



Robert Krimmer, Rüdiger Grimm (Eds.)

Electronic Voting 2008 (EVOTE08)

**3rd International Conference
Co-organized by
Council of Europe, Gesellschaft für Informatik
and E-Voting.CC**

**August 6th-9th, 2008
in Castle Hofen, Bregenz, Austria**

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Proceedings

Series of the Gesellschaft für Informatik (GI)

Volume P-131

ISBN 978-3-88579-225-3

ISSN 1617-5468

Volume Editors

Mag. Robert Krimmer

Competence Center for Electronic Voting and Participation

E-Voting.CC gGmbH

Pyrkergergasse 33/1/2, A-1190 Vienna, Austria

Email: r.krimmer@e-voting.cc

Prof. Dr. Rüdiger Grimm

Universität Koblenz-Landau

Institut für Wirtschafts- und Verwaltungsinformatik

Universitätsstraße 1, D-56016 Koblenz, Germany.

Email: grimm@uni-koblenz.de

Series Editorial Board

Heinrich C. Mayr, Universität Klagenfurt, Austria (Chairman, mayr@ifit.uni-klu.ac.at)

Jörg Becker, Universität Münster, Germany

Hinrich Bonin, Leuphana-Universität Lüneburg, Germany

Dieter Fellner, Technische Universität Darmstadt, Germany

Ulrich Flegel, SAP Research, Germany

Johann-Christoph Freytag, Humboldt-Universität Berlin, Germany

Ulrich Furbach, Universität Koblenz, Germany

Michael Koch, TU München, Germany

Axel Lehmann, Universität der Bundeswehr München, Germany

Peter Liggesmeyer, TU Kaiserslautern und Fraunhofer IESE, Germany

Ernst W. Mayr, Technische Universität München, Germany

Heinrich Müller, Universität Dortmund, Germany

Sigrid Schubert, Universität Siegen, Germany

Martin Warnke, Leuphana-Universität Lüneburg, Germany

Dissertations

Dorothea Wagner, Universität Karlsruhe, Germany

Seminars

Reinhard Wilhelm, Universität des Saarlandes, Germany

Thematics

Andreas Oberweis, Universität Karlsruhe (TH)

© Gesellschaft für Informatik, Bonn 2008

printed by Köllen Druck+Verlag GmbH, Bonn

Gedruckt mit Unterstützung des Bundesministeriums für Wissenschaft und Forschung in Wien.

Preface

For the third time Castle Hofen is the meeting place to discuss the current state of the art in electronic voting around the world for academia, administration and vendors in the field. All of these benefit from the high level of interdisciplinarity and interest on all sides.

The past two years have been like a rollercoaster for electronic voting – on one hand there are success stories like legally binding internet elections – on the other hand major set backs as the decision to go back to paper and pencil for elections after years of e-voting experiences.

These experiences show the need for exchange of information and knowledge which has always been an aim of this conference. In the past six years, attendants from over 30 countries have used this opportunity which makes the conference a fixed point in the schedule of e-voting experts from all over the world.

On our call for papers we received over 30 submissions of which we had to select the 17 best for presentation. This was done in a double-blind-review process, that wouldn't have been possible without the tremendous effort, which the programme committee members and the additional reviewers put in the process.

Special thanks go to the Council of Europe and the working group ECOM – E-Commerce, E-Government and Security of the Gesellschaft for Informatik for their support in organizing this conference.

Further thanks go again to the Gesellschaft for Informatik and the Lecture Notes in Informatics editorial board under Prof. Mayr and Jürgen Kuck from Köllen Publishers who made it possible to print the workshop proceedings in such a perfect manner. We are also indebted to the Austrian Ministries for Science and Research (BWF), for Interior (BMI), the Ministry for European and International Affairs (BMeiA) and the Regional Government of Vorarlberg for their continued support.

Without the help of the programme committee, who were always available with their advice, the conference would not have reached the status it has today.

Finally we would like to thank Terry Davis, general secretary of the Council of Europe and Jürgen Weiss, vice chairman of the Austrian Federal Council that the conference can take place under their auspices.

Vienna, Koblenz, August 2008

Robert Krimmer, Rüdiger Grimm

Co-Organizers



E-Voting.CC Competence Center for Electronic Voting and Participation



Council of Europe



Gesellschaft für Informatik
Working Group for E-Commerce, E-Government and Security

Introductory Words

New communication technologies have a tremendous potential for empowering people. Millions of people engage in all sorts of electronic transactions. They download information online or through their mobile telephones.

Democracy is part of this development. There have been many experiments with voting through the Internet, voting on computers in polling stations, and even voting by digital TV or mobile phone.

While experimenting with these forms of voting, some important new issues, in comparison to traditional voting, come up. How does one observe voting through a computer? Or counting such votes? How does one guarantee a transparent election when people vote on a machine? Security and legal aspects also play an important role in the voting process.


In 2004, the Committee of Ministers adopted a Recommendation on E-Voting, which is the first and so far the only existing international text setting standard for electronic voting. The application of this recommendation is reviewed every two years at a Council of Europe meeting to keep up with the rapid developments in the use of information technology. This conference is a part of the process; it is one of the few conferences that brings together governments and international organisations, academia and the business sector, in order to discuss their experiences with e-voting.

Right Hon Terry Davis

Secretary General of the Council of Europe

Supporters



Federal Ministry for
 European and International Affairs



Introductory Words: Today more Democracy means E-Voting

E-Voting gives us an important opportunity to obtain more democracy and more civil participation. Therefore, we have to welcome every consideration and all possible instruments of electronic voting in Austria—for elections, for binding or non-binding consultative referendums as well as in petitions. We have to see e-voting as a chance to offer more services for citizens, to promote a plus in the voter turnout and also in the use of direct democracy.

As our behaviour and our possibilities in many aspects of our lives are changing, our election system should also evolve to meet the needs of contemporary society. For people becoming more and more mobile, it is also necessary for politics to keep up with recent trends and to give democracy new chances. All together, we could launch a sensible realisation. So it must be beyond doubt that the secrecy of ballot obtains first priority.

Nowadays, although everyone surely deals with his or her money very carefully, we trust the Internet enough to carry out banking transactions and shopping excursions online. In postal voting we trust in the post, and in E-Voting there are even more elaborate solutions that make the process secure and anonymous.

I take questions, doubts or even fears very seriously. Democracy contains dialogue and this has to be led. At the same time, however, I find it incomprehensible that in times of decreasing voter turnouts this additional possibility for citizens to make use of their right to vote, which means a possibility for more democracy, seems not to be recognised as such. In the view of growing disenchantment with politics, no one can shut their eyes.

E-Voting may – especially for young people – be an incentive to vote effectively. I think that particularly the young generation will make use of this new technology rather than of the previous instruments. Several countries have shown that the system is accepted. My aim in Austria is to show how E-Voting works. Therefore, I would like to offer this additional way of voting for the first time at the elections for the Austrian National Union of Students in 2009. The legal base is already established, the technical preparations well advanced. Now it is necessary to motivate students to smooth out potential concerns commonly and to make use of this new way of voting!

I wish the participants of the conference many new scientific insights and a pleasant day.

Dr. Johannes Hahn

Austrian Federal Minister for Science and Research

Partner

All presentations are available in Audio & Video including slides at <http://www.e-voting.cc/2008> with the help of



Introductory Words

The current working program of the Austrian Federal Government includes the introduction of postal voting as well as the examination of the use of electronic voting. The first part of this program, postal voting, was implemented in 2007 and has already been proven in practice during the regional elections in Lower Austria in March of this year. With regard to E-Voting, the different premises are currently being evaluated by the Ministry for the Interior and according to the head of the Austrian electoral management board, implementing E-Voting in Austria could be implemented on relatively short notice.

The federal minister for science and research has announced the use of E-Voting as an additional voting channel for the Austrian student-union's elections in 2009. This is possible because the legal basis was installed beforehand. As students have profound knowledge in the daily use of the Internet, they are a perfect target group for this pilot-test. The Austrian Federal Economic Chamber could also be a possible e-voting election as the legal basis exists as well.

In all these cases E-Voting does not mean the use of voting machines to facilitate the counting of the votes, it rather offers a further voting channel via the Internet, along with the familiar voting ballot at the voting station and postal voting. Although E-Voting is mainly a channel to vote at elections, it will also play an important role in referendums, plebiscites as well as petitions for referendums. The use of all these instruments will facilitate the citizen's participation in the political process. This may specially be the case where elections have non-binding character or with regard to elections with specific target groups. Experience with periodic surveys among employees of large enterprises has shown that anonymity can be secured without large efforts and e-voting also leads to high participation rates in these cases.

Bearing in mind the long time it took to introduce postal voting in Austria and the immense doubts it has raised with respect to secrecy of the vote and prevention of misuse, we can anticipate how much work still needs to be done before e-voting can finally be introduced. According to the latest polls, around sixty percent of the Austrian population are still sceptical of E-Voting. One part of these doubts is not nourished by knowledge of facts but by mere feeling. To create a field of trust around E-Voting we need to experience pilot tests and get used to the thought that electronic electronics are a part of the electoral process. Initially it is a challenge for scientists to which the "Competence Centre for Electronic Voting and Participation" commendably contributes by organizing this conference in Schloss Hofen every second year. Thereby international exchange of experience plays an important role – also experiences from abroad can convince. I therefore wish the EVOTE08 Conference and its participants in my home region Vorarlberg a comfortable location for fruitful scientific work.

