed on voting systems, but depending on the method used for electronic voting, the vulnerability changes. In the following section we will examine the level of vulnerability for the two electronic voting systems defined in this research, DRE and EDV.

The security threats for **Direct Recording Electronic Voting Systems** are characterised by the fact that pieces of malicious code can be installed on the target machine, such as viruses, worms or Trojans. The problem here is that the malicious software can be installed from any input device (floppy or CD-ROM drive), by e-mail or by executing some routine download from the internet; it can even be an unwitting download during a visit to a website. The crash of the system is one form of attack that sabotages the election. The consequences of a Trojan are even more serious because once it is installed it does not need to be activated, but may be executed by remote control, by a timer mechanism programmed into the malicious code, or it may be triggered automatically once it detects a specific event in the host computer such as the start of the election system. The integrity and secrecy of the results can be seriously compromised by a code that for instance could change a percentage of votes to a specific party or by a code that allows an attacker to spy on the ballot (IPI, 2001).

Security mechanisms designed to help avoid these attacks focus more on the election procedures, like the definition of controls for election officials to detect and prevent any connection to the internet. The voting machines do not have access to the internet but the computer used to authenticate the voters could have access. These computers should be configured to deny any intent to open web-sites. The DRE software can also be configured

not to allow any reboot of the machine during the election, nor to accept any software different from the election system to be loaded onto the DRE equipment (IPI, 2001). A key risk is that the vendor of the DRE software may already have installed a malicious code like a Trojan onto the system, which would be very difficult to detect.

There is another threat for DRE voting systems that has been highlighted by Lauer (2004), related to the trade secrecy of some software that does not accept examination of the code or adequate testing of the software before the election. To avoid this risk, election administrators should require Open Source system components and the option to inspect and test the source code at any stage of the election process.

Electronic Distance Voting systems are more vulnerable to attacks, especially Internet Voting, which is also threatened by DoS. The main server of the election can be protected by firewalls, but the voter's computer may be a personal computer or a computer in a public place such as an internet café. This means that the computer will not necessarily have enough protection, allowing a hacker to spy on the voting process and to intercept it with some malicious action. An example of a malicious action is the modification of the vote without the detection or knowledge of the voter, compromising the integrity and accuracy of the election system. The network traffic connected to the internet is also vulnerable to attacks by DoS, which can impact the availability of the internet service, thus sabotaging the election.

Some of the security mechanisms used to contain these risks are technologies such as Secure Socket Layer (SSL) or digital certificates, which aim to guarantee a secure connection between the end user's voting device and the host server. Authentication is a key process that has to be trustworthy and this means the use of encryption. This authentication protocol can be based on a conventional cryptosystem or a public-key system or both (Diffle and Hellman, 1976, and Needham and Shroeder, 1978, cited by Gong, 1993).

Finally, we can say that electronic voting, and especially EDV, is a voting method with many advantages, but the security risks associated with it cast doubt on the convenience of

this kind of voting. The security of an electronic voting system is the basis for the social acceptance of the e-electoral process, and until now, technological advances have not been able to provide completely secure electronic voting systems, even though technical security can be enhanced by physical and procedural security measures (Xenakis and Macintosh, 2005).

In conclusion, we can see that both voting systems, DRE and EDV, have vulnerabilities, but until now DRE seems to be more reliable than EDV. DRE maintains more control over the electoral process, allowing officials and observers of the voting process to detect flaws or failures.

Considering that EDV is more risky, the analysis of security threats needs more extensive research. Therefore this study will focus on the DRE voting system, which is the voting system selected by the Brazilian government for that country's electoral processes. The next chapter explains the Brazilian electronic voting experience and analyses the risk associated with these processes.

Chapter IV

Overview of the Brazilian Elections

1. Brazilian National Elections

As Kohno, T. et al. (2004) stated that an election system must be robust in order to avoid any dishonest and fraudulent behaviour and transparent enough so that the entire population as well as the candidates accept the results. On the other hand, they also noted that a voting system should be understandable by all the voters, even those that are illiterate or disabled. This is one of the greatest successes of the Brazilian voting process: It was carried out in the whole country, including the most remote villages in the deep Amazonian jungle, where the only mode of transportation available is the canoe (Riebeek, 2002).

Another success of the Brazilian process was the speediness of the process, which was considered one of the main goals of the election: from the recording of the votes to the disclosure of the results took only 24 hours in total. Unfortunately, many problems and vulnerabilities were also identified in these elections in regard to the security of the process, and affecting technical and political issues (Oliveira, 2001). One of the most discussed flaws of the election was that the voter confirmed his or her vote on the screen of the voting machine and not on a printout of the vote, which made it impossible to conduct a manual audit of the votes.

The Brazilian elections were studied in order to identify the failures and flaws of the process, as well as the criteria for assessing the security of electronic voting based on the lessons learned from the Brazilian experience. One of the experts on Brazilian electronic

voting states that the voting system used in Brazil is still a high risk system vulnerable to fraud due to the natural conflict between security and the necessity to maintain the inviolability of the vote (Brunazo, 2001).

In this chapter, a short history of the elections in Brazil will be presented as context information before the voting system and the different phases of the process are described. Finally, the main failures detected by academics and experts on the Brazilian electronic voting system will be addressed.

2. Brief History of Brazilian Elections

Brazil introduced electronic systems in the voting processes as early as 1982. On this occasion, they were used for the "back-end" of the election, i.e. the counting phase. It was considered to be a disastrous experience because it was discovered that military agents had tried to manipulate the process (Brunazo, 2005). But this was not a reason to give up the development of a total electronic voting system for the entire process: In 1996, electronic voting was used from the voter registration, including the authentication of the participants, to the publication of the final results. In this experience Brazil used the Electronic Ballot Box (EBB) with DRE technology. It was used only for the larger cities, comprising one third of the total number of voters (Brunazo, 2005).

The DRE voting system was used again in 1998. It was extended to two thirds of the total number of voters. Finally, in the municipal elections of October 2000, the electronic voting process covered 100% of voters (Brunazo, 2005).

The importance of these elections was the fact that Brazil was the first country in the world to carry out completely electronic elections that covered the entire country. 107 million voters took part in the elections, which implied providing approximately 354 000 ballot box machines to 5 600 municipalities across the country. A nationwide network was required, based on 28 large mainframes and thousands of terminals and access points to enable voters to elect nearly 5 400 prefects and 53 000 municipal legislators (Brunazo, 2000).

In October 2002, Brazil went on to another national election, this time for the posts of the country's president as well as governors and legislators. In this case there were more than 115 million voters using approximately 405 000 ballot boxes countrywide (Riebeek, 2002).

The key success was the speed of the process: within 24 hours, the results were known countrywide. Despite the opinion of the president of the Supreme Electoral Court, many Brazilian experts have analyzed the process and determined that there were vulnerabilities that weakened the system (Brunazo, 2005). One of the vulnerabilities was that the vote was not printed to confirm that it was correctly registered on the system, which eliminated the possibility of doing a manual audit of the tally. In this sense there have been many attempts in the National Congress to approve the verification of the vote on paper or VVPB (Voter Verifiable Paper Ballot), but the Supreme Electoral Court was against the VVPB and obtained an approval from the National Congress to not implement the verification of the vote on paper (Brunazo, 2005).

One of the failures reported in the election of 2002, during the presentation of the results, was a sudden drop in the number of votes for Luiz Inácio da Silva (Lula) to minus 41.000. The incident caused a great commotion. After some reboots to restore the count, the Supreme Electoral Court explained that the negative result was a "formatting error" (Rezende, 2003). In this election the winner was Mr. Lula da Silva.

It is important to explain that in Brazil, the Supreme Electoral Court has complete power over the elections. It is in charge of regulating, administering and judging the electoral process (Brunazo, 2005). This is unusual in a democratic country. Brazilian academics consider this to be the cause of a lack of transparency in the process, because all the decisions are made by a single institution. The same institution makes the regulations, establishes the limits of the elections, administers the budget for the voting process, manages the elections and judges any litigation. For instance, the Supreme Electoral Court decided to use the DRE machines without a paper ballot confirmation of the vote and also opted to use only one electronic ballot for three different stages of the process, namely for authenticating the voter, registering the vote and partially counting the votes in that ballot.

This is a typical characteristic of the Brazilian electronic ballot box and creates a security gap for the inviolability and secrecy of the vote.

After the election of 2002, there have been more experiences. All of them relied on the DRE voting system, using the same basic procedure. For the purposes of this study, we will analyze the 2000 elections to understand how the platform for DRE voting systems is structured using the electronic ballot boxes designed for Brazil.

3. Analysis of the Brazilian Voting Process

The technology selected for the Brazilian voting processes is based on the Electronic Ballot Box (EBB), called "Urna Electrónica" or UE in Portuguese. In the election of 2000 three types of UE were used, the UE96, UE98 and UE2000, depending on the year of manufacture and first use. All the models have the same basic hardware, which is made up of two main parts: the voter terminal and the "microterminal". The voter terminal consists in motherboard with a processor and memory capacity, a flash card unit, a floppy disk unit, an integrated monochromatic LCD (Liquid Crystal Display) screen, a numeric keypad and a printer (UNICAMP, 2002). The "microterminal" is used by the official administering the voting process and consists in a numeric keypad and two functional keys: CONFIRMATION and CORRECTION (Posner, 2006). It also has three LED lights; the first is red and when it is on indicates that the unit is connected to an energy source (that can be external or internal, through a battery). The second light is yellow and, when lit, announces that the corresponding voter terminal is being used. The third light is green, and if it is switched on it means that the EBB is free to be used by the next voter (Rial, 2004).

The voting software used by the latest model of EBB runs on the Microsoft Windows CE operating system and the application is from Unisys Corporation (Riebeek, 2002). All the mode of UE run over VirtuOS, which is an operating system developed by Microbase, which is a Brazilian company. The VirtuOS is compatible with Microsoft Windows and works in client-server environments supporting multiple protocols. The EBB also includes cryptographic algorithms to digitally sign all the electoral data (UNICAMP, 2002).

4. The Voting Process

The voting process starts with the preparation of the EBB one week before the election day. The EBB is prepared by deleting all the information stored in the memory from previous elections. Then it is loaded with a copy of the operating system, the application programs and the databases of the candidates, the municipalities, and the voters of the corresponding section where the EBB will be located. All this data is digitally signed in order to verify the integrity of the information. Then the EBB is programmed to start only on the election day. If it is switched on before that day, it will send a message asking to wait until the predetermined day. After this the EBB is physically closed and sealed (Camargo, 2005).

On the day of the election, each EBB is tested to verify the consistency of the hardware and software. The election process starts with the identification of the voter in the "microterminal", which is done by entering his/her registration number. This unit or "microterminal" can be adapted to accept a magnetic card or bar code to identify the voter (Rial, 2004). Once the voter is recognized, the EBB is unlocked and the voter is enabled to use it. Photos of the candidates are displayed on the screen of the terminal along with the name of the candidate, his or her party affiliation and a number or code. The voter selects the candidate from the screen by typing the code or number assigned to the candidate (Pezzuol, et al., 2001). The votes are encrypted and recorded in the flash memory. When all the voters registered for that EBB have voted, a tally of the votes of that EBB is performed; these results are printed and transferred to floppy disks. The disks are sent to regional offices of the Supreme Electoral Court, where the data is transmitted via dialup to the central headquarters in the nation's capital, Brasilia, for the final tally (Riebeek, 2002). A soft copy of the votes is kept in the memory of the machine.

In the elections of 2002 three percent of the voters (3%) used another type of machine that enabled them to verify their vote on a printout before confirming it on the screen (Rezende, 2003).

The Brazilian academic and expert on electronic voting, Brunazo Filho (2005), divided the voting process into four main steps: identification of the voter; secret voting; partial counting of the votes in each EBB; and total counting of the votes. In the next section each of these steps will be explained to provide a detailed description of the voting process and its security issues.

The first step is the **identification of the voter.** It starts when the voter presents his/her "título de eleitor", the identification card with the registration number, to the election official. The official types the number into the "microterminal" unit. Once the official has confirmed the identity of the voter, the EBB is ready to be used. This step concludes the authentication of the voter.

The second step in the process consists in the **secret voting** carried out using the voter terminal. This other unit of the EBB has a numeric keyboard and three functional keys: a white one that says "WHITE" and is used to vote null, an orange button that says "CORRECT" to vote again in case of an error selecting the vote, and a green button with the label "CONFIRM" to save the vote. The voter starts the process by typing the number of the candidate he or she wants to select and the terminal will show the photo, name and party of the candidate selected on the screen. If the voter is satisfied, he or she has to press confirm, or else press correct to choose another candidate. This process is repeated if the voting is for more than one category (president, governor, or legislator). In any of the options the voter can select the white key to vote null and continue with the next category. When all the candidates for the different categories have been selected, the screen will show the word "END" and the EBB will not accept any other option until it is activated again by the official that has the control unit or "microterminal". The control unit will automatically switch to green showing that the EBB is blocked and that the "microterminal" is ready to receive the next voter (Rial, 2004).

The next step is the **partial counting** that is done on each EBB once all the electors have voted (approximately 500 voters per EBB). The official administering the voting process has to introduce a password to register the end of the process for that voting machine. A first report of the EBB is printed, called the "Boletim da Urna" or BU; if it does not show

any error message the official presses the confirm key to print 4 more copies of the report. One of the reports is left at the polling station for public information; the second is given to the supervisors of the different parties at the polling station. The other three are sent with all the other voting material to the regional voting center. The information that the BU has is the identification of the polling place, the starting and ending hour of the voting process, the total votes by party, by candidate, number of null votes and the security code corresponding to that voting machine (Rial, 2004).

In addition to the BU, the results of each EBB are saved on other two media: a floppy disk that is sent to the regional voting center with the BU for the final tally of the votes, and a flash memory card that keeps a record of the votes inside the EBB. Once the first report is confirmed the voting machine encrypts the data to save it to the floppy disk and the flash memory card.

After the regional offices of the Supreme Electoral Court have received the BU and the floppy disks of the polling places, they send the encrypted data to the central headquarters of the Supreme Electoral Court where the final step of the process is carried out, the **total counting of the votes** and the publishing of the results. The transmission of the encrypted data is done through a private network that does not have any connection to the internet or any public network.

Security gaps can be found in all the steps of the voting process., The next section will describe some of the failures detected in each phase.

5. Identified Risks

By the brief overview given of the Brazilian voting process, we can infer that it bears the risk of flaws at many stages, which makes it even more important to pay attention to the security issues. This has been analyzed by many experts on electronic voting processes, who recommended solutions to avoid some of the flaws. For instance, their proposals included measures to improve the protection of the algorithms that compute the seeds of the data encryption (Pezzuol, et al., 2001); processes for analyzing the weakness of each

stage of the process and showing the vulnerabilities of the system in a technical audit (Oliveira, 2001); or providing criteria for the assessment of electronic voting security (Neumann, 1993; Brunazo, 2000); as well as many other suggestions on the software/firmware of the electronic voting system.

The four stages identified in the Brazilian election are each associated with risks. The most important are reviewed in this section and some suggestions are given to improve the process.

One of the main problems detected is that there are three different sub-processes of the election that are carried out on the same computer: the identification of the voter, the casting of the vote, and the partial counting. This creates a vulnerability in respect of the secrecy and anonymity of the vote, as the software could be changed to keep track of the vote for each person. Another, related security issue is the fact that the control unit or "microterminal" is connected to the voter terminal: The official administering the voting process has to type in a code to unlock the EBB to be used by the voter, but the program can be easily modified to tie the authentication process to the casting of the vote as the machines are connected and share the software. This will imply a violation of the voting principles of confidentiality and privacy of the election.

Another weakness of the current Brazilian voting process is the impossibility of doing a manual recount or manual audit of the votes. This represents a flaw in the sense that any audit performed will be based on the same data. If there is any doubt about the alteration of the software that implies changes of the data or votes loaded in the EBB, any recounting over the same data will not represent a guarantee of a proper audit because it is done on potentially altered data. The paper trail is the only way to determine if the votes stored on the EBB have been violated.

The paper trail will also provide the voter with the additional benefit of allowing him or her to confirm that his/her vote has been correctly recorded. The academic and electronic voting specialist, Mercuri (2002) considers it essential to have an individual print-out for examination by the voters, and to have a wholly independent audit trail. She states that as

all voting systems are prone to error the ability to perform a manual hand-count of the ballots is extremely important.

Another concern voiced in many studies is that the operating systems used (VirtuOS and Windows CE) are not open source, which means that the code is not available for public audit. This makes it impossible for neutral supervisors or experts to test the source code. The software is made by its manufacturers and there is no way to review the source, which is important in this kind of public process.

The authentication of the voter is another weak point, in the sense that it is done by typing in the voter's registration number. This can be done even without the voter being present: If a voter is absent, the registration number can be entered into the system and it will accept the vote from any other person. In this sense it is important to implement another identification mechanism such as verification through a magnetic card that only the voter possesses.

During the partial tally of the votes other risks have to be contained, like the possibility of changing the votes while they are being added up or the modification of the results. The EBB can also be changed before printing the results, for prepared EBBs with false votes.

The final tally of the votes on the server located at the Supreme Electoral Court is also a possible link subject to modification and tampering.

The identification in the EBB of the personnel working during the election to give them access to use the computer is not explained in any source reviewed for this research, but this password system has to be reinforced by encryption and digital signature to allow only the duly authorized person to enter into the election information system.

After this review of the Brazilian voting process this research will continue with a view of other experiences in different countries that used the same technology as in Brazil, the DRE voting system.

Chapter V

Voting Experiences in Other Countries

1. Introduction

The DRE system has been used in other countries and after the Brazilian experience the usage of this kind of technology for voting processes has increased. In Europe it has been used successfully in many countries. In Belgium, for instance, electronic voting was initially used in 1991 in a pilot project in two districts. This experiment was expanded in 1994 when 20% of voters recorded their vote electronically, and since 1999 a total of 44% of voters have been using electronic voting systems. During the voting processes of 2000, 2003 and the European elections of 2004 the percentage of voters in Belgium that used electronic voting was maintained at 44% (de Vuyst and Fairchild, 2005). In the elections of October 2006 100% of voters used electronic voting to cast their vote for the elections of 589 local government councils and 10 provincial councils (OSCE/ODIHR[1], 2006).