Jürgen Weiss, Vice President of the Austrian Federal Council

Programme Committee

- Mike Alvarez, USA
- Frank Bannister, Ireland
- Jordi Barrat, Spain
- Josh Benaloh, USA
- Nadja Braun, Switzerland
- Thomas Buchsbaum, Austria
- Chantal Enguehard, France
- Simon French, UK
- Ruediger Grimm, Germany
- Thad Hall, USA
- Catsumi Imamura, Brasilia
- Norbert Kersting, South Africa
- Shin Dong Kim, Korea
- Laurence Monnoyer-Smith, France
- Hannu Nurmi, Finland
- Wolfgang Polasek, Austria
- Michael Remmert, France
- Josep Reniu, Spain
- David Rios, Spain
- Fabrizio Ruggeri, Italy
- Kazue Sako, Japan
- Berry Schoenmakers, Netherlands
- Robert Stein, Austria
- Dan Tokaji, USA
- Alexander Trechsel, Switzerland
- Melanie Volkamer, Germany
- Poorvi Vora, USA
- Dan Wallach, USA
- Gregor Wenda, Austria

Additional Reviewers

- Navarro Ángel Sánchez, Spain
- Joakim Astrom, Sweden
- Carol Boughton, Australia
- Danilo Bruschi, Italy
- Osvaldo Catsumi Imamura, Brasil
- David Canning, UK
- Letizia Caporusso, Italy
- Gerard Cervello, Spain
- Michel Chevallier, Switzerland
- Jeremy Clark, Canada
- Ishbel Duncan, UK
- Joao Falcao e Cunha, Portugal
- Joao Faria, Portugal
- Rosa M. Fernandez, Spain
- Stefanos Grizalis, Greece
- Tina Jukic, Slovenia
- Sokratis Katsikas, Greece
- Karl-Heinz Ladeur, Germany
- Costas Lambrinoudakis, Greece
- Ylle Madise, Estonia
- Tarvi Martens, Estonia
- Marc Mausch, Germany
- Rebecca Mercuri, USA
- Lilian Mitrou, Greece
- Peter G. Neumann, USA
- Goran Obradovic, Canada
- Anne-Marie Oostveen, Netherlands
- Ana Paiva, Portugal
- Emilia Perez Belleboni, Spain
- Joan Josep Piles, Spain
- Miguel Pimenta Monteiro, Portugal
- Judith Rossebo, Norway
- Emilia Rosti, Italy
- Jose Ruiz, Spain
- Christian Rupp, Austria
- Peter Ryan, UK
- Jose Luis Salazar, Spain
- Gorm Salomonsen, Denmark
- Guido Schryen, Germany
- Frederic Solop, USA
- Aleksandra Sowa, Germany
- Tim Storer, UK
- Kare Vollan, Norway
- Michel Warynski, Switzerland
- Alexandros Xenakis, UK

Content

Overview

Robert Krimmer, Rüdiger Grimm15

Session 1: E-Voting Experiences.....19

E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years

Leontine Loeber.....21

Improving the Transparency of Remote E-Voting: The Estonian Experience

Epp Maaten, Thad Hall.....31

Session 2: Empirical Findings.....45

Assessing the Impact of E-Voting Technologies on Electoral Outcomes: an Analysis of Buenos Aires' 2005 Congressional Election

Gabriel Katz, R. Michael Alvarez, Ernesto Calvo, Marcelo Escolar, Julia Pomares..47

Assessing Internet Voting as an Early Voting Reform in the United States

Alicia Kolar Prevost.....63

Session 3: Legal & Procedural Issues of E-Voting81

A Methodology for Assessing Procedural Security: A Case Study in E-Voting

Komminist Weldemariam, Adolfo Villaforita83

Secure Remote Voter Registration

Victor Morales-Rocha, Jordi Puiggali, Miguel Soriano95

Long-term Retention in E-Voting – Legal Requirements and Technical Implementation

Rotraud Gitter, Lucie Langer, Susanne Okunick, Zoi Opitz-Talidou109

Session 4: Comparison of E-Voting125

The E-Voting Readiness Index

Robert Krimmer, Ronald Schuster127

Malfunction or Misfits: Comparing Requirements, Inputs, and Public Confidence Outcomes of E-Voting in the U.S. and Europe

John Sebes, Gregory A. Miller137

Session 5: Verification of E-Voting.....151

Simple and Secure Electronic Voting with Prêt à Voter

David Lundin.....153

Improving the Farnel Voting Scheme

Roberto Araújo, Peter Y.A. Ryan.....169

| | |
|---|-----|
| Session 6: Certification of E-Voting | 183 |
| Development of a Formal IT Security Model for Remote Electronic Voting Systems | |
| <i>Melanie Volkamer, Rüdiger Grimm</i> | 185 |
| The Certification of E-Voting Mechanisms. Fighting against Opacity | |
| <i>Jordi Barrat i Esteve</i> | 197 |
| Session 7: Technological Issues of E-Voting | 207 |
| Code Voting with Linkable Group Signatures | |
| <i>Jörg Helbach, Jörg Schwenk, Sven Schäge</i> | 209 |
| CAPTCHA-based Code Voting | |
| <i>Rolf Oppliger, Jörg Schwenk, Christoph Löhr</i> | 223 |
| Session 8: Political Issues of E-Voting | 237 |
| E-Voting in Brazil – Reinforcing Institutions while Diminishing Citizenship | |
| <i>José Rodrigues Filho</i> | 239 |
| The Voting Processes in Digital Participative Budget: A Case Study | |
| <i>Cristiano Maciel, Gleison Pereira de Souza</i> | 249 |

Overview

Robert Krimmer¹, Rüdiger Grimm²

¹ E-Voting.CC

Competence Center for Electronic Voting and Participation
Pyrkergergasse 33/1/2, A-1190 Vienna, Austria
r.krimmer@e-voting.cc

² Universität Koblenz-Landau

Institute for Information Systems Research
Universitätsstraße 1, D-56016 Koblenz, Germany
grimm@uni-koblenz.de

Democracy and elections have more than 2,500 years of tradition. Technology has always influenced and shaped the ways elections were held. Today elections are the core element of democracy as a society's way to make decisions. Elections are the way to express how societies use technology and as new technologies emerged and evolved, elections changed accordingly. While there have been democratic structures in societies like India or Babylon, the birthplace of democracy is attributed to old Athens in 507 BC. From thereon similar structures of direct democracy, bound by face-to-face societies, also developed in several places around the world like in ancient Rome, with the Vikings or in the Cantons of Switzerland. The next level of democracy developed with the creation of nation-states in the late 18th century with the need for representatives. This form of indirect democracy spread from the United States and France around the globe to today's predominant role of democracy as a rule of government and was mainly limited by the nation's borders.

One can see this development as three comings of democracy:

1. The Face-to-Face Society
2. The Territorial Society
3. The Global Society.

With the latest emergence of technology we face a new challenge to spread the influence of one country around the globe to allow out-of-country voting and enable disenfranchised voters. This leads to multiple effects on the electoral process including e-campaigning, electronic supported candidate nominations, central voter registers, electronic eligibility checks in polling stations, to casting votes electronically and support for result or mandate calculation. This development is not uniform in all countries but can be observed everywhere to some extent.

It is the task of this conference series to enable the discourse amongst researchers, administrators and vendors so that understanding, cooperation and future research can emerge. As such this year's conference concentrates around eight core topics.

The first session deals with the different experiences made with E-Voting in the Netherlands and in Estonia. During the last two years the Dutch E-Voting system has been successfully challenged by activist groups which have led to a stop of electronic voting. The paper of *Leontine Loeber* gives an analysis of the situation. *Epp Maaten* and *Thad Hall* then will give an overview of the Estonian E-Voting experiences. Technically and politically the Estonian system has been used twice in practice. The authors suggest improvements which could be made with regard to enhancing the transparency of the voting system.

In the second session the coherence between electronic voting devices and voting outcome is discussed by *Gabriel Katz*, *Michael Alvarez*, *Ernesto Calvo*, *Marcelo Escolar* and *Julia Pomares*. Their study estimates the effect of different E-Voting technologies on the likelihood that citizens cast their vote for different parties for the National Congress and the Legislature of Buenos Aires and shows considerable effect. *Alicia Kolar Prevost* then presents her findings that programs designed to make voting easier have not succeeded in boosting turnout, and have even had the unintended consequence of exacerbating the demographic biases that already exist in the electorate. She will give an outlook to the implication this could have on future voting reforms.

Session three will deal with the paper by *Komminist Weldemariam* and *Adolfo Villafiorita*. They present a methodology for procedural security analysis in order to analyze and try to make elections more secure. Their approach is based on modelling the electoral procedures in the form of business process models. *Victor Morales-Rocha*, *Jordi Puiggali* and *Miguel Soriano* will show the importance of an accurate voter register and will present a scheme to improve this vital aspect. Further on recommendations on long-term retention in E-Voting will be given, applying the results of *Rotraud Gitter*, *Lucie Langer*, *Susanne Okunick* and *Zoi Opitz-Talidou* to a state-of-the-art E-Voting scheme. They will also review technical measures to meet the security requirements of long-term retention in E-Voting.

The fourth session deals with comparing the E-Voting experiences in different countries. First *Robert Krimmer* and *Ronald Schuster* present a methodology on how to measure the context of E-Voting in 31 countries. Then *E. John Sebes* and *Gregory A. Miller's* paper compares and analyses the E-Voting experiences in the US, which have been disenchanting, with the experiences in Europe where E-Voting is more and more adopted.

The topic of the fifth session are new and improved protocols. *David Lundin* presents the Prêt à Voter voting system. It is characterized through very high security properties. His working group aims to make the system truly applicable for elections with many races and various candidates by allowing the vote to be formed using a voting machine and by printing a minimalistic receipt. A concept is also presented to secure electronic voting systems. The Farnel voting scheme will be discussed by *Roberto Araújo* and *Peter Y. A. Ryan*. This concept will be improved through trustworthy talliers. Further they will present a novel way to initialize the Farnel box and a new scheme based on combining Farnel with Prêt-à-Voter style encoding of receipts.

Session six's discussion is concentrated around certification of E-Voting systems. *Melanie Volkamer* and *Rüdiger Grimm* present an approach of a formal trust model for remote electronic voting which is needed for an in depth analysis of E-Voting systems. *Jordi Barrit i Esteve* then discusses the different approaches on how to certify E-Voting machines in Europe as well as publication requirements.

Technological issues around code voting are dealt with in session seven, where *Jörg Helbach*, *Jörg Schwenk*, and *Sven Schäge* propose the application of group signatures for it. *Rolf Oppliger*, *Jörg Schwenk* and *Christoph Löhr* use a different approach to code voting with CAPTCHA.

The last session then gives room to political issues. Here *José Rodrigues Filho* goes about E-Voting in Brasil where he discusses the role of institutions. The voting process in participatory budgeting builds the final part of these proceedings where *Cristiano Maciel* and *Gleison Pereira de Souza* present a case study.

As can be seen from the contributions in this conference the discussion on E-Voting has not been decided yet. Moreover the research needs are highly interdisciplinary and discourse amongst the disciplines has to be an aim of any future research. As such we hope that Castle Hofen will give a good place for this in the future.

Session 1: E-Voting Experiences

E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years

Leontine Loeber

Dutch Electoral Council
Herengracht 21
2500 EA Den Haag
The Netherlands
Leontine_Loeber@xs4all.nl

Abstract: This document is a case study of a country in which e-voting used to be the general norm: The Netherlands. It gives a detailed description of the events in the last two years surrounding e-voting in the Netherlands. During this time, the security and reliability of the voting machines that were used were questioned successfully by an action group. This led to court cases, the withdrawal of the certification of these machines and eventually to a complete stop of their use. In the current situation, The Netherlands reverted back to paper ballot voting at least until a whole new system is designed, approved of by Parliament, built and implemented. In this document the author tries to explain why this happened at this particular time. The paper concludes with some ideas on what other countries that are considering the introduction of e-voting might learn from the Dutch experience.

1 Introduction

The last two years have been a rollercoaster for those involved with e-voting in the Netherlands. During the municipal elections of March 2006, nearly 99% of the voters cast their vote with the use of a voting machine. Both in the 2004 European Parliament elections and the national elections of November 2006, the voters living abroad could use the internet as a channel for voting. During the European Parliament elections of June 2009, both groups of voters will have to use the traditional methods of paper ballot and postal voting. It is still uncertain if e-voting will return shortly after those elections. Where the introduction of the use of voting machines in legislation in 1965 happened without any discussion and parliament was, as recently as 2005, asking for the introduction of internet voting for all voters, they now have an unprecedented interest in every little step that the Cabinet takes in regards to this subject.