The Netherlands is another leading European country in electronic voting. It has been legally possible since 1965 to use electronic machines in elections, but the DRE voting method was used for the first time in 1990, when Nedap machines manufactured by a Dutch company were employed (OSCE/ODIHR[2], 2006). In this country electronic voting has been criticized because the source code is not public; only two companies were allowed to test it, the manufacturer Nedap and Brightsight, a testing laboratory that certifies the system for the government. But even with these controversies electronic voting is still in use in the Netherlands: In the parliamentary elections of November 2006 approximately 90% of voters used DRE voting machines and almost 20,000 voters abroad voted through internet voting or by mail.

In Germany electronic and software based machines have been permitted since 1999. Germany also used the Nedap voting machines, but is now experimenting with a new device: a digital electoral pen. This digital pen is still in the testing phase and the government has not yet approved its countrywide usage. The City of Hamburg ran a test

election in 2005 to evaluate the device (Volkamer and Vogt, 2006). Their experience will be analyzed further in this chapter.

In the United Kingdom small pilot projects have been conducted since 2000, using a combination of voting methods. The experiences with DRE voting machines are considered successful as no major problems were detected and indeed the assessment reports suggested that the faster declaration of the results was a significant benefit (Pratchett, 2002).

Other countries in Europe that have gathered experiences with e-voting are Italy, Spain, Estonia, France, and Switzerland; however, their projects relied mostly on internet voting, which is not covered in this research.

In Asia it is important to highlight the Indian experience with electronic voting, which was first introduced in 1982 and where the usage of Electronic Voting Machines (EVM) was legally approved in 1989. In the parliamentary elections of 1999 the EVM machines, manufactured by Electronic Corporation of India and Bharat Electronics, were used in 45 constituencies. In 2003 they were used again on an experimental basis (Benoit, 2004).

Australia used electronic voting for the first time in the parliamentary elections of 2001, for approximately 16,559 voters. The Australian Capital Territory (ACT) implemented a system named EVACS (Electronic Voting and Counting System) that runs on Linux, which is an open source operating system. The finished source code was published for public review, and some bugs were found after public and academic reviews, but the general opinion was positive. The voting system was tested in the 2001 election and a comparative manual count showed that the system had performed successfully (Benoit, 2004) . This experience is presented in this research.

In South America electronic voting has not been extensively used, but Brazil is acting as a promoter in the region. In 2003 Brazil signed agreements with Argentina and Paraguay to implement and use the Brazilian DRE machines or UE in these countries. Another country that has used DRE voting is Venezuela, during the 2004 recall referendum on President

Hugo Chavez. The voting machines selected were manufactured by the Smartmatic Corporation and used by approximately 70% of the electorate, but many irregularities were found (Taylor, 2005).

Finally, the U.S. experiences with DRE are also important to highlight due to the different controversies and initiatives raised in the process, which are considered useful for this study. Elections in the United States are notable because the country is highly decentralized: each state has the autonomy to select its own voting process, so that many different technologies are used during the same elections. Among the various electronic voting experiences in different states, one of the voting processes that has been widely analyzed is the experience of the state of Florida, especially during the U.S. presidential elections in November 2000, labeled by some authors as the "Florida fiasco" (Weiss, 2001; Riera, 2003). It caused the loss of millions of votes, revealing many security flaws in the electronic machines, as well as deficiencies in the systems. But as a consequence many initiatives were set up to upgrade the elections equipment in order to restore lost confidence to computer based elections.

There are many other countries that have introduced electronic voting in their elections but the summary given above involves the most representative and interesting for this research. In the next section the voting procedure of the following countries will be explained: United States, Belgium, the Netherlands, Germany, Australia, Paraguay, and Venezuela.

2. Overview of the Electronic Voting Process in Belgium

Belgium currently uses two different voting systems: the "Digivote" and the "Jites", which are mutually incompatible, although their voting and counting procedures are similar. The source code of both systems was published in a government portal for review by the citizens and the general public (OSCE/ODIHR[1], 2006).

The different municipalities have to choose the system they want to use, and once the system is selected the process starts three or four weeks before the election day, when the lists of candidates are registered on the system. The Justice of the Peace of each

municipality has to review and approve the lists and then the regional officers of the Ministry of the Interior, who administer the voting process, start to prepare the sets of floppy disks to be used in the polling stations. The information loaded on the disks is encrypted and a password is generated for each polling station.

The day before or on the morning of the election day the polling station chairperson receives a package with the floppy disks, the password and a set of magnetic voting or ballot cards.

The hardware in each polling station consists in the voting machines, one computer and one electronic ballot box. Approximately 1000 electors are registered per polling station and one voting machine accepts 200 voters. The software has three modules: the voting application that is installed on the voting machines, the application to initialise the magnetic cards and the program to tabulate the results (OSCE/ODIHR[1], 2006).

On the election day the voting machines and ballot box are activated with the information decrypted from the floppy disk. When the voter arrives, he or she is identified as a registered voter and receives a magnetic ballot card (OSCE/ODIHR[1], 2006). Then he/she goes to the polling booth where inserts the card into the voting machine to see the list of the candidates on the screen. The voter selects his/her choice on the screen, whereupon the vote is encrypted and stored on the magnetic card. The voter takes the card from the machine and leaves the polling booth, showing the card to the polling station official to confirm that it does not have any mark that could identify it. Once the card has been confirmed the elector inserts the card into the election ballot box. When the magnetic card is inserted into the ballot box the encrypted vote is stored in the RAM of the computer and on the floppy disk, to store the votes on another external device in case of any power failure.

At the end of the voting process the electronic ballot box summarises the votes and the totals are encrypted and stored in several backup disks. These disks are transported manually by the chairperson of the polling station to the municipality's main electoral office, where all the votes are tallied and the results published (OSCE/ODIHR[1], 2006).

The limitation observed in this process is the absence of a paper audit by the voter, which bears the risk of creating some doubts about the accuracy and confidence of the votes as they are only stored digitally. The vote that is registered on the magnetic card is not verified by the voter and the only way to recount is through the votes stored on the magnetic cards.

3. Overview of the Electronic Voting Process in the Netherlands

The DRE voting machines used in the Netherlands are deployed by the Nedap/Groenendaal corporation, and the model that is most used is the ES3B (OSCE/ODIHR[2], 2006).

In each polling station there is one personal computer running Micrsoft Windows, to which many ES3B voting machines are connected, as is a reader unit and a printer. Nedap also provides some special models of voting machines designed to be used by people with impaired vision. The special models include audio headphones to assist users during the voting process.

The voting machines have a small screen and a touch-sensitive surface with labels to identify each candidate. The voter has to touch the label corresponding to his or her choice and the screen will show the name of the candidate selected. To confirm the vote the elector has to press a red button, whereupon the vote is added to the other votes. When all the voters assigned to the polling station have voted, the computer prints out the totals and that report becomes the official record of results for the polling station (OSCE/ODIHR[2], 2006).

The main problem with these voting machines -- besides the lack of a paper audit allowing voters to verify their vote -- is the fact that the firmware is proprietary to Nedap and no public review of the source code is possible. The only company that can test the firmware is Brightsight, a testing laboratory that certifies systems used by the government. For instance one of the weaknesses is that the machines are tested by Brightsight before they are sent to the polling stations, but at the polling station no official inspection is carried out

to verify that the firmware is still the authorised one. The OSCE report highlights that some municipalities do perform a pre-election test, but it is not mandatory.

4. Overview of the Electronic Voting Process in Germany

Germany has employed the Nedap voting machines in some electoral processes but what is interesting to outline in this research is a new device that has been tested in the City of Hamburg since 2005, the Digital Electoral Pen.

The Digital Electoral Pen uses so-called Anoto technology, which has been developed by the Swedish Anoto Group AB (Volkamer and Vogt, 2006). It consists in a pen with a compact scanner and a paper ballot that contains dot patterns as a 2 dimensional barcode. When the voter makes his or her selection, the pen loads the coordinates where the pen was used, and this information is used by the system to match it with the electronic voting form to cast the vote.

The polling station has to have one personal computer, at least one digital electoral pen, three docking stations, one printer and a portable storage device to transfer the results. When the voter arrives at the polling station, the polling clerk initializes the digital pen with the first docking station and once activated the pen is handed to him/her. The voter receives the digital pen and the paper ballot, and once in the polling booth selects his/her choice by writing a cross in a box behind the candidate chosen. In this moment, the digital pen stores the coordinates where the cross was made on the paper ballot. If the voter wants to correct the vote, he or she has to destroy the paper ballot and go to the polling clerk, who will delete the data in the pen with the docking station and initialize it again. The voter then receives another paper ballot and the initialized digital pen to start the process again. Once the voter is sure about his or her vote he or she has to drop the paper ballot into the ballot box and insert the pen in a docking station that will copy the data to the electronic ballot box and delete it from the pen to prepare it for the next user (Volkamer, and Vogt, 2006).

There is more than one advantage in this voting method. Firstly, it is a process similar to traditional voting processes: the use of electronic means to record the vote is practically

invisible for the voter.. Secondly, it is possible to recount the votes manually using the paper ballots. Thirdly, it speeds the publication of the results as the counting process is done electronically.

This voting method has not yet been approved in Germany and is still in the testing phase for certification and legal approval, but as a new voting technology it is important to consider it in this research.

5. Overview of the Electronic Voting Process in Australia

The Electronic Voting and Counting System (EVACS) used in Australia is based on barcodes to authenticate the votes. A set of barcodes is produced before the election day. 50,000 barcodes were produced for the election of 2001, with a unique number associated with the voters and with each polling place. Each polling place had a personal computer (PC) that emulated a server, with two hard disks for backup and a removable zip disk, nine standard PCs with a barcode reader attached, plus one additional PC with the barcode attached and headphones; these 10 PCs were connected to the server. One additional PC was installed but not connected to the server, and was used for demonstrations (ACT, 2002).

For security reasons the software was loaded onto the server on the morning of the election from a tested, officially-approved CD-ROM.

The voting process starts with the identification of the voter as a registered voter. Once the voter has been authenticated, the election officer asks him or her if he or she wants to vote electronically or on paper. If the voter selects electronically, he or she receives a barcode and is directed to the polling booth that has one of the PCs installed. The “welcome screen” of the system asks the voter which language he or she wants to use (the software has twelve different languages loaded). Once the language has been selected the voter is instructed by the system to swipe the barcode using the barcode reader in order to bring up the ballot on the screen. The voter has to navigate through the different candidates with the arrow keys and once the desired option is highlighted, he or she presses the SELECT key. For the

parliamentary elections of 2001 there were multiple posts up for election, so when the voter pressed the SELECT key the number 1 appeared behind the name of the first candidate selected and the voter had to repeat the steps for the next candidates, which were numbered in the order selected until all the choices were made.

The voter has the option to erase a choice with the UNDO key and select a different candidate. At the end of the selection the voter presses the FINISH key and a confirmation screen is displayed with all the candidates selected in preferential order. At this point the voter has the option to press the UNDO key to return to the ballot and correct any of the options or, if the voter is satisfied with the selection, he or she has to approve it by swiping the barcode again and the vote is recorded on the server. The welcome screen is then displayed again on the monitor for the next user. When the voter leaves the polling booth he or she has to insert the barcode into a ballot box.

At the end of the election day the database with the votes is encrypted and stored on the removable zip disk (ACT, 2002).

One of the problems reported with this voting method was the failure of the barcodes. Sometimes the barcode reader did not recognize the barcode and it was necessary to swipe it several times. If the barcode was not recognised the assistance of the election officer was required in discarding the barcode. This was done by means of a security process where the voter and the election officer signed a form to certify the damaged barcode and another barcode was issued to the voter. Another disadvantage was the level of usage of technology, which was seen as being complicated. This can be demonstrated by the statistics reported in the Australian Capital Territory (ACT) report on the Legislative Elections of 2001, where it was shown that only 7.57% of voters chose to vote by electronic means (ACT, 2002).

One advantage of this method is the secrecy or privacy of the vote because the vote is associated with the barcode and not the voter, which maintains the anonymity of the vote.

6. Overview of the Electronic Voting Process in United States

Computer based voting systems were first introduced in the United States in 1970, and since then are becoming increasingly popular due to their advantages over paper based voting techniques (Ruttledge, 2002). The complexity in the United States is that each state has the autonomy to select its own voting method, which implies that many types of voting methods are involved in the same election.

Some of the elections between 2000 and 2006 have been seriously threatened by system failure and recounting problems. In the presidential elections of 2000 in Florida, many problems were detected that caused the loss of 4 to 6 million votes. The voting method used in this case was based on punched cards and this failure stirred up many controversies. It also caught the attention of academics and researchers that recommended the replacement of the old voting machines in favour of new voting technology (Caltech, 2001). The details of this election will not be analyzed in this study as our interest is in the DRE voting methods.

In 2002 Florida moved to the use of touch screen voting machines, which were first used in the primary elections of September 2002. Many problems were found during this voting process as well. In Miami-Dade County, for example, the voters reported that the machines reset themselves while the voters were trying to vote. In Palm Beach County the electors encountered difficulties in selecting the candidate because when they touched the screen nothing happened, or the machines froze up while voting. The polling workers reported problems when trying to activate the electronic cards used to authenticate the voter and in some cases the card was rejected. It was also detected by the voters that it was possible to select a candidate that had not been touched by pressing the screen in two different positions simultaneously, resulting in an unintended vote (Mercuri, 2002).

The State of Florida bought voting machines from different companies, among them Sequoia Voting Systems located in Oakland, California, and Election Systems & Software Inc. (ES&S) located in Omaha, Nebraska. Both systems had problems: The ES&S presented performance delays in booting up with some machines and other computers reset themselves at any stage of the voting process, a problem also reported with the Sequoia Systems machines (Mercuri, 2002).

Another manufacturer of DRE voting machines from the United States is Diebold Election Systems Inc. from Canton in Ohio, which developed the Accu-Vote TS touch screen system. This system was used in two counties of Maryland, and it was reported in a study by University of Maryland that evidence was found of a digital divide, in other words, people familiar with computers found the system easy to use, but those with less experience in computers encountered difficulties in voting and needed help in the voting process (Evans, and Paul, 2004). The Diebold system also revealed delays in the voting process due to problems with the authentication of the voters (Mercuri, 2002).

The voting process for the different systems is basically the same. It starts with the registration of the voter, which is done previous to the election day. On the day of the election, the voters identity is checked against the registered voters. Once is verified that is a registered voter and has not voted, receives a smart card from the voting clerk and is directed to the polling booth where the voting machine is located. The voter has to insert the smart card to be able to make his/her selection by pressing the touch screen; if the voter confirms the vote, it will be cast and recorded on one of the internal flash memory cards. The smart card is then initialized and the voter has to return it to the voting clerk. At the end of the election the official that is administering the voting process has to insert an administrator smart card or "ender card" and the system will store the totals on another, removable memory card and print the totals as a hard copy. The removable memory card is taken to the tabulation center (Feldman et al., 2007).

The main failures found with the DRE touch screen systems developed by the three companies aforementioned are caused by software bugs, which caused votes to be lost and resulted many controversies. Besides these problems it is considered important to highlight the lack of a paper audit trail for the voter to verify the vote recorded.

The fact that this country had many problems with its voting processes raised initiatives to improve the election process and to standardise it throughout the country. One of these initiatives was the creation of the Help America Vote Act (HAVA) by President Bush in October 2002, to establish a program to provide funds for the upgrade of the election procedures and voting systems, to create a Commission for assistance in the administration

of Federal elections and to establish minimum standards for election procedures (HAVA, 2002). The HAVA allocated the amount of US$3.86 billion for election upgrades, to replace punch-card and mechanical-lever voting machines with newer voting systems (Evans and Paul, 2004).

Another interesting issue of this country is the definition of security standards since 1990, when the first set of national requirements for voting equipment was introduced, published by the U.S. Federal Election Commission (FEC). Later, in 2002, a revised version of these requirements was approved, which included security aspects, as well as human factors, disability access and functional and audit requirements that should be considered in the electronic voting processes of the country (Deutsch and Berger, 2004).

7. Overview of the Electronic Voting Process in Venezuela

In Venezuela electronic voting was used in a national referendum on the 15th of August 2004 to decide whether to recall President Hugo Chávez from the presidency. The Venezuelan electoral authority CNE ("Consejo Nacional Electoral"), which supports Chávez, announced that 59% of the votes were "NO", indicating the rejection of the recall, so the decision was that Chávez would stay as president without recall (Felten et al., 2004).

The votes were casted in voting machines based on a touch screen interface, manufactured by the Smartmatic Corporation. After registering a vote the machines produced a voter verifiable paper receipt, and once the voter had verified the vote confirmation of the vote, he or she inserted the receipt into a ballot box to enable future manual audits (Felten et al., 2004).

According to the authorities, the overall process was smooth and flawless, but the opposition raised some fraud allegations. For instance the first security audit was done in only 1% of the voting machines, which were not selected randomly, with the government deciding which machines to audit. A second audit was performed, with participation of the opposition, and showed that approximately 400 polling stations had two or more machines with the same number of "yes" votes, and in 380 polling stations it was found that two or

more machines had the same number of "no" votes. The analysis by academics Felten, Rubin and Stubblefield (2004), of the Venezuelan referendum, did not detect any statistical anomalies, even though they suggested that the silent switching of some percentage of "yes" to "no" before the vote was stored in memory, would not produce statistical irregularities.

In this we have a new element to analyze, which is social engineering or social responsibility for computer security. How can the non technical intrusion in a voting process be detected and avoided? The human intrusion will be briefly analyzed in the next chapter that wraps up the foundation and propose a model for the DRE voting systems.

Chapter VI

Design of a Model for Direct Recording Electronic Voting Systems

1. Introduction

The review of the different experiences of DRE voting systems shows clearly that achieving the required level of transparency in elections is more difficult with electronic than with paper-based voting systems. One of the main concerns is the reliability of the votes registered on the system. Reviewing the performance of the system during the election is not easy. It mainly depends on the certification of the software through the tests made before the election and on the paper trails. Therefore the challenge of using

technology in these kinds of processes includes implementing proper procedures to verify the integrity of the data. The problem is that there is no straightforward method to verify that the vote has not been modified before it is stored. Even if the software has been checked and certified as reliable and protected from any external intrusion, it is still at risk of manipulations from the inside (Vollan, 2005).