What happened in the Netherlands to cause this complete turn away from e-voting and what are the prospects for the future? This paper will try to give more insight in the events that caused this landslide.

2 Voting machines

2.1 Legal Requirements for the Use of Voting Machines

The Dutch legislation on elections was set up in such a way that the election process that is used when voting with a paper ballot was also applicable to voting with voting machines. Only in the situations where voting with a machine significantly differs from voting with ballot papers, exceptions were made in lower legislation. Because the two processes existed alongside each other, there has never been, until now, a fundamental discussion concerning the question as to whether the introduction of e-voting should lead to a reconsideration of the way the fundamental principles of free, fair and secret elections are guaranteed.

The Dutch Elections Act was, as stated above, based on the principle of voting by paper ballot. It only contains three provisions regarding e-voting¹. These provisions state that electronic voting is possible and give some general demands for electronic means that are used in the voting process. The most important requirement in the act is a certifying procedure. The act also states that the means must guarantee the secrecy of the vote. All other regulations for voting machines were found in lower legislation in chapter J of the Decree of 19 October 1989, establishing new regulations for implementing the Elections Act and the ministerial Regulation for the approval on voting machines 1997.

To obtain an approval, a supplier had to submit a prototype of a machine to an independent certification agency that tested the machine against the requirements stated in the ministerial regulation. The test results were not made public. Based on the test report of the agency, the supplier could apply to the Minister of the Interior for an approval of the prototype. Once the prototype was approved, the supplier gave the agency ten machines of which the agency tested one against the prototype. If the tested machine was built according to the approved prototype, the agency would conclude that the machine could be approved. Again, for the final approval, the supplier had to apply to the Minister. The regulation had an appendix which contained the demands that a machine had to meet before it could be approved. These demands had not been updated since the regulation came into force in 1997. The regulation also contained a number of grounds based on which the Minister could decide to withdraw a given approval.

¹ The articles J 32 to J 34 in the Dutch Elections Act.

2.2 History of Voting Machines

The use of voting machines in the polling station has known a long tradition in the Netherlands. Already in the 1950's there was interest for the electronic voting machines used in the United States. In 1966 the first machines of this type, made by Automatic Voting Machine Corporation (AVM), were introduced in the Netherlands. In 1965 the Electoral Act was modified in the sense that the possibility of elections with the use of electronic means was opened. It was left up to the municipalities, who are under Dutch law responsible for organising elections, whether they wanted to use machines or not. The legal provisions called for an approval of voting machines by the Minister of the Interior after which municipalities either bought or rented the machines from the suppliers. This led to a situation where, in 2005, there were two suppliers who divided the market: Nedap and Sdu. Nedap built voting machines with panels that were big enough to contain all the candidates for an election². They were one of the first companies to build voting machines for the Netherlands and they supplied machines to approximately 90% of the municipalities. They are also active in other countries.

The Sdu machines are smaller and have a touch screen instead of buttons. The voting on these machines is done in two steps, whereby a voter first chooses a party and then, from the list of that party, a candidate. Sdu does not sell the machines to the municipalities, but rents them per election. Both types of machines are stand alone machines, although the Sdu machine does have a GPRS connection. This connection can only be used once the election is closed to send the results to the municipality.

2.3 Fraud during the Municipal Elections of 2006

In one municipality, there was a suspicion of fraud during the 2006 elections. A certain candidate obtained 181 preferential votes in one polling station. In all the other polling stations together he only obtained eleven votes. The fact that he was a polling worker and the person controlling the voting machine in the polling station where he got the large number of votes, led to an investigation. However, because the Nedap machine that was used does not have a paper trail, a manual recount of the votes was not possible. The District Attorney therefore asked all the voters to come in for a shadow election. The voters were asked to secretly cast their vote again. During this election the candidate only got a very small number of votes. Also, a number of voters testified that they felt that the suspect had told them too early that they had cast their vote. This gave the District Attorney enough reason to indict. The court in lower instance acquitted the suspect due to lack of evidence. However, when the District Attorney appealed, the appellate court did decide to convict. They found that the testimonies, combined with the results of the shadow election, gave enough cause to convict the suspect of election fraud. This case made people wonder if fraud was possible while using voting machines and if so if fraud had happened before. Was this person the first, or was he just caught because in his case it was so obvious?

² The Dutch system is based on a preferential vote for a candidate. In a general election, approximately 600 candidates compete.

2.4 Campaign by NGO we don't trust voting computers

In 2006 an action group by the name of we don't trust voting computers was founded³. This happened after the municipal elections of March 2006 during which the municipality of Amsterdam used voting machines for the first time. Most of the founders of the action group live in Amsterdam and were confronted with these machines. The leader of the group is Rop Gonggrijp, a well-known hacker and founder of the internet company xs4all. They started their campaign in the spring of 2006 with a series of requests based on the Freedom of information act. Through these requests they wanted to obtain as much information as possible concerning the voting machines and the decision making process surrounding the approvals. They also approached municipalities in an attempt to buy voting machines. This was successful; they managed to get a couple of Nedap machines. While they were doing this, the Cabinet fell and it became clear that there would be general elections in November.

The action group managed to decipher the operating system for the Nedap machine and wrote an overwrite program that would make it possible to commit fraud with the machines. This program would transfer a certain number of votes casts from one candidate to another. Because the machine did not have a paper trail, this fraud could go undetected if applied on a small scale. While examining the machine, the action group also detected that the radiation transmitted by the screen on the machine can be read from a distance⁴. This makes it possible to break the voter secrecy since in the Netherlands the name of a voter is read out loud in the polling station. The action group presented their finding during a press conference on October 4th [Gr06]. Although the fraud possibility is probably the biggest problem since it changes the outcome of the election, most attention went to the question of voter secrecy. This is caused by the fact that secret elections are not only guaranteed by the Dutch constitution, but also a requirement in the first protocol of the European Convention on Human Rights. The Dutch government is therefore obliged to do anything in their power to guarantee a secret election.

³ The Ngo has a website, www.wijvertrouwenstemcomputersniet.nl, which also contains information in English.

⁴ In computer science, this is known as the Tempest problem. The problem was detected in normal computers as early as the 1980's.

The Cabinet decided after the press conference to have the Secret Service test all types of machines in use for this Tempest problem. It turned out that the most common used Nedap machines did not radiate beyond 5 metres. The Sdu machines however could be 'read' from a distance of over 30 metres, due to their larger screen. This was such an uncontrollable situation that the Cabinet did not see any other option than to withdraw the approval of these machines, even though it was only three weeks before the election. The election did take place, with a crisis team supporting the 32 municipalities whose Sdu machines could not be used. Ten of them were able to use Nedap machines and in 22 municipalities, including Amsterdam, the voting was once again done with paper ballot and pencil. During the elections, which were observed by the Organisation for Security and Cooperation in Europe, there were no major problems with the voting machines [OD07]. The extra security measures that were taken seemed to function well, and although five machines were taken out of service because they might have been tampered with, tests revealed that they were all functioning normal.

After the elections preparations had to be made for the Provincial elections of March 2007. Sdu went to court to fight the withdrawal of their approval and managed to get a court order for a new test by the Secret Service. Although they got a number of attempts, they did not manage to deliver a machine with a radiation range under 5 metres. It was then decided not to renew their approval. For the elections, the same security measures as during the general elections were in place and everything went well.

2.5 Advisory Committees

The events surrounding the general elections led to an increased attention from Parliament. They asked the Minister to set up two independent advisory committees. The first looked into the past, especially to the decision making process concerning the use of voting machines. This committee published a report in April 2007 that stated mistakes had been made in the past. One of the major issues they detected was that the ministry did not have enough technical knowledge, which led to a situation where the suppliers not only controlled the market, but were also influential in the decision making process. Also, the responsibility for the elections and the electoral legislation had in the past shifted several times between different parts of the ministry. This caused a shattered knowledge of the system and its origins. Just before the elections of November 2006, it was not clear which division was responsible for what, which led to an inability to respond quickly to the problems that arose due to the criticism on e-voting. Furthermore, the committee concluded that the embedding of the voting machines within the legal framework was very weak. The lack of technical knowledge had caused a certification process in which the security of the machine was not tested properly. Therefore, they recommended an update of the regulation concerning the certification of the voting machines [He07].

The second committee was asked to give recommendations regarding the electoral process in general and on new ways of e-voting in particular. They published their report 'Voting with Confidence' on September 27th of 2007. One of the recommendations was that the Minister of the Interior should get more responsibilities in the electoral process. This would mean that the current legal position of the municipalities in the process would be changed. Another recommendation concerned a new way of using technology in the voting process. In light of the problems that arose because of the lack of a paper trail with the old machines, they recommended a new system. This system would consist of a voter printer and a vote counter machine. The printer should basically function like a pencil; the voter selects a party and then a candidate, after which the printer would print this selection. The printer does not store the votes. The voter takes the print and puts it in a ballot box. At the end of the day, the votes are counted with the vote counter, which is a scanner [Ka07]. The main advantage of this system over the traditional paper ballot voting is that it prevents voters from casting unintentional invalid votes. It also makes it possible to adapt the system for blind people, for example through the adding of a voice recorder. Last, it speeds up the counting process. Compared to the current system of voting machine, the main advantage lies in the paper trail and the fact that the voter can check whether the printer printed the vote correctly before casting it. Therefore, the proposed system does not require a high level of trust in technology by the voter.

2.6 Aftermath

During the press conference in which the 'Voting with Confidence' report was presented, the State Secretary for the Interior announced that the 'Regulation for approval of voting machines 1997' would be withdrawn. The action group had already filed a court case against the approval of the Nedap machines given in March 2007. As a result of this procedure, on October 1st 2007, the District Court of Amsterdam decertified all Nedap voting machines that were in use in The Netherlands. Since the approval of the Sdu machines was already withdrawn, there were no more certified machines at that time. On October 21st 2007 the 'Regulation for approval of voting machines 1997' was actually withdrawn. Also, the Decree of 19 October 1989 was amended, taking out the provisions that gave the Minister the competence for making new regulations for the approval of voting machines. Therefore, it was also no longer possible to certify new machines. This means that until new e-voting mechanisms are developed and the rules concerning their use are entered into legislation, the current legislation only allows for voting by paper ballot. However, Nedap did file an appeal against the decertification order by the District Court. They also lodged a complaint with the Ministry of the Interior against the withdrawal of the regulation. The State Secretary has recently decided to uphold the withdrawal decision. It is expected that Nedap will also file an appeal in this case. Both cases are therefore still running, so the situation might change once again in the near future. Since it is uncertain when the ruling in these cases will come and what the outcome will be, municipalities, the ministry and the Electoral Council have started preparations to hold the first nation wide election with paper ballots in over 40 years.