The risks of a DRE voting system have been classified by Vollan (2005) in three categories: those that are caused by bad software designs or bugs that cause failures in the normal performance of the system, those caused by manipulations from outside the system such as attacks by hackers, and those caused by manipulations from inside the system.

The risks caused by software bugs are usually detected in the testing phase before the software is certified. Risks caused by manipulations from outside are mitigated by firewalls and safety procedures such as not providing any access to public networks, or not allowing the use of any external storage into the hardware. Finally, the risks caused by manipulations from inside the system are more difficult to detect because a silent change in the data can be programmed to be triggered after the software has been tested and once the election starts. Such changes might be undetectable and the result would be a fraud difficult to prove (Vollan, 2005).

Another risk element that has to be considered as part of the manipulations from the outside is the social engineering or human intervention aspect, namely tampering with the system by tricking other people. These are non-technical attacks that are present in all implementations of computer systems and the voting systems are not extent of such attacks.

In this chapter a model for a DRE voting process will be proposed taking in account previous experiences and providing containments for main risks detected. This proposal will be preceded by a section that analyses the social engineering aspect and its consequences in the electronic voting processes as many of the manipulations from inside and outside are consequence of this aspect.

2. Influence of Social Engineering on Electronic Voting

Social engineering refers to the threat to the confidentiality of the information created by deluding authorised users to reveal information by telling them some plausible untruth (Anderson, 2001). It is a non-technical intrusion that normally involves the manipulation of people to break security procedures to access computer systems.

In politically troubled countries with fragile democracies a transparent electoral process is not guaranteed. Social engineering attacks are common in these countries and represent a threat to the overall process. Human intrusion is a threat for paper-based voting systems and electronic voting alike. It takes advantage of innocent people to break security systems and have access to the data manipulating the votes.

Social engineering is commonly used to fool people on the password level, for example by asking them for their password to perform some technical support and instead using it to access confidential information. In electronic voting a polling station worker can be fooled to provide the voting system's access code, allowing the attacker to use it to tamper with the data or to install malicious code. Such attacks are often planned to be performed on the day of the election after all the certifications and audits of the system have taken place.

If there is no paper audit it will be difficult for observers to detect the fraud. The absence or poor quality of security procedures creates additional vulnerabilities that threaten the voting process.

Even when provision is made for a paper audit the voter is not always able to demonstrate the fraud. A DRE voting machine can be tampered with to change the vote intermittently. In this case, if a receipt is printed, the voter will detect the fraud but it might be difficult to demonstrate that the DRE is cheating. To prove the misbehaviour of the voting machine the voter would have to reveal his/her vote in first place. If the malicious code is programmed to ignore one in every fifty votes, for example, then the next inputs to replicate the failure will be unsuccessful. The voter will not be able to demonstrate or prove the fraud (Karlof et al., 2005).

Mitigating this kind of attack involves reviewing weaknesses related to the personnel administering the election, the procedures and the policies (Fischer, 2003). With regard to the people involved in the voting process as well as the manufacturers of the voting machines, it is important to ensure that they are trustworthy.

Another consideration to be taken into account is the training of the officials who will man the polling stations where the voting will take place. They have to take responsibility for the password and authentication process. They will also have to be clearly instructed with regard to the procedures to follow in case of problems. The education of the voter is also important as a way to avoid fraudulent acts through social engineering.
In the model proposed the selection and training of the election personnel is an important activity that is included in the overall process in order to mitigate the risk of social engineering attacks.

3. Proposal of a Model for Direct Recording Electronic (DRE) voting system

After the study of some experiences with DRE and analyzed the most important risks and problems detected in those cases, a high level model can be proposed in order to avoid these problems and contain the risks identified in this study. The model of DRE selected is the Electronic Ballot Voting, which refers to the casting of the votes at public sites and the voting platform is controlled by election officials and personnel trained to support the voters.

The intention is not to do an exhaustive plan but to define the main steps that should be followed in any electronic ballot voting process.

The model suggested is shown in the figure 2 which includes the activities at the top and the resources involved in the process at the bottom. The resources or people involved in the process are represented by broken lines or by continuous lines. The broken lines refer to a

non direct involvement in the activity, with no responsibilities. The continuous line means a full commitment with that activity.

The time is represented in the horizontal axis where the dotted line means that it is not defined the specific duration for those activities: it can take from months to years to complete them.

The process starts with the **Definition of the number of servers and voting machines** that need to be installed to cover all the voters. This activity is tied to the **Selection of the infrastructure** that consists in the analysis of the different software, hardware and network that can be used. The network will connect the servers located in the regions with the main or central server where the votes will be totalized and published. There are some important considerations to take in account when defining the infrastructure:

a. The software that identifies and register the voters have to be a separate application from the one that records the votes. This will ensure the privacy of the voting, avoiding any attempt to link the vote to the voters which will break the anonymous and secrecy of the voting process.

b. The software should allow a paper trial, therefore the installation of printers in all the polling sites has to be considered.

c. It is highly recommended to use an open source Operating Systems to make available the source code for public audit and testing by neutral experts and academics. This was successfully done in Belgium for two different voting systems, as was highlighted in the chapter five of this study.

d. For the authentication of the voter it should be considered an identification mechanism that guarantees that the voter will be authenticated only once and that nobody else will replace his/her identity. One of the mechanisms that have been used in previous experiences is through a magnetic card that is handed to the voter before the election day. There is a risk associated to this mechanism, if the card is lost or taken by another person. Another mechanism more sophisticated but also more secure is the biometric identification system, which has the disadvantage of the costs implications.

e. The identification and authentication of the personnel that will work in the election is another process to be examined in detail to avoid any unauthorized personnel to have access to the election system. A digital signature is recommended or a biometric identification system.

The definition of the hardware has to be done simultaneously with the selection of the infrastructure because depends on the type of voting machines that the infrastructure is designed and defined. As a high level calculation, the country has to be divided in regions and in each one the number of polling sites will depend on the voters registered for that specific region and the number of voting machines will depend on the capacity of the specific voting machine selected; in the Brazilian elections was used one ballot box for approximately 500 voters. It has to be considered also two PCs in each polling site and one printer. One of the PCs will be a stand-alone machine with the database of the voters registered in that specific polling centre, that will be used to authenticate the voters. The other one will be connected to the voting machines and to the central server in the region. This second PC will consolidate all the votes of the polling site and will send this partial result to the server. The server in each region will receive all the votes from the different polling sites and will send them to the main computer. These servers will be connected by a VPN to the central server.

For these activities the resources involved are the election officials responsible for the selection of the infrastructure, and the vendors that will advise and inform about their products.

The next step is the **acquisition of the infrastructure** or the voting platform which starts with the calling for a tender process to receive the different offers from the vendors. It is important to follow a transparent process and allow public reviews. The selection of the vendor is an important task that if it is managed transparently will give confidence to the citizens to rely on the process increasing the participation. It is suggested to publish the source code of the systems offered, in a government portal, to allow the general public to review it and detect bugs or malfunctioning of the systems. The resources involved in this activity are the election officials, the vendors and the voters on the first stages of the activity when they participate on the review of the source codes.

As it is shown in the diagram the **selection of technicians and selection and training of the personnel** will start in parallel with the acquisition of the infrastructure. The technicians will be a combined group from vendors' personnel and technicians hired by the election officials. This activity should start once the vendor is selected. The selection and training of the personnel that will work in the polling sites is an important activity that has to start the soonest possible to ensure a complete training on the voting tools that will be used during the process. The training should include information about the risk of social engineering in the process. This personnel has to be reliable and well trained to support the voters during the voting process but they also have to be prepared to detect and manage any failure or flaw on the system or on the process and take proper actions.

The personnel and technicians that are being trained are not directly involved with the process at this stage, as it is shown with a broken line.

The next step consists in the **installation and configuration of servers** which directly involves the technicians to install the hardware, software and network. The servers will be implemented from the beginning, not as the voting machines that, due to security reasons, should be implemented a few days before the election day. The administrators of the voting process together with the vendor have to select carefully the personnel that will be in charge of the implementations, and once the installation starts there should be supervisors through all the setup of the servers.

It is important to highlight that neither the servers nor the PCs will have access to the internet; these machines will be dedicated servers having only the voting system loaded.

During the installation of the servers the voters have to be loaded into the database. This is a **registration process** that the voters have to follow to give their details and the place where they intend to vote. The way this process will be done depends on the authentication system selected; it can be face-to-face or an online registration. The personnel will have the responsibility to register the voters and maintain the database during this process, starting their direct involvement with the whole process.

Until now the process may take a few months or even years to end up with the servers installed and the voters registered in the system. The next activities instead have to be done close to the election day, because it implies the implementation of the whole system which expose it to external intrusions. It is recommended to have one week as the maximum period to start the following activities. In the Brazilian voting process these activities started one week before the election day, as it is explained in the chapter four of this study.

Once the servers are implemented and tested, and the registration process is finished, the process continuous with the **preparation of the voting material.** This preparation consists in the creation of the passwords by encryption procedures, for each polling site as well as the disks or CDs that will be sent to the regions, together with all the printed material needed to setup the environment in the polling sites. The resources involved are the election officials and the personnel and technicians. The vendor is involved indirectly from now until the end of the process.

The **setup of the environment** starts with the installation of the operating system, the database of the candidates and the application program into the voting machines, and the installation of the database of the voters for each region in the personal computers of each polling site. From the Brazilian experience the voting machines are loaded with all the information in the central offices and all the data is digitally signed, the system is deactivated and the machines are sealed to be sent to the regions. This is a good practice if the security of the system is guaranteed that will not be violated during the transporting of

the machines. The personal computers and printers that will be installed in each voting site have to be also prepared and sent to the regions. Once the machines are sent to each site it is recommended to reactivate the software only the morning of the election, like the Belgium experience that is referred in the chapter five of this mini-dissertation. The preparation of the platform in the polling sites consists in the installation of the security systems, voting machines, PCs, printers, and the testing of the machines and the connectivity between the voting machines and the PC and from the PC to the regional server. The duration of this activity depend on the number of polling sites and the number of resources available. It has to be a short period as the election officials will take control of the public places selected as voting centers like libraries, schools, hospitals, post offices, shopping centers and embassies. The last installation is the voting software that should be done the same day of the election or the night before. There will be external observers that have to certify that the system is working under all the security standards required.

The day of the election the personnel will start authenticating themselves and the supervisor of the polling site will activate the voting application through an encrypted password.

During the **voting process** the voter is authenticated first through the stand-alone PC and if it is an authorized voter, he/she will be instructed to vote in one of the voting machines. The personnel working in the polling site have to explain the voter the details of the voting process. Once the voter has registered the vote, he/she has to wait for the print out to confirm the vote and introduce it in the ballot box. If the voter notices an error or mistake on the print out, he/she has to ask for the vote to be cancelled and proceed to vote again.

At the end of the voting process, the polling site will be closed and the PC connected to the voting machines will consolidate the votes and do a **partial counting**. An external backup has to be done with all the data and the results, which will be kept together with a printed report of the partial results. Security measures have to be taken into consideration to file these evidences of the results and transport them to the regional office. All this information will also be transmitted automatically to the regional offices to be totalized per region.

Once each region receives and summarizes all their votes, the results has to be sent to the central server where the **total counting** will take place and the results will be published, ending the process.

The next chapter has some final recommendations to consider for the DRE voting processes and it ends with the conclusions of this mini-dissertation.

Chapter VII

Recommendations and Conclusion

1. Introduction

This research analyzed, evaluated and compared the most critical aspects of the electronic voting. The proposed model is based on the lessons learnt from the references cases that were analyzed and it identifies the sub-processes where the security is important to maintain the integrity, confidentiality and reliability of the information.

It was examined the performance in all the phases of the Brazilian experience with DRE voting process as well as, the critical vulnerabilities. It was also presented experiences with DRE voting in other countries to take the best of each process and design a refined model.

2. Recommendations

To make the recommendations of this study we will follow the different phases of a DRE electronic voting process and highlight, in each one, the actions that are recommended to take, in order to mitigate the risks foreseen through this research.

The first stage is the **preparation of the elections,** which involves many activities that take place prior to the election day. With regard to the selection of the system it is recommended to carefully analyze the software in order to ensure its compliance with the

principles required for a trustworthy voting process. Some of these principles or criteria were presented in this study, namely as authentication, confidentiality, uniqueness, integrity, availability, reliability, accuracy, flexibility, verifiability, and convenience, and will be taken to formulate the recommendations.

One of the biggest concerns with an electronic voting process is the confidentiality and secrecy of the vote. If only one system is used for the whole process the votes can be linked to the voter, failing to achieve the secrecy of the vote. To comply with confidentiality it is recommended to select two systems, one for the authentication of the voter and the other for the casting of the vote. This will result in two independent databases allowing the votes to be anonymous.

Another recommendation is to develop the software under an open source operating system in order to allow more individuals and experts to review the source code. This will enhance the detection of bugs and errors in the system. We have seen, in the case of the Netherlands, that the firmware was not available for public review, thus limiting the tests. This brings the risk that the software is not well reviewed and many bugs may not be detected in time to correct them before the election day. In the Florida case systems errors were reported as the main failure of the elections. It is important to allow citizens to review the source code through a public website and to ensure enough time is provided to test the software and take their concerns into consideration. This will raise the voters' confidence, adding value and robustness to the election system and thereby ensuring that it is reliable and accurate.

The selection of the personnel that will be working in the election is a key activity that generally does not receive the attention it should. It is recommended to define a profile and choose reliable people not susceptible to untoward persuasion. They should receive training that includes security issues. It is important to explain to them all the vulnerabilities they will be exposed to and how to be prepared to avoid technical and non-technical intrusions. These people will have passwords to access the systems and they might have to deal with intruders trying to get access to the system.

Voters should be educated in order to avoid misunderstandings concerning the usage of the electronic machines while casting their vote. This is especially important for persons who are not computer literate. Such education can be organised through public sessions or through information provided by mass media such as television. The level of technology used in the voting system can be high but as long as the voters are well-informed and know how to follow the voting process, it should not be any problem to cast the votes. It is also recommended to have a stand alone PC in the polling place to demonstrate the voting process to those that require more help.

Flexibility refers to the compatibility and accessibility of the system. It is recommended to ensure that the voting system has special features to allow people with disabilities to vote without help and in secrecy. Language is another issue in some countries; we have found that in Australia the voting system had twelve different languages loaded onto the system. If the country has more than one official language it is recommended to select a voting system that permits different languages.

Once the voting system has been selected and tested it needs to be certified. The certification of the firmware is recommended to be done by independent reviewers. In the case of Brazil it was reported that the review was not objective because the institution that manages the elections and chooses the system is the same one that tests and certifies the firmware. Besides the inclusion of third parties for testing the system, it is also important to have a third party, independent from the administration of the elections, to certify the hardware and software.

Before the election the systems have to be installed on the voting machines, the recommendation is to download the software the same day or the day before in order to avoid any intrusion during the transport of the machines to the polling station. This can increase the risk of encountering problems when installing the software just a few hours before the election, but the personnel can be prepared to put in place further actions to solve almost any issue.

The security mechanism used to authenticate the authorised personnel that work at the polling station has to be robust and validated to block any attempt to access the system by unauthorised people. The use of cryptographic keys is recommended and if possible a biometric identification system can be used to enhance the security of the authentication process.

The election starts with the **identification of the voter,** which serves to authenticate his/her, identity and confirm that he/she is a valid voter. As explained in chapter three, the voter is validated by confirming his/her identity in the main database of registered voters. The recommendation in this process is to have a secure protocol system for the exchange of the information.

This system has to be tested and certified in order to ensure that unauthorized individuals do not get access to vote and that once a person has voted he/she is not able to vote again.

During the **casting of the vote** it is recommended that the system enable the validation of the vote by printing it; the voter should then introduce this paper into a ballot box so that it can be used for a manual audit. This issue has been extensively discussed and one of the main exponents is Mercuri (2002), who states that due to the vulnerabilities of the electronic voting systems it is extremely important to have the option to perform a manual audit of the ballot.

It is also recommended that the voting system include help screens and user friendly design to avoid misunderstandings and problems during the voting act such as under- or overvoting.

The availability of the system has to be guaranteed during the voting process. If any interruption is detected it is recommended to have a procedure in place to discard the votes that were being cast when the interruption occurred and to allow the voters to restart their voting process.

Partial counting is done at the polling site and it is an automatic function of the system once the voting has been finalised. The closure of the voting has to be done by authorised individuals and, like the start of the process, the end requires the authentication of the individual performing the closure of the voting.

Total counting is performed at a central office were all the partial counting results are received. The transportation of the partial results is a delicate matter as it is an opportunity for intruders to attempt to access and alter these results. This can be done manually by transporting the results in external devices such as floppy disks or compact discs, or automatically through an access to the main server via the internet or a virtual private network (VPN). If it is done manually it is recommended to take security precautions such as keeping more than one backup at the regional office and sending more than one copy of the results in different disks or compact disks. If it is done automatically the recommendation is to use VPN access and setup controls to block any download either by external input devices or via the internet. Access to the internet has to be blocked and it is important to implement a firewall to close any security gap during transmission of data.

In regard to the costs associated with the DRE voting systems, which have not been included as a topic for this study, it is important to highlight that even though it is a huge investment for the first elections, it implies savings in further elections, as the hardware and software are reusable and it also reduces the costs of paper and printing material for paper-based voting.

Conclusions

DRE voting systems can be considered as a good alternative for elections when the goal is to incorporate technology without incurring the risks associated with remote voting, such as having to interact via public networks or the internet. Some of the advantages are the speed of the overall voting process and the reliability and accuracy of the data compared with the human errors that can occur when the whole process is manual. The use of electronic kiosk voting helps bring down abstention rates by improving accessibility. However, after the review of some DRE experiences around the world, it can be stated that this approach is not free of vulnerabilities and the election might have many security gaps if proper controls are not in place and appropriate security measures are not taken on time.