3 Internet and Telephone Voting

3.1 Experiments

In 1999 a project was started to investigate possibilities for remote e-voting. This project was in first instance mainly meant for voters from abroad. The intention of the Minister at that time was however to also in time expand the possibility of remote e-voting to voters within the Netherlands. The voters from abroad were seen as an ideal test group for this type of e-voting. Since 1985 almost all Dutch citizens living abroad have been eligible to participate in elections. The main requirement for them is that, in contrast to voters living within the Netherlands, they have to register separately to become a voter. Before 2004 they could choose to vote by mail, by proxy, or in person in a polling station within the Netherlands. Approximately 25000 voters register per election to participate. The procedure for voting by mail was seen as problematic and time-consuming and not all the votes were received in time to count in the elections. Therefore, an experiment was held during the European Parliament elections in 2004 whereby voters from abroad could choose to vote via the internet or the telephone. During the registration process they had to apply for this. The experiment was held under special legislation, the Online Voting Experiment Act. The Internet voting was a success; the telephone experiment was only used by a very small number of voters. Because of these results, the government decided to abandon the telephone experiment, but to carry on with the internet voting. During the national elections in 2006 a new experiment was held with the internet voting. Again, this was a great success; out of the 34.305 registered voters from abroad 21.593 voters (63%) chose to vote via Internet in the registration period. During the elections, 19.815 voters (92%) did eventually cast their vote through the Internet. These voters were asked to fill in an online questionnaire on internet voting. 11.003 voters (65%) responded to the questionnaire. Out of these voters, 99% preferred internet voting over voting via mail. 94% wanted the government to implement internet voting permanently⁵.

3.2 Future

These figures and the positive experiences of the governments working with internet voting, led to the plan to implement internet voting for voters from abroad into the regular Election Act, since there was no reason to keep experimenting.

⁵ See also www.minbzk.nl/bzk2006uk/subjects/constitution-and/internet-elections

However, the controversy surrounding the voting machines also rubbed off on the discussion surrounding internet voting. If a certifying procedure was deemed necessary for the machines, then why not for the internet service that was used during the election process? This question was asked by Parliament in a discussion with the State Secretary for the Interior in November 2007. The Parliament adopted a motion stating that a certifying procedure should be installed for internet voting. In January 2008 the State Secretary announced that the instalment of such a procedure would cost a lot of time and money and that it was therefore not possible to allow voters from abroad to vote via the internet in the European Parliament elections of 2009. Just before this announcement, the action group filed several Freedom of Information requests concerning internet voting. Now that the voting machines are out of the way, at least for the moment, it looks like the future of internet voting is going to be the next topic of debate in the discussion surrounding Dutch Elections. It is therefore still very uncertain if internet voting will in the future become a permanent option. The demand for nation-wide internet elections that Parliament still made in 2005 has not returned on the agenda and probably will not for a long time.

4 And now?

On the 30th of January 2008 the Parliament debated the proposed new system with the Minister. Several of the parliamentary fractions called for a very thorough approach and made it clear that they would rather vote with paper ballots a bit longer than to rush into new ways of electronic voting. The State Secretary decided to set up a technical advisory committee to examine the feasibility of the new system and to set up guidelines for the technical testing of the vote printer en counter. The results and recommendations of this committee are not known at this moment. They will report to the Minister shortly, as she had promised Parliament that Cabinet will decide on the future of this system before May 1st. Since then, she has announced that this decision will be delayed until probably half May. Already it has been made clear that the 2009 elections for the European Parliament will be held with paper ballot voting. After all, even if the Cabinet and Parliament decide to implement the new system, it will not be possible to develop and test it in time for these elections. This means that currently the Dutch municipalities are in the process of preparing elections in the old fashioned way. For a large group of voters this will mean that they will have to vote with paper for the first time in their lives, even though they have been voting for 30 years. A lot of effort will have to go towards explaining to these voters how this works. What will happen after the European Parliament elections is still a big mystery, even for those involved in the decision making process at this time. The biggest question is whether it will be possible to design a new system for electronic voting that can withstand the fast changes in computer science and the pressure of anti e-voting group and at the same time be voter friendly, easy to use and not too costly.

5 Conclusions

The mere fact that the introduction of voting machines in the Netherlands did not lead to discussion and seemed to go rather smoothly did not ensure that this topic would not be controversial later on. On the contrary, because the introduction went so easy, maybe the political attention for the subject was not great enough, causing neglect and a lack of knowledge with both the Ministry and the Parliament. New developments in computer science and security issues were not linked to voting machines even though there was enough reason to do so. A note hereby however is that also computer scientists have only recently started to consider the subjects of trust, transparency and verifiability in relation to the use of computers in elections. The consequence was that only when the actions of an action group led to a major crisis on the subject, was it acknowledged that there might be a problem.

What can we learn from this? First of all, an important lesson is that the introduction of e-voting should be accompanied by intensive testing. If possible, in this procedure both supporters and critics of e-voting should be involved. Another valuable lesson is that once e-voting is introduced government can not step back and let the market and suppliers take over. Close supervision is necessary to ensure the guarantees of fair, free and secret elections. It is also necessary to reconsider choices that have been made in the past to embed these basic principles in the electoral process. It is not correct to think that voting with a computer is almost the same as voting with a pencil and that the same rules can apply. Issues of transparency, voter secrecy and verifiability will have to be guaranteed, no matter which system you use. But the manner in which these fundamental demands are guaranteed in the process will have to differ. This means that when a change to e-voting is being considered, this has to involve a complete review of the voting process and most likely, an adaptation of certain rules and procedures. This prevents problems later on that might lead to the decline of trust in the system.

A last lesson is that once trust in the voting system declines, it is hard to win this back. Without this support, the legitimacy of the chosen legislator will diminish. It is therefore important to realise that the fact that e-voting can work in one country does not automatically mean it is suitable for all countries. A lot depends on the general level of trust in government, but also the level of trust in the corporations that supply the machines use in the electoral process. If government or the corporations are seen as biased towards certain parties or candidates, the use of voting machines will most likely fuel suspicion of fraud within the elections. In the Netherlands, there is a trend of declining trust. This trend is not only visible in the case of e-voting, but also with other technical solutions. In a recent case, government wanted to introduce a chip card as a means for payment in the public transportation system. This card would replace the current paper payment method. A lot of people feared that this could compromise the privacy of the traveller, especially after some experts proved it was possible to hack the card and read its contents. The further introduction of the card has once more become a topic of debate. Even trust in government in general seems to be declining. In the autumn of 2001, 70% of the voters expressed trust in political government. In the spring of 2004, this number had fallen to only 39% [AI05]. It is therefore not quite unexplainable that the controversy surrounding e-voting only started very recently.

Finally, it is important to realise that elections are not like other areas where computers are being used. E-Voting is often compared to electronic banking. There are, however, big differences between the two. First, with banking there is no need for public accountability of the system. It is sufficient if there is an independent auditor. With elections however, every voter should be able to verify that the system works correctly. If this is not possible, trust in elections and thereby trust in the legislator will decline. Another difference is that with electronic banking, a bank can afford a minor system problem once in a while. Mistakes caused by these problems can be corrected. They will also most likely be detected because millions of people can and will check their bank statements. With elections, there is no possibility for corrections. Even if detected, any minor glitch in the system can have a major impact on the question as to who will rule the country for the next four years. A few of these mistakes and the trust is gone, which can have disastrous effects. Therefore, there should be little room for experiments with new technology in elections. This does not have to mean that there is no future for e-voting. It does mean that new systems should not be used in legally binding elections without rigorous scrutiny and certification. And even when the system passes these requirements, it will always be necessary to re-evaluate the system and the certification of it on a regular basis.

References

- [AI05] Andeweg, R.B.; Irwin, G.A.: *Governance and Politics of the Netherlands*. Palgrave MacMillan, New York, 2005; pp. 228-229.
- [Gr06] Gonggrijp, R. et. al.: *Nedap/Groenendaal ES3B voting computer a security analysis*, October 6, 2006, to be found on www.wijvertrouwenstemcomputersniet.nl.
- [He07] Hermans, L. et. al.: *Voting machines, an orphaned subject*”, Report by the Advisory Commission regarding the decision making process for voting machines, April 17, 2007, only available in Dutch through the Ministry of the Interior and Kingdom Relations.
- [Ka07] Korthals Altes, F. et. al.: *Voting with confidence*”, Report by the Election Process Advisory Commission September 27, 2007, to be found on www.minbzk.nl.
- [OD07] OSCE/ODHIR: *Final Report on the 22 November 2006 Parliamentary Elections in The Netherlands*, March 12, 2007.

Improving the Transparency of Remote E-Voting: The Estonian Experience

Epp Maaten¹, Thad Hall²

¹National Electoral Committee
Lossi pl 1a, 15181 Tallinn, Estonia
epp.maaten@riigikogu.ee

²Institute of Public and International Affairs, University of Utah
260 South Central Campus Drive, Room 252
Salt Lake City, UT 84112, USA
thadhall@gmail.com

Abstract: Pilot projects in the area of remote e-voting have been carried out in several countries but the number of those projects in which the Internet-cast votes are legally binding remains small. Estonia, indeed, has been the first country to introduce Internet voting in which legitimate results were obtained at the national level. In local government elections in October 2005 and March 2007 parliamentary elections, Internet balloting was used without controversy. The number of I-voters was three times higher in 2007 compared to 2005.

Elections need to enjoy broad public confidence to be a legitimate, meaningful democratic exercise. Remote e-voting has twice been offered as an additional channel to Estonian voters, and in both cases the system's operation has been considered successful, both technically and politically. Technically, all systems and procedures functioned well and there were no security problems. Politically, the election results were legitimate and there were no proceedings initiated to challenge the Internet voting option.

This paper gives an overview about tools for voters that reduce the negative effects of remote e-voting and improve confidence in the new voting system. A question will be proposed how the observation of remote Internet voting can be put in practice in order to resolve the transparency problems. After two Internet-enabled elections, international observers and researchers have made many recommendations regarding how to improve the transparency of the electoral administration. The paper discusses whether the recommendations focusing on testing, auditing and certification of the voting system are applicable in the light of Estonian experiences.

1 Introduction

Internet voting (I-voting) represents new opportunities for improving the electoral process, but it also presents new challenges. In particular, it is critical that I-voting is introduced in a manner that safeguards the transparency of the elections, which is one of the fundamental principles for democratic elections⁶. I-voting, like other changes in the mechanisms used to capture votes—from paper ballots to voting machines—is a technology that changes the direct means of participation but not the nature of democracy itself. We should, therefore, seek to determine how we can integrate this new technological solution into the old traditions of voting.

The basic question in electoral administration no longer focuses on whether new technology developments are acceptable in electoral processes but rather on what kind of technology is suitable for a specific country, taking into account its political and social culture, level of technological infrastructure, and its electoral system. In the Estonian case, the preconditions were favourable for introducing the most ambitious change in the nature of voting – voting over Internet. It can be clearly said that the Public Key Infrastructure (PKI), the digital signature, and the existing process of authentication have served as absolute prerequisites for the creation of an efficient e-country. Internet voting is just part of the overall concept of e-governance in Estonia [Ma07]. Good communications infrastructure, voters' high e-readiness, the widespread use of the national ID card, which enables securely to authenticate on-line voter, and its relatively small population of 1.3 million complete the list why I-voting has been a success in Estonia.