The administrators of the voting processes have to evaluate the costs of the electronic system itself as well as of the implementation of the proper controls to create a safe and reliable process. The procedures have to be well defined and communicated to all the participants in the elections through brochures and advertisements in radio and TV. The cost of training the personnel is another item to be included in order to avoid any misunderstanding of the procedures during the election.

The selection of the vendor of the voting system is one of the most delicate activities for the administrators of the elections, and it is worthwhile to analyze carefully the different options and assess each one, if possible by running trials on a small percentage of the voters before it deciding on a solution.

Finally the implementation of a physical verification of the vote that can be used for manual audit is a key function to implement in a DRE voting system. Even if all the other security measures are in place it is good practice to have a backup of the votes in hard copy

to verify them and ensure that the DRE system is supported and in consequence trustworthy.

Bibliography

1. ANDERSON, R., *Security Engineering: A Guide to Building Dependable Distributed Systems.* Published by John Wiley & Sons, Inc., New York, NY, USA, 2001.
2. AUSTRALIAN CAPITAL TERRITORY (ACT), 2002. *The 2001 ACT Legislative Assembly Election. Electronic Voting and Counting System Review.* Produced by Publishing Services for the ACT Electoral Commission. Canberra, Australia, 2002.
3. BECHTOLD, S., 2003. *Governance in Namespaces.* Loyola of Los Angeles Law Review, 2003, 36:pp.1239-1320.
4. BENOIT, KENNETH, 2004. *Experience of Electronic Voting Overseas.* First Report of the Commission on Electronic Voting on the Secrecy, Accuracy, and Testing of the Chosen Electronic Voting System. Dublin: Government Publications Office, 2004. Appendix 2J: pp311-326.
5. BRUNAZO FILHO, A., 2001. *Criterios para Avaliação da Segurança do Voto Eletrônico.* Workshop em Seguranza de Sistemas Computacionais, 2001, UFSC, Florianópolis, SC., Brasil. [Online] Available: http://www.ppgia.pucpr.br/~maziero/pesquisa/wseg/2001/12.pdf
6. BRUNAZO FILHO, A., 2000. *Avaliação da Segurança da Urna Eletrônica Brasileira.* Article presented in: Simpósio de Segurança em Informática (SSI'2000), São José dos Campos, Brasil: Instituto Tecnológico da Aeronáutica, out/2000. [Online] Available: http://www.votoseguro.org/textos/SSI2000.htm
7. BRUNAZO FILHO, A., 2005. *El Voto Electrónico en Brasil – Las nuevas tecnologías en los procesos electorales.* Grupo Editorial Planeta S.A.I.C., Buenos Aires Argentina. Copyright 2005, CIPPEC.

8. CALTECH / MIT Voting Technology Project, 2001. *Voting What is What could be.* Published by the California Institute of Technology and the Massachusetts Institute of Technology Corporation, July 2001.

9. CAMARGO, VINICIUS J., 2005. *Security in E-voting.* Department of Computer and Systems Sciences of the Royal Institute of Technology. 2005. Stockholm, Sweden.

10. CARRACEDO GALLARDO, J. et al., 2002. *Votación electrónica basada en criptografía avanzada - Proyecto VOTESCRIPT.* II Congreso Iberoamericano de Telemática. CITA' 2002. Mérida (Venezuela). Septembre 2002.

11. CONNOLLY, N., 2004. *Issues with Electronic Voting.* Dublin Institute of Technology, School of Computing Research Paper (ITSM), DIT, Dublin 8, Ireland.

12. DEUTSCH, H. and BERGER, S., 2004. *Voting Systems Standards and Certifications.* Communications of the ACM, October 2004, 47(10): pp. 31-33.

13. EVANS, D. and PAUL, N., 2004. *Election Security: Perception and Reality.* IEEE Computer Society. IEEE Security & Privacy, Jan/Feb 2004, 2(1): pp.24-31.

14. FELDMAN, A.J., HALDERMAN, J.A. and FELTEN, E.W., 2007. *Security Analysis of the Diebold AccuVote-TS voting machine.* Proceedings of the USENIX/Accurate Electronic Voting Technology on USENIX/Accurate Electronic Voting Technology Workshop. Boston, Massachusette. 2007:pp.2.

15. FELTEN, E.W., RUBIN, A. and STUBBLEFIELD, A., 2004. *Analysis of Voting Data from the Recent Venezuela Referendum.* Johns Hopkins University and Princeton University, September 2004. [Online] Available: http://www.venezuela-referendum.com/

16. FISCHER, ERIC A., 2001. *Voting Technologies in the United Status: Overview and Issues for Congress.* Technical Report RL30733, Congressional Research Service, March 2001. Library of Congress. National Council for Science and the Environment. Washington, U.S.A. [Online] Available: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-1630:1

17. FISCHER, E., 2003. *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues.* Congressional Research Service (CRS) Report for Congress, Washington, D.C., USA, November 2003. The Library of Congress, Order Code: RL32139.

18.GONG, LI., 1993. *Increasing Availability and Security of an Authentication Service.* IEEE Journal on Selected Areas in Communications, 1993, 11(5):pp.657-662.

19.GUIMARÃES, M. F., SELL, C.A., TURCATO, R.P., ASSUITI, C.H., CUSTÓDIO, R.F. and SANTOS, R.A.P., 2001. *Proposta de um Sistema Electrônico de Auditoria aplicado à Urna Electrônica Brasileira.* Paper published by CERTI Foundation 2001. Florianópolis, SC, Brazil. 2001.

20.HELP AMERICA VOTE ACT (HAVA), 2002. *Help America Vote ACT of 2002.* H.R. 3295. Public Law 107-252. 107th Congress.

21.IKONOMOPOULOS, S., LAMBRINOUDAKIS, C., GRITZALIS, D., KOKOLAKIS, S. and VASSILIOU, K., 2002. *Functional Requirements for a Secure Electronic Voting System.* Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives, 2002: pp.507-520.

22.INTERNET POLICY INSTITUTE (IPI), 2001. *Report of the National Workshop on Internet Voting: Issues and Research Agenda.* Washington, USA, March 2001.

23.JONES, DOUGLAS W., 2001. *Evaluating Voting Technology.* Testimony before the United States Civil Rights Commission. Tallahasse, Florida, USA, January, 2001. [Online] Available: http://0-www.cs.uiowa.edu.innopac.up.ac.za:80/~jones/voting/

24.KARLOF, C., SASTRY, N. and WAGNER, D., 2005. *Cryptographic Voting Protocols: A System Perspective.* Proceedings of the 14th USENIX Security Symposium. August 2005. [Online] Available: http://www.cs.berkeley.edu/~nks/papers/cryptovoting-usenix05.pdf

25.KOFLER, R., KRIMMER, R. and PROSSER, A., 2003. *Electronic Voting: Algorithmic and Implementation Issues.* Proceedings of the 36th Hawaii International Conference on System Sciences. 2003. Publication date: 6-9 Jan. 2003:pp.7.

26.KOHNO, T., STUBBLEFIELD, A., RUBIN, A., and WALLACH, D., 2004. *Analysis of an Electronic Voting System.* Proceedings of the IEEE Symposium on Security and Privacy. May 2004:pp. 27-40.

27.LAUER, THOMAS. 2004. *The Risk of e-Voting.* Electronic Journal of e-Government (EJEG). 2004, 2(3):pp.177-186.

28.LINDSAY, D. 1993. *An overview of leading security issues*. In *information Security: An integrated Approach*, J. E. Ettinger, Ed. Chapman & Hall Ltd., London, UK:pp. 11-19.

29.McGALEY, M. and GIBSON, J. P., 2003. *Electronic Voting: A Safety Critical System.* Technical report NUIM-CS-TR2003-02. Department of Computer Science, National University of Ireland, Maynooth, Ireland. March, 2003. [Online] Available: http://www.evoting.cs.may.ie/Project/report.pdf

30.MERCURI, R., 2001. *Electronic Vote Tabulation Checks & Balances,* Ph.D. Dissertation, Philadelphia, PA, USA: School of Engineering and Applied Science, University of Pennsylvania. Published by the University of Pennsylvania, UMI Order Number: AAI3003665. [Online] Available: http://www.notablesoftware.com/Papers/thesdef.html

31.MERCURI, REBECCA, 2002. *A Better Ballot Box.* IEEE Spectrum, Oct. 2002, 39(10): pp.46-50.

32.NEUMANN, PETER G. 1993. *Security Criteria for Electronic Voting.* In Proceedings of the 16th National Computer Security Conference. Baltimore, Maryland, September 20-23, 1993: pp.478-482.

33.OLIVEIRA, E.L., 2001. *Voto Electrônico – Processo Eleitoral Brasileiro.* Informática Pública (IP): Belo Horizonte: Empresa de Informática e Informacao do Municipio de Belo Horizonte, 2001, 3(1):pp.17-28. [Online] Available: http://www.ip.pbh.gov.br/ANO3_N1_PDF/ip0301oliveira.pdf

34.ORGANIZATION for SECURITY and COOPERATION in EUROPE (OSCE) and OFFICE for DEMOCRATIC INSTITUTIONS and HUMAN RIGHTS (ODIHR). (2006)[1]. *Expert Visit on New Voting Technologies.* Technical Report. Kingdom of Belgium. 8 October, 2006.