The argument in this paper is that Estonia's current election system—which includes I-voting as a mechanism for voting—has a high level of legitimacy and transparency on three levels: political/legal legitimacy, voter transparency, and system transparency. At each level, the legitimacy can be measured through the actions of government, the actions of voters, or the actions of the electoral administrators in charge of elections. At each level, participants have been able to engage the system in the most transparent ways possible. The next sections detail the importance of transparency in elections, providing a theoretical framework for appreciating the importance of transparency in elections.

2 Transparency in Elections

Transparency is an internationally recognized principle for elections. The Administration and Cost of Elections (ACE) Project⁷ has developed a set of standards for elections, with transparency a critical component. As they note⁸:

⁶ See HW08a and HW08b for a summary of the literature on electoral transparency.

⁷ The eight entities who are ACE Partner Organizations are: Elections Canada, EISA, Instituto Federal Electoral (Mexico), IFES, International IDEA, United Nations Development Programme (UNDP), the United Nations Department of Economic and Social Affairs (UNDESA), and the United Nations Electoral Assistance Division.

⁸ <http://aceproject.org/ace-en/topics/ei/ei20> accessed February 22, 2008.

”Transparency makes institutional systems and the actions/decisions they take widely accessible and understood... Electoral administrators and election officers should be held accountable for decisions they make when administering elections; legislators should be held accountable for the content of the laws they pass and the level of funding allocated for elections...[It] builds understanding of the process, the difficulties encountered, and why electoral administrators and election officers make certain decisions. Transparency increases the credibility of the process and the legitimacy of the results. If the electoral process is free and fair, accurate, transparent and monitored, and if laws and regulations are enforced, it is difficult for participants and voters not to accept the election results or the legitimacy of the newly elected representatives.”

ACE is not the only organization that is concerned about transparency. The Organization for Security and Co-operation in Europe’s (OSCE) Office for Democratic Institutions and Human Rights (ODIHR) is also focused on transparency through their efforts related to election monitoring and observation. Like the ACE Project, the OSCE/ODIHR has a strong interest in ensuring that elections are run in a free and fair manner; in fact, this organization monitored the 2007 Estonian Parliamentary Elections [OSCE07].

The rationale for transparency in elections is simple; when elections are not transparent, individuals may engage in some sort of fraud or electoral manipulation that cannot be observed. In addition, even if nothing nefarious happens, a lack of transparency creates a situation where government officials cannot answer questions about the election in a way that satisfies either political parties or the citizenry. Erin Peterson notes that transparency has been closely tied to the idea of accountability and legitimacy in both the public and private sectors because it provides the public with important information about how institutions function⁹. Other scholars have found that transparency, especially in the vote counting process and the ability of observers to follow the election and watch key actions, are critical to confidence in the election process [Hy08]. In evaluating the legitimacy of an election system, transparency is a key attribute in the overall evaluation of the electoral process [Hy08].

In evaluating legitimacy, there are key features to examine based on international principles¹⁰. In order to evaluate the Estonian electoral system with Internet voting, it is important to determine whether the system has legal legitimacy among the public, the government, third-party election monitors, and the electoral administrators that implement election. It is also important that there are procedures in place that facilitate election observation and electoral transparency.

⁹ Pe07 cites the works of Be95; BO99; FS02; Mo98; PR96; and SL01 as leading scholars in the area of transparency.

¹⁰ See HW08a and HW08b for a review of this literature.

Our review of the Estonian case utilizes these international norms as a framework for understanding the way in which the Estonian government fosters transparency and legitimacy in the electoral process. We begin our evaluation by considering whether the political process that allowed for Internet voting is viewed as legitimate and was developed in a transparent political process (i.e., one in which I-voting was not adopted in a politically-motivated fashion to introduce bias into the system). Second, we are interested in examining whether the voters themselves view the Internet voting system as legitimate and fair. Third, we consider the administrative environment in which Internet voting is implemented and whether that system promotes transparency. Fourth, we consider how Internet voting is observed and audited. A transparent system should be one that promotes openness and is viewed as legitimate; by using international norms for election transparency as a framework, we can see how well Estonia's system fares.

3 The Legitimacy of the Estonian I-voting System

The legitimacy of I-voting in Estonia comes from the fact that the nation has relatively strong political support and an excellent legal framework that provides for Internet-related government services generally, including I-voting [DM02, DM04; MMV06]. The backbone to the entire system is the Digital Signature Act (DSA) of 2000. This Act provides for Estonians to be able to authenticate themselves during online transactions, including I-voting, and to use a digital signature. In 2002, Estonia began providing its citizenry with an identity card that had two individual's digital certificates embedded in it. When a user inserts the card into a standard smart card reader affixed to a computer and then connects to the websites enabling different services via the Internet, the individual can then enter their first personal identification number (PIN1) and the user is authenticated and can access an array of governmental and private services online. In order to give electronic signature the second certificate is activated by giving PIN2. According to Administrative Procedure Act, public sector is obliged to accept digitally signed documents and a digital signature has the equal legal value as a handwritten signature.

The DSA links closely with the set of laws enacted in 2002 that allow for I-voting in various electoral settings: the Local Communities Election Act, European Parliamentary Election Act, and the Riigikogu Election Act. After significant amendments in 2005, these laws detail the manner in which I-voting is to be administered. The statutes detail when voters can cast ballots over the Internet, the use of the DSA in voter authentication, the process for allowing I-voters to cancel their vote using an early-vote paper ballot, reconciling voter registries so that I-voters cannot cast a ballot on election day, and the ballot reconciliation process for I-votes on election night. The strong authentication requirement for I-voters i.e. the usage of ID card, is also for mitigating the risk of vote selling. Forwarding one's ID card will compromise a person's identity in all transactions not only in elections.

Electoral laws were sponsored and supported by the Prime Minister and the Minister of Justice and continue to be supported by the Parliament. In addition, the Estonian ministries have been supporters in I-voting and have championed its success in talks around the world. The most controversial issue of guaranteeing secrecy of remote I-voting by allowing people to vote repeatedly is also supported by the Estonian Supreme Court, which has ruled that repeated I-voting is constitutional because the technological benefits outweigh any deficiencies. Specifically, the court stated that “the infringement of the right to equality and of uniformity, which the possibility of electronic voters to change their votes for unlimited number of times can be regarded as amounting to, is not sufficiently intensive to outweigh the aims of increasing the participation in elections and introducing new technological solutions.” [Court05]. If these laws were no longer deemed legitimate by either the political parties or the public, the Parliament would obviously be in a position to change them but there has been no reason to do so. No election results have been challenged during the I-voting elections and no parties have officially questioned the transparency of the process in the political or legal setting.

One reason why the system is deemed to be transparent is that the laws governing I-voting ensure that the Internet is but one way that voters can cast ballots in Estonia. Voters can also vote in person during the early voting period on a paper ballot or they can vote on a paper ballot in person on Election Day. Internet voters can use the early voting period to ensure that their vote was secret. On the early voting period the election law allows an I-voter to cast multiple I-votes, with only the last vote counted and included in the reconciled election totals. In addition, if an I-voter casts a paper ballot during the early voting period, no I-vote is counted, only the paper ballot. By re-voting, the voter who was illegitimately influenced is able to cast a new vote once the influence is gone. Thus, an I-voter has multiple means of ensuring that their vote counted is a secret, un-coerced vote.

The legal framework for the Estonian I-voting system provides the system with legitimacy because the decision to move to I-voting was made in an open, deliberative process. The government carefully considered the issues associated with I-voting and ensured that there was an appropriate set of legal mechanisms in place to fulfil this expectation. The timing of I-voting, concomitant with early voting, allows an I-voter the opportunity to cast a secret, un-coerced ballot.

4 Voter Legitimacy: Options for Dealing with Negative Effects of I-Voting

As was noted previously, the improper influence of remote voters by others is a theoretical but potentially significant problem, although such threats are tolerated with vote-by-mail in numerous jurisdictions. As Alvarez and Hall have noted, the threats that exist with I-voting are similar to the threats that exist in almost all other modes of voting [AH04, AH08]. In order to reduce the potential threat of coercion or a problem with a perceived loss of privacy in remote I-voting, reversible voting during the early voting period is allowed under Estonian electoral law.

If we consider the experience of voters in the two I-voting experiences, we see that there is little evidence of coercion or concerns about privacy, based on the behaviour of voters. The number of I-voters who decided to go to the polling station in order to replace their I-vote with a paper ballot has decreased from 0.3% in 2005 to 0.1% in 2007 (see Table 1). Also, the percentage of repeated votes compared to the total number of I-votes diminished accordingly from 3.8% to 2.5%. The small percentages of repeated votes as well as the significant increase of the total number of I-voters indicate that the confidence in the existing I-voting system has grown. These two statistics suggest that few voters have felt the need to use the various reversible voting mechanisms that exist to guard against coercion. However, it is valuable that the small percentage of voters who have used the system, for whatever reason, have had a system in place to allow them to change their vote and avoid this concern. Likewise, the reporting of these data by the Estonian government provides voters with confidence that their votes were reversed in the process and their replacement vote tabulated.

| | Local elections 2005 | Parliamentary elections 2007 |
|---|----------------------|------------------------------|
| Number of I-votes | 9 681 | 31 064 |
| Repeated I-votes | 364 | 789 |
| Number of I-voters | 9 317 | 30 275 |
| I-votes cancelled by paper ballot | 30 | 32 |
| I-votes counted | 9 287 | 30 243 |
| % of I-votes among total votes given | 1,9% | 5,4% |
| % of I-votes among total advance votes given | 7,2% | 17,6% |
| % of I-votes cast abroad (51 countries in 2007) | n.a | 2 % |

Table 1: Internet voting statistics of 2005 and 2007 elections [NEC2007].

In addition, we see a large growth in the percentage of voters who used the I-voting channel from 2005 to 2007. In its first use, 1.9% of voters used I-voting; in 2007, 5.4% used the system. In a survey of voters and non-voters in both elections, respondents who cast I-votes in 2005 reported having also I-voted in 2007. I-voters were very loyal to the technology, suggesting that their experience in 2005 convinced them of the system's effectiveness [TSB07]. By comparison, other voters were not loyal to their voting method; election day voters tended toward early voting and early voter to I-voting. In addition, there was some evidence that I-voting brought a small but potentially significant number of non-voters into the electoral process. This is important because studies in the United States have suggested that a lack of confidence in the electoral process can lead individuals to decide not to vote [AHL08]. Internet voting in Estonia seems to have the reverse effect, potentially drawing in some voters who previously did not participate in the electoral process. A survey of voters after the 2007 parliamentary elections found that 1 in 10 internet voters suggested that they might not have voted if the internet option had not been available [TSB07]. The contrast between America and Estonia can be seen here between the relatively low level of technology trust in the United States and the high I-government support in Estonia.