35.ORGANIZATION for SECURITY and COOPERATION in EUROPE (OSCE) and OFFICE for DEMOCRATIC INSTITUTIONS and HUMAN RIGHTS (ODIHR). (2006)[2]. *The Netherlands Parliamentary Elections.* Technical Report. 22 November, 2006.

36.PEZZUOL J.R., CARVALHO, L. and COELHO, J., 2001. *Data Encription in an Electronic Ballot Box. 14th Symposium on Integrated Circuits and Systems Design. SBCCI* . Pirenopolis, Brasil. September 10-15, 2001:pp.156-160.

37.POSNER, TOMER, 2006. *Application of Lean Management Principles to Election Systems.* M.S. thesis, Dept. of Mechanical Engineer, MIT, Cambridge, MA, Institute of Technology. 2006. Cambridge, MA: Caltech-MIT Voting Technology Project VTP, Working Paper #42 (February). [Online] Available: http://www.vote.caltech.edu/theses/tomer-thesis_12-05.pdf

38.PRATCHETT, LAWRENCE, 2002. *The Implementation of electronic voting in the UK.* De Montfort University. Published by LGA Publications, the Local Government Association, Local Government House, London SW1P3HZ, May 2002.

39.REYNOLDS, ANDREW and STEENBERGEN, MARCO, 2006. *How the World Votes: The Political Consequences of Ballot Design, Innovation and Manipulation.* Electoral Studies. September, 2006, 25(3):pp.570-598.

40.REZENDE, PEDRO, 2003. *Electronic Voting Systems: Is Brazil ahead of its time?.* Prepared for the First Workshop on Voter-Verifiable Election Systems, Denver, Colorado, USA, July 28-29, 2003. [Online] Available: http://www.cic.unb.br/docentes/pedro/trabs/election.htm

41.RIAL, JUAN, 2004. *Posibilidades y límites del voto electrónico.* Elecciones. 2004, Vol. 3: pp. 81-108.

42.RIEBEEK, H., 2002. *Brazil holds all- electronic national election.* IEEE Spectrum, Nov. 2002, 39(11):pp.25-26.

43.RIERA, A. and BROWN, P., 2003. *Bringing Confidence to Electronic Voting.* Electronic Journal of e-Government (EJEG). 2003, 1(1):pp.43-50.

44.RUBIN, AVI., 2001. *Security Considerations for Remote Electronic Voting over the Internet.* ;login: The Magazine of Usenix & Sage. February, 2001, 26(1):pp. 20-28.

45.RUTTLEDGE, L. 2002. *Voting Systems in the United States: An Examination of Histories, Degrees of use and Performance Characteristics.* Presented to the Interdisciplinary Studies Program in partial fulfillment of the requirement for the degree of Master of Science, University of Oregon. June 2002.

46.SALTMAN, ROY G., 1988. *Accuracy, Integrity and Security in Computerized Vote-Tallying.* U.S. Department of Commerce, National Bureau of Standards Special Publication 500-158. August 1988.

47.SZOR, PETER, 2005. *The Art of Computer Virus Research and Defense.* Addison Wesley for Symantec Press. February 2005.

48.TAYLOR, JONATHAN, 2005. *Too many ties? An empirical analysis of the Venezuelan recall referendum counts.* Department of Statistics, Stanford University, Stanford. November 7, 2005.

49.TUESTA SOLDEVILLA, F., 2004. *El Voto Electrónico.* Elecciones. Lima: ONPE. July 2004, 3(3):pp. 55-80.

50.UNICAMP, 2002. *Avaliação do Sistema Informatizado de Eleiçoes (Urna Eletrônica).* Technical Report from the Universidad de Campinas. Contrato TSE nº 54/2001, Serviços, Brasília, DF, BRASIL, 05/2002. TSE-FUN. May, 2002. [Online] Available: http://www.tre-sp.gov.br/urna/rel_final.pdf

51.VOLKAMER, M. and VOGT, R., 2006. *New Generation of Voting Machines in Germany. The Hamburg Way to Verify Correctness.* International Association for Voting Systems Sciences. 2006. German Research Center for Artificial Intelligence (DFKI GmbH), Stuhlsatzenhausweg 3, 66123 Saarbrücken, Germany [Online]. Available: http:// fee.iavoss.org/2006/papers/fee-2006-iavoss-New-Generation-of-Voting-Machines-in-Germany.pdf

52.VOLLAN, K., 2005. *Observing Electronic Voting.* Norwegian Institute for Human Rights, University of Oslo. NORDEM Report No. 15/2005. [Online] Available: http://www.humanrights.uio.no/forskning/publ/publikasjonsliste.html

53.de VUYST, B. and FAIRCHILD, A., 2005. *Experimenting with Electronic Voting Registration: The Case of Belgium*. The Electronic Journal of e-Government, 3(2):pp. 87-90. [Online] Available: www.ejeg.com

54.WEISS, A. 2001. *Click to Vote.* Journal Networker from the ACM Digital Library. 5(1):pp.18-24.

55.XENAKIS, ALEXANDROS and MACINTOSH, ANN, 2005. *Procedural Security and Social Acceptance in E-voting. System Sciences, 2005, HICSS'05.* Proceedings of the 38th Annual Hawaii International Conference on System Sciences. Jan. 2005.

Direct Recording Electronic (DRE) Voting Project Development

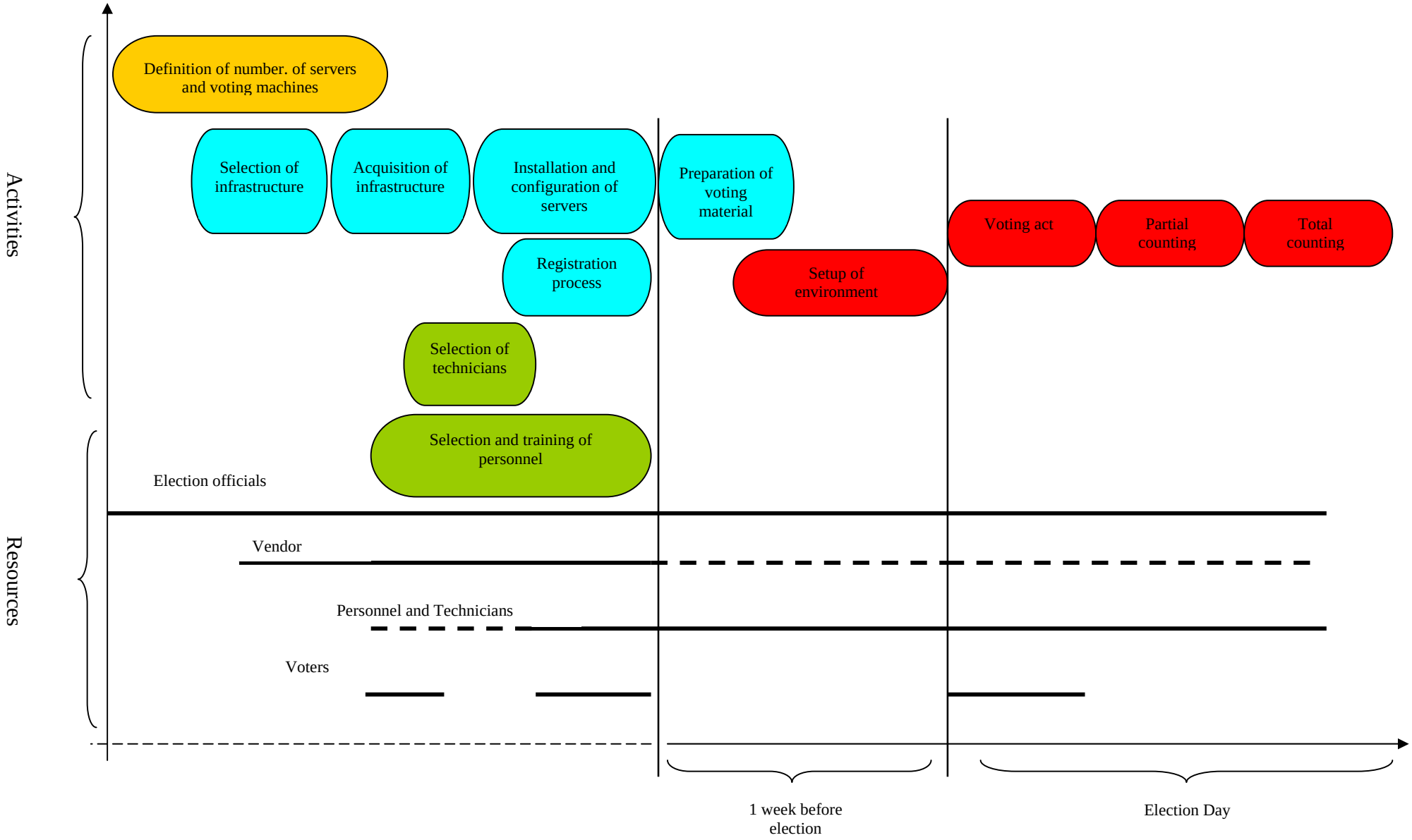

Figure 2