The Estonian government has also used simple methods to increase voter understanding of and confidence in the I-voting system in an attempt to overcome any concerns about the lack of transparency and complexity. In both elections in which I-voting has been used, prior to the voting period, the government allowed all individuals eligible to vote the opportunity to test out the I-voting system in order to encourage people to see how the system worked. This helped the voters detect any problems they might encounter before the real I-voting period started. In Estonia, the primary concerns among the country's election officials, outside observers, political parties, and citizens, relate to the cost and acquisition of the hardware and software needed to read an ID card on a personal computer, updating expired ID card certificates and the renewal of PIN codes needed for electronic use of the ID card. The government engaged in a nationwide pre-election information campaign to inform voters about these potential issues and to encourage voters to try the system before the voting period started. In 2007 elections, about 4,000 voters did test the system.

5 Transparent Election Administration

In addition to having voters test the system so that they would know how the electronic equipment worked during the voting period, there were also other issues about which the national election officials wanted to educate I-voters. Specifically, in order to raise the confidence of voters, they were informed that they should ensure that the file of the voting application had not been modified in transmission or intercepted by untrusted parties. This was done by explaining to voters how, once the live voting period had started for I-voting, they could verify the authenticity of the voting application. Before the start of the I-voting period for some operational systems, the election officials published information about the cryptographic hash functions that were used, and during voting period voters could examine the checksums.

As an additional element of transparency, the number of I-voters who had cast ballots was updated regularly on the I-voting website during the early voting period. This very simple process allowed the wider national audience, as well as the political parties, to know how many i-voters had voted and to determine if the trend in the number of i-voters casting ballots seemed reasonable. At the end people were also able to compare the number of I-voters with the number of I-votes counted. The transparency of the election process was not mere window-dressing on the part of either election officials or voters. One real example that illustrates that the importance of allowing voters and the political parties to monitor the I-voting should not be underestimated. As the i-voting system was closed at the end of the early voting period, the final number of I-voters disappeared from the I-voting website for a couple of minutes. This incident caused immediate and intense feedback from voters.

A high level of transparency is appealing because it provides the voters as much data as they need so that each voter is convinced that her vote has been correctly registered. One key question is to know how much information can be reflected back to the voter without creating other problems. For example, one possibility is to let the voter inspect the ballot as it is registered in the trusted part of an Internet voting system (analogous to checking the statement of account in Internet banking). The ballot can only be inspected, not modified [Sk06] and the possibility for inspection may give the voter even greater trust in the system.

This idea has been thoroughly discussed during the development process of the Estonian Internet voting system but the realization of it was postponed. Therefore, other methods were used in order to convince the voter. If the voter decided to replace the I-vote with a new one, he got a notification of an earlier recorded I-vote. A second option for verifying the correctness of electoral administration was offered on election day in the polling station of voter's residence, where the fact of an valid I-vote had to be reflected on the polling lists in order the prevent voting more than once.

The I-voting system actually provides I-voters with more assurance that their ballots were included in the final tabulation and were tallied accurately compared to the traditional paper ballot system. The I-voter has two mechanisms that could increase the confidence of voters. First, voters who use the I-voting mechanism know that there is no misinterpretation of their ballot by a third-party. They do not have to worry whether the polling place workers can read their writing on election night and properly count their ballot; by contrast, all I-votes were counted. Second, the voter can check acceptance of an electronic I-vote during the I-voting period or after the end of the advance poll as described earlier.

6 Transparency and Observation in Practice

In the case of Internet voting, observation is of particular importance for several reasons. First, the introduction of new technologies can influence public opinion with regard to the ability of the election process to produce honest, verifiable results. In Estonia the electoral administration enjoys broad confidence of the electorate. This confidence is reflected in the fact that, even with the implementation of this new voting mechanism, the interest of domestic observers in observing the Internet voting was quite modest in last elections. Second, the introduction of such a new technology can influence international opinion about Estonia. This interest is reflected in the high interest that international observers have had towards Estonian I-voting and their efforts to assess whether Estonian elections using I-voting are conducted in line with international standards for democratic elections, provide an opportunity to identify potential concerns, and enhance the integrity of the elections process not only for Estonian public opinion but internationally. Third, there are also theoretical concerns that, given the electronic nature of the voting, the system is inherently less transparent than is traditional precinct based balloting.

According to the Estonian electoral laws, all activities related to elections are public. Observers have access to the meetings of all election committees and can follow all electoral activities, including the voting process, counting and tabulation of results. Internet voting has been no different. All significant documents describing the I-voting system have been made available for all, including observers. In order to enhance the observers' knowledge about the system, political parties were invited to take part in a training course before each election in which I-voting was used. Besides political parties, auditors and other persons interested in the I-voting system also took part in the training. The training was followed by surveys of concrete procedures that were necessary for a set up of the I-voting system. Observers were invited also to a test of the counting process. However, few political parties exercised their opportunity to observe the I-voting procedures.

Throughout the I-voting observation period of one month, the main observation tool was the checking of the activities of electoral administrators against written documentation describing the necessary procedures. The key management function required extra attention, as the security and anonymity of I-votes was predicated on the encryption and decryption of votes. During counting event - the highlight of the election period - the management of the private key was demonstrated to observers. NEC mastered this key, and its members collegially could open the anonymous encrypted votes. The process of conducting the counting of ballots was all conducted with observers able to watch all ballot counting activities on large screens in the observation area. The process was fully narrated and observers were able to follow each step.

It is important that observers are deployed for a length of time necessary to allow meaningful observation. If some important stages influencing the correctness of final results have not been observed, the conclusions about the integrity of the system can not be made. In last elections of March 2007, I-voting procedures started several weeks before the elections day. Especially for casual foreign observers, the length of the observation period appeared to be a challenge. The OSCE did audit the 2007 elections and, in its report, it states that "election administration implemented the [Internet voting] system in a fully transparent manner, and appeared to take measures to safeguard the conduct of internet voting to the extent possible" [OSCE07].

The Estonian NEC has also been very supportive of analyses of its voting system by academic observers. In both 2005 and 2007, the NEC provided support to studies conducted by the Council of Europe that evaluated public confidence in the I-voting system. These two studies both found that there was a high level of public confidence in I-voting and provided an independent audit of public attitudes toward the I-voting system. Given the fact that transparency and confidence are not tangible but are attitudinal, these studies of public opinion in Estonia allowed the NEC and others involved in the elections to have additional knowledge that the I-voting system was effective and the procedures being used were acceptable to the public.

7 Validating the Voting Systems – Audit, Certification, Testing

The Estonian I-voting system was developed with the underlying principle being that all components of the system should be transparent for audit purposes. Procedures should be fully documented and critical procedures should be logged, audited, observed, and videotaped as they are conducted.

Specifically, during last elections, NEC has conducted audits on the source code and on the electoral procedures. A common requirement is that the source code of the voting system should be available for auditing. In Estonia, though, the code is not universally available but it can be audited if agreed to by the NEC. In order to rule out any manipulation by insiders, every election and audit by external auditing company had been ordered and it covered all of the technical and operational activities controlled by electoral committee. The audit was conducted by KPMG Baltics, which reviewed and monitored security sensitive aspects of the process continuously, such as updating the voters list, preparation of hardware and its installation, loading of election data, maintenance and renewal of election data and the process of counting the votes. The auditors' report about the 2007 Parliamentary election was released after all procedures, including the deletion of I-votes, were carried out. The report stated that the I-voting followed the rules described in the system's documentation and the integrity and confidentiality of the system were not endangered.

The I-voting system produces a wealth of system log information that can be used to monitor the work of the system thoroughly. In its different production functions, the I-voting system produces different logs on received, cancelled, and counted votes, also invalid and valid votes. The Audit Application enables to determine what happened to an I-vote given by a concrete person without revealing the voter's choice. These logs provide external auditors as well as observers with information that they can use to ensure that the system is working correctly.

The OSCE, in its report about the 2007 Parliamentary elections, recommended that, in addition to the audits of the process now conducted, all components of the system should be audited by an independent body in accordance with publicly available specifications, with all reports made public [OSCE07]. NEC has not published the audit reports referring to the contracts and given the consideration that publishing reports could make the system more vulnerable to attacks. In the future, the NEC should consider asking its auditors to produce both an internal audit report, intended for the NEC, and a report that can be made public, with certain information redacted.

In order to validate the electronic voting system, certification procedures could be established and other measures like testing and audits of different aspects should be taken. The Council of Europe has stated that it is necessary to promote the development of certification and accreditation schemes for e-voting systems in the member countries [CoE06]. A certification process will be very useful if there are a number of e-voting systems available. It might become very hard for any electoral authority to make sure a particular product is ready to be used, will operate correctly and will produce accurate, reliable results [Rec04].

Currently there is no domestic or international body that is ready to certify Estonian I-voting system. Estonia instead uses a system similar to that used in other countries, where a third-party audits the source code to ensure that the system operates as is specified. In addition to the audits discussed previously, system testing was also done on separate operation and functional components of the system in order to test the functionality and accuracy. Two weeks prior to the advance electronic voting period, the I-voting system was also tested by the public and contracted testers.

8 Conclusions

It is critical all election systems have fundamental safeguards for transparency in place because without them the public confidence necessary for legitimating elections cannot be ensured. Tools like observation, independent auditing, and system testing are suitable for assessing the actions of the electoral administrators. In addition, third party evaluations of public confidence in the process also serve to enhance our understanding about whether the public views the election with confidence and sees that the election administration was in fact transparent. These tools might not be easily accessible or of interest to the average person; however, it should be simple for those individuals who do want to participate.

The two Estonian I-voting experiences seem to prove that it is possible to solve the legal as well technological obstacles inherent for remote e-voting concerning the transparency of elections. The high degree of public confidence enjoyed by electoral administrators in last elections, as well as the fact that the legitimacy of the whole election process—including Internet voting—has not been questioned, strongly suggest that the elections have been carried out transparently. Moreover, the electoral administrators have provided procedural mechanisms that educate voters and the political parties about the process and allow each, through simple activities, to be an active participant in the election observation and evaluation process. The test voting process, the ability to re-vote, and the ability to determine that their vote was accepted all provide voters with a chance to evaluate and check the I-voting system.

In order to increase public awareness about IT security and teach people how to use the Internet safely, new initiatives, like public-private project “Computer Security 2009” and state’s Information Society Awareness Program have been started. The aim at further increasing the use of e-services with due attention to security issues and application of ID-card, will most probably raise the popularity of Internet voting in the future. Based on researches success of Internet voting is clearly linked to the overall ICT awareness [TSB07]. Next elections using I-voting as an option will take place in the year 2009.

ICT has already dramatically changed the way elections are conducted in many countries, and it must be accepted that this process will go on and affect more and more countries. Even if Estonia is still the only one practicing Internet voting countrywide on legally binding elections, it could be a matter of time when people in other countries also overcome their native conservativeness against new solutions. To get experiences, the first step has to be taken and trust can be built only based on experiences. Insecurity is the part of every IT system, but in order to reduce the insecurity a lot can be done. And learning from experience is highly valuable in making the I-voting transparent and confident

References

- [AHL08] Alvarez, R., Hall, T., Llewellyn, M.: Are Americans Confident Their Ballots Are Counted? *Journal of Politics* 2008 [Forthcoming].
- [AH04] Alvarez, R., Hall, T.: *Point, Click, and Vote: The Future of Internet Voting*. Washington, DC. Brookings Press 2004.
- [AH08] Alvarez, R., Hall, T.: *Electronic Elections: The Perils and Promise of Digital Democracy*. Princeton University Press 2008.
- [Be95] Bell, A.: Constitutional Aspects. *The International and Comparative Law Quarterly*. Vol. 44, No. 3. (Jul., 1995), pp. 700-705.
- [BO99] Bloomfield, R. and M. O'Hara.: *Market Transparency: Who Wins and Who Loses?* *The Review of Financial Studies*. Vol. 12, No. 1. (Spring, 1999), pp. 5-35.
- [CoE06] Remmert, M.: *E-Voting in Europe: Standards, policy practice*, 2006.
- [Court05] Decision of the Supreme Court of Estonia of Electronic Voting, <http://www.nc.ee/klr/lahendid/tekst/RK/3-4-1-13-05.html>.
- [DM02] Drechsler, W., Madise, Ü.: "E-Voting in Estonia." *Trames*, 2002, 6(56/51), 3, 234-244.
- [DM04] Drechsler, W., Madise, Ü.: *Electronic Voting in Estonia*. In: N. Kersting and H. Baldersheim (eds.) *Electronic Voting and Democracy. A Comparative Analysis*. Basingstoke: Palgrave Macmillan 2004, pp. 97-108.
- [FS02] Faust, J., Svensson, E.O.: *The Equilibrium Degree of Transparency and Control in Monetary Policy*. *Journal of Money, Credit and Banking*, 2002, vol. 34, No. 2., pp. 520-539.
- [HW08a] Hall, T., Wang, T.: *Show Me the ID: International Norms and Fairness in Election Reforms*. *Public Integrity*, 2008, 10, 2: pp. 97-111.
- [HW08b] Hall, T., Wang, T.: *Normative Principles for Evaluating Election Fraud*. In Alvarez, R.M. Hall, T.E. and Hyde, S. (eds): *Understanding, Detecting, and Preventing Election Fraud: Domestic and International Perspectives*. Washington, D.C., Brookings Institution Press 2008.
- [Hy08] Hyde, S.: *How International Election Observers Detect and Deter Fraud*. In Alvarez, R.M. Hall, T.E. and Hyde, S. (eds): *Understanding, Detecting, and Preventing Election Fraud: Domestic and International Perspectives*. Washington, D.C., Brookings Institution Press 2008.
- [Ma07] Maaten, E.: *Practicing Internet Voting in Estonia*. In *Baltic IT&T Review 2007*, <http://www.ebaltics.com/00704985?PHPSESSID=f5849c543bdc4a1b621bd4c73eb62fc0>
- [MMV06] Maaten, E., Madise, Ü., Vinkel, P.: *Internet Voting at the Elections of Local Government Councils in October 2005*. Report on Internet Voting to the National Election Committee, Tallinn 2006, <http://www.vvk.ee/english/report2006.pdf>.

- [Mo98] Moncrieffe, J.M.: Reconceptualizing Political Accountability. *International Political Science Review / Revue internationale de science politique* 1998, Vol. 19, No. 4. (Oct.), pp. 387-406.
- [NEC07] National Electoral Committee of Estonia: Parliamentary Elections 2007 – Statistics of e-voting, http://www.vvk.ee/english/ivoting_stat_eng.pdf.
- [OSCE07] OSCE/ODIHR Election Assessment Mission Report, Republic of Estonia, Parliamentary Elections, 4 March 2007, <http://194.8.63.155/item/25385.html>.
- [PR96] Pagano, M., A. Roell.: Transparency and Liquidity: A Comparison of Auction and Dealer Markets with Informed Trading. *The Journal of Finance*, 1996, Vol. 51, No. 2, pp. 579-611.
- [Pe07] Peterson, E.: Transparency In United States Election Law. Thesis Manuscript, University of Utah.
- [Rec04] Recommendation No. R (2004) 11 of the Committee of Ministers to members states on E-Voting, [http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/01_Recommendation/Rec\(2004\)11_Eng_Evoting_and_Expl_Memo.pdf](http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/01_Recommendation/Rec(2004)11_Eng_Evoting_and_Expl_Memo.pdf).
- [SHN06] Skagestein, G., Vegard Haug, A.V., Nødtvedt, E., Rossebø, J.: How to create trust in electronic voting over an untrusted platform. In: Krimmer, R. (Ed.) *Electronic Voting 2006*, Bonn: Gesellschaft für Informatik 2006, pp. 107-116.
- [SL01] Stirton, L., Lodge, M.: Transparency Mechanisms: Building Publicness into Public Services. *Journal of Law and Society* 2001, Vol. 28, No. 4., pp. 471-489.
- [Tr06] Perspectives e-voting. Presentation made at the E-Voting Conference in Tallinn, October 2006, http://www.ega.ee/files/27.10.06_Michael_Remmert_e-haaletamise%20konv.pdf
- [TSB07] Trechsel, A.H., Schwerdt, G., Breuer, F., Alvarez, M., Hall, T.: Report for Council of Europe - Internet voting in the March 2007 Parliamentary Elections in Estonia. http://www.coe.int/t/e/integrated_projects/democracy/EVoting/Report_Evoting_Estonia_for_the_CoE_2007.doc.

Session 2: Empirical Findings of E-Voting

Assessing the Impact of E-Voting Technologies on Electoral Outcomes: an Analysis of Buenos Aires' 2005 Congressional Election

Gabriel Katz^{1*}, R. Michael Alvarez¹, Ernesto Calvo², Marcelo Escolar³, Julia Pomares⁴

¹California Institute of Technology

²University of Houston

³Universidad de Buenos Aires

⁴London School of Economics

*corresponding author: gabriel@hss.caltech.edu

Abstract: Using data from an e-voting experiment conducted in the 2005 Congressional Election in Argentina, we estimate the effect of different e-voting technologies on the likelihood that citizens cast their vote for different parties for the National Congress and the Legislature of Buenos Aires. Our results indicate that voters are extremely receptive to the information cues provided by the different voting technologies and associated ballot designs, and that particular voting devices have a significant impact on voter choice, systematically favouring some parties to the detriment of others. We conclude that the choice of alternative electronic voting devices might have considerable effect on electoral outcomes in multi-party electoral systems.

1 Introduction

An increasing number of countries around the world have adopted electronic voting systems in national and local elections since the 1990s, and many others are conducting pilot projects [AH08]. While the academic literature has focused mainly on the reliability and accuracy of different electronic voting technologies [AH08], [St04], [AS05], only a few empirical studies have directly examined the effect of different voting technologies on election outcomes [Wa04], [CM07], [HW07]. Empirical studies have even been fewer in multiparty electoral systems, where with a larger number of parties and candidates on a ballot, voters might be more responsive to readily available information and thus may resort to different cues in order to identify and distinguish the various electoral options and to select their preferred choice [RS06].

In this paper, we analyze how different voting technologies influence voters' choice and election outcomes in multiparty races, examining evidence from a voting pilot conducted in the 2005 congressional election in Buenos Aires, Argentina, in which four e-vote prototypes were tested. We show that voters alter their electoral behaviour and their vote choice in response to different e-vote technologies, and that this might translate into different electoral outcomes across voting devices. Our main findings are in line with the results of [CSP07], in the sense that 'technology matters,' and that different voting technologies and associated ballot designs might have substantive effects on election results in multi-party electoral systems.

2 The E-Voting Experiment in Buenos Aires' 2005 Election

Voters in the congressional election held in Buenos Aires in October 2005, elected National representatives and State legislators using a party-list paper ballot system that included candidates for all offices¹¹. Seats were allocated using a PR-D'Hont formula with closed party lists of magnitude 13 for representatives and 30 for legislators. Thirty parties presented candidate lists for National representatives, while forty one parties presented lists for the state legislature. Three parties captured approximately 66% of the valid votes in the election of national representatives and 64% in the election of state legislators: President Kirchner's *Frente para la Victoria* (FPV), the center-left opposition party *Alianza para una Republica de Iguales* (ARI), and the center-right *Propuesta Republicana* (PRO)¹². The campaign for national representatives was very intense, with high spending in support of the candidacies of Rafael Bielsa (FPV), Elisa Carrio (ARI), and Mauricio Macri (PRO). By contrast, candidates to the local legislature spent almost no money during the campaign [CSP07].

The e-pilot was conducted in 41 precincts randomly distributed throughout the city and included 14,800 participants. After voting in the official election, participants in each precinct were asked to participate in a non-binding election in which they were randomly assigned to one of four possible voting devices and were asked to vote a list of national deputies and a list of local legislators. Because the experiment was carried out in a single electoral district, with participants in each precinct being randomly assigned to the different voting devices and facing similar menus of party choices, we expect no correlation between the characteristics of the district or the election and voters' behaviour¹³.

¹¹ The description of the e-vote pilot borrows from [CSP07].

¹² The vote-shares of ARI, FPV and PRO in the election of national representatives (state legislators) were 22.0% (20.8%), 20.5% (19.5%) and 34.1% (33.2%), respectively. If blank ballots are excluded, the vote share of these three parties comes close to 70%.

¹³ Organizational problems prevented the testing of all the prototypes in all the precincts, as originally planned. While Prototypes 1 and 2 were tested in all the precincts, Prototype 3 was tested in 40 precincts, and Prototype 4 in only 17. Although we do not expect this to have resulted in serious imbalance between the participants assigned to the different prototypes, we take this problem into account in the analysis below.

After the vote, participants were asked to complete two surveys. The first survey was a short self-administered survey (six questions) conducted with 13,830 respondents. Half of the questions were identical across prototypes, dealing with general perceptions about their e-vote experience. The remaining questions tested usability issues specific to each device. A fourth of the participants also answered a longer exit poll. This survey provided information about the voters' political sophistication, their familiarity with technology, their patterns of political participation, and their opinions and attitudes towards electronic voting.

The four voting devices tested in the pilot were developed with the institutional process of Argentina in mind. *Prototype 1* was a direct recording electronic (*DRE*) design with two separate modules. A screen in the first module allowed voters to review the lists of candidates, and a numerical keypad was used to register the vote. Voters would insert a "smart card" into the first module and use the keypad to navigate through screens to cast their ballots. When done, they removed their smart card, moved to a second module, and again inserted their smart card, automatically recording their vote. *Prototype 2* was a touch-screen *DRE* machine with a voter verifiable paper trail. After activating the system with their plastic "smart card" voters could scroll and select party lists directly by tapping onto the screen. When done with their ballot, a paper audit trail would be generated underneath a glass screen. If the voter affirmed that that indeed was how she wanted her vote to be cast, the paper audit trail fell into a bin and the voter was done; if not, the paper audit trail was rejected and the voter was allowed to cast the ballot again. *Prototype 3* was an optical scan (*OS*) prototype located inside a voting booth. The voter picked paper ballots for the party list she wished to support inside the booth, inserted those ballots into a rolling scanner that displayed the selected party on the prototype's screen, and would then proceed to confirm her selection. This prototype required separate ballots for each race, allowing direct comparison of the marks that identify a party across races. Finally, *Prototype 4* was an optical scan device with a single ballot listing all the parties running candidates for office in the two congressional. The voter marked her preferences for each race with a pencil and introduced the ballot into a scanner; the ballot would then fall into a ballot box. In all prototypes, participants voted for National representatives first and State legislators second.

An important difference between the DRE and OS prototypes was the way in which voters were required to search for their preferred candidates. In the DRE prototypes, party labels were randomly rotated on the screen and, because of space restrictions, a limited number of labels were displayed on each screen. Two and three screens were required to display party labels for national representatives and state legislators in *Prototype 1*, while three and four screens were required in *Prototype 2*. The placement of the party labels rotated randomly for each voter, preventing order effect biases from favouring the same party. In the case of *Prototype 3*, poll workers sorted the paper ballots numerically¹⁴. According to the information obtained from the polling place workers, however, ballots rapidly mixed in the voting booth, complicating the search for the voters' preferred ballots. Finally, in *Prototype 4*, party names were listed by their official list number in increasing order. The non-random ordering of parties may have increased the likelihood of order effects but it also facilitated the recognition of the same party across races.

A second relevant difference among the prototypes was how voters accessed information about candidates and parties. The first prototype displayed 15 party names on each screen, including the list number and party logo information. In order to view the list of candidates, however, the voter needed to enter the three-digit party number. If the voter did not know the name of the party, she would need to access each list until finding a recognizable candidate name. *Prototype 2*, on the other hand, displayed the name of the first candidate under the party label, together with the number and logo information. The complete list of candidates was then displayed on a second navigation level. Parties with prominent first candidates (such as the pro-Kirchner Rafael Bielsa from the FPV or Mauricio Macri of the center-right PRO) were readily identified by voters¹⁵. However, very little information about the party name or number was recalled when casting the legislative vote. Hence, while voters faced fewer problems in recognizing their preferred choice for national representative, they could not use such information when choosing state legislators.

Different information was available to voters using the optical scan systems. Ballot papers for *Prototype 3* included all the relevant information, such as party name, party logo, identification number, and the complete list of candidates for each race. The only difficulty in identifying the preferred choice, therefore, was in finding the correct paper ballot. In *Prototype 4*, a booklet provided voters with all the party information; the ballot introduced in the rolling scanner listed only the party name, number and logo. The main characteristics of the four prototypes tested in the experiment are summarized in this paper's supplementary materials (Appendix I).

¹⁴ When registering the candidates running for an election, each party is assigned a list number. Candidates and Parties advertise this number during the campaign, together with the party and candidate's name.

¹⁵ Bielsa was President Kirchner's Foreign Relations Minister at that time, while Macri is a famous businessman and was the president of one of the most famous soccer teams in Argentina.

3 A First Look at the Impact of Different E-Voting Technologies

The survey data lets us examine how voters interacted with each prototype and how the different voting technologies and the associated ballot designs affected voters' electoral choice. Table 1 presents data about which ballot features participants used to identify their preferred candidates. Nearly half of the voters cast their ballot based on the name of the party, followed by the name of the first candidate. The name of the party was particularly important for those participants using *Prototype 4*, and was less so for those using *Prototype 3*. Also, the name of the first candidate was more relevant for those assigned to *Prototype 2*, while participants using *Prototype 1* were less likely to use it as a voting cue, using more frequently the party number instead. This is consistent with the characteristics of the ballot designs associated with the different prototypes: the name of the first candidate figured prominently on the computer screen in the case of the second prototype, while voters using *Prototype 1* could access the candidates' names only after entering each party's number in the keypad. We found a statistically significant relationship between the information used by respondents to identify their preferred candidate and the voting technology used (p-value = 0.08).¹⁶

| Information used as voting cue | Prototype 1 (%) | Prototype 2 (%) | Prototype 3 (%) | Prototype 4 (%) | All prototypes (%) |
|--------------------------------|-----------------|-----------------|-----------------|-----------------|--------------------|
| Party name | 51.4 | 51.0 | 44.3 | 53.4 | 49.4 |
| First candidate's name | 33.3 | 50.1 | 47.1 | 45.0 | 44.2 |
| Party Logo | 27.3 | 30.3 | 22.4 | 7.4 | 25.8 |
| Party number | 35.4 | 21.0 | 19.9 | 28.6 | 25.3 |
| Other features | 4.1 | 2.7 | 7.5 | 6.4 | 4.6 |
| N | 879 | 1,158 | 858 | 189 | 3,084 |

Table 1: How voters found their preferred candidates¹⁷

Table 2, in turn, reports the percentage of participants who stated they were not able to vote for their preferred candidate for each of the prototypes, sorted by education and political information levels¹⁸.

¹⁶ Given that respondents could use several ballot features to identify their preferred choice, the assumption of independence among units required by standard tests of independence is violated. Thus, we used the bootstrap resampling method proposed in [LS98] to test for the association between voting cue and prototype.

¹⁷ Table entries are the percentage of respondents in each prototype that used each of the ballot features to identify their preferred candidates. Since participants could use several of the ballot features as voting cues, percentages do not necessarily sum to 100 rows across.

¹⁸ Both surveys included the question: "Were you able to vote for your preferred party/candidate?" Political information was computed as the average of respondents' number of correct answers to three questions asking them the names of the ministers of economy, education and health.

The survey data indicates that education significantly affected the ability of the participants to vote for their preferred party while only 3.8% of voters with college education were unable to cast a vote for their preferred option; this figure was almost 2.6 times higher for those with high school education or lower. The difference in the proportions between the two groups is statistically significant, with a 95% confidence interval of [0.04, 0.08]. Although less educated voters experienced more difficulties in all of the prototypes tested, the gap between participants with college education and the rest was much smaller for *Prototype 2*, suggesting that this device imposed lower barriers on less educated voters. The p-value of Woolf's test for homogeneity across prototypes is 0.001 [Wo55], indicating that there are considerable differences across voting technologies regarding the difficulties experienced by less educated participants.

When examining the data by political information levels, again, *Prototype 2* seems to have been more effective in enabling voters with null or low information levels to vote for their preferred choice. *Prototype 3*, in contrast, exhibits the higher rates of reported voting problems for all levels of political information. The Cochran-Armitage Trend Test [AG02] provides evidence of a modestly negative linear relationship between political information and reported voting problems (two-sided p-value = 0.1), but this is only statistically significant (at the 0.01 level) for *Prototype 1*. Overall, almost 90% of the voters were able to vote for their preferred party; *Prototype 2* exhibited the highest rate of success (93.9%), while *Prototype 3* had the lowest score (82.6%).

| Variable | Prototype 1 (%) | Prototype 2 (%) | Prototype 3 (%) | Prototype 4 (%) | All prototypes (%) |
|------------------------------|-----------------|-----------------|-----------------|-----------------|--------------------|
| Education | | | | | |
| College | 3.0 | 2.7 | 6.5 | 3.6 | 3.8 |
| Secondary or lower | 12.6 | 4.5 | 13.6 | 12.9 | 9.8 |
| N | 3,175 | 3,873 | 2,743 | 887 | 10,678 |
| Non-response rates | 21.4 | 18.4 | 28.2 | 27.5 | 22.8 |
| Political information | | | | | |
| Null | 9.9 | 3.4 | 11.4 | 0.0 | 7.3 |
| Low | 7.3 | 4.1 | 11.7 | 2.4 | 6.9 |
| Medium | 1.7 | 4.3 | 11.5 | 7.3 | 5.7 |
| High | 3.0 | 3.8 | 10.5 | 3.8 | 5.4 |
| N | 835 | 1,108 | 823 | 185 | 2,951 |
| Non-response rates | 5.0 | 4.3 | 4.1 | 2.1 | 4.3 |

Table 2: Percentage of voters who could not vote for their preferred candidate¹⁹

¹⁹ Table entries are the percentage of respondents in each prototype that were not able to cast a vote for their preferred candidate, among all respondents belonging to each row-category assigned to that prototype. The data on education levels was taken from the short self-administered survey, while the data on political information was obtained from the longer exit poll.

The fact that the four prototypes imposed different information demands on the participants and seem to have influenced the cues they used to identify the candidates, suggests that the e-voting devices could have had systematic effects on electoral outcomes. For instance, parties with more visible candidates should have fared relatively better among voters using *Prototype 2*, and those with more recognizable names/logos might have benefited from the ballot design and screen display in the DRE devices. Figure 1 explores this issue further, plotting the means and 95% confidence intervals of the vote-shares of the parties in the election of National representatives and State legislators under each prototype^{20,21}. For all the prototypes tested, each of the three majority parties, *Alianza para una Republica de Iguales* (ARI), *Frente para la Victoria* (FPV) and *Propuesta Republicana* (PRO), exhibited higher vote-shares in the first election, jointly obtaining 65% of the total vote cast for the parties competing in the election of National representatives. In contrast, minority parties gathered almost 50% of the vote in the less visibility race for State legislators. However, there are considerable variations in the support for the different parties across prototypes. The support for minority parties in both races was substantially higher under *Prototype 3*, reaching 48.7% in the election of National representatives and 55.7% in the election for the local legislature. In contrast, their vote-share was the lowest under *Prototype 4*, with 36.4% and 41.6% respectively. The support for the largest parties also varied across prototypes. For the four prototypes tested, the vote-share of ARI, FPV and PRO in the in the National (Local) election was 21.0% (18.2%), 15.6% (12.6%) and 22.6% (19.9%), respectively. However, the three large parties fared considerably better under the two DRE devices than under *Prototype 3*. We used bootstrapped Kolmogorov-Smirnov tests to examine the differences in each party's average support between pairs of prototypes [Ab02]. We found statistically significant differences at the usual confidence levels between the average vote-shares of FPV and PRO under *Prototypes 1* and *2* and their support under *Prototype 3* in both congressional races, as well as between the support for ARI under *Prototypes 1* and *3* in the national election. There are also significant differences in the support for the smaller parties under *Prototype 3* and each of the other prototypes in the two elections analyzed²².

²⁰ Vote-shares are expressed as percentages of the total number of votes cast for the competing parties in both races, excluding blank and null votes. Although *Prototype 3* had a higher rate of blank ballots than the other e-voting devices [CEP07], the results regarding the relative support for the different parties remain virtually unchanged when including blank ballots in the analysis.

²¹ Note that, while ARI's vote-shares in the two experimental elections were similar to those in the official elections, the support for FPV and PRO was lower and the vote for the smaller parties was higher in the pilot, compared to the actual elections.

²² See Appendix II of the paper's supplementary materials for details.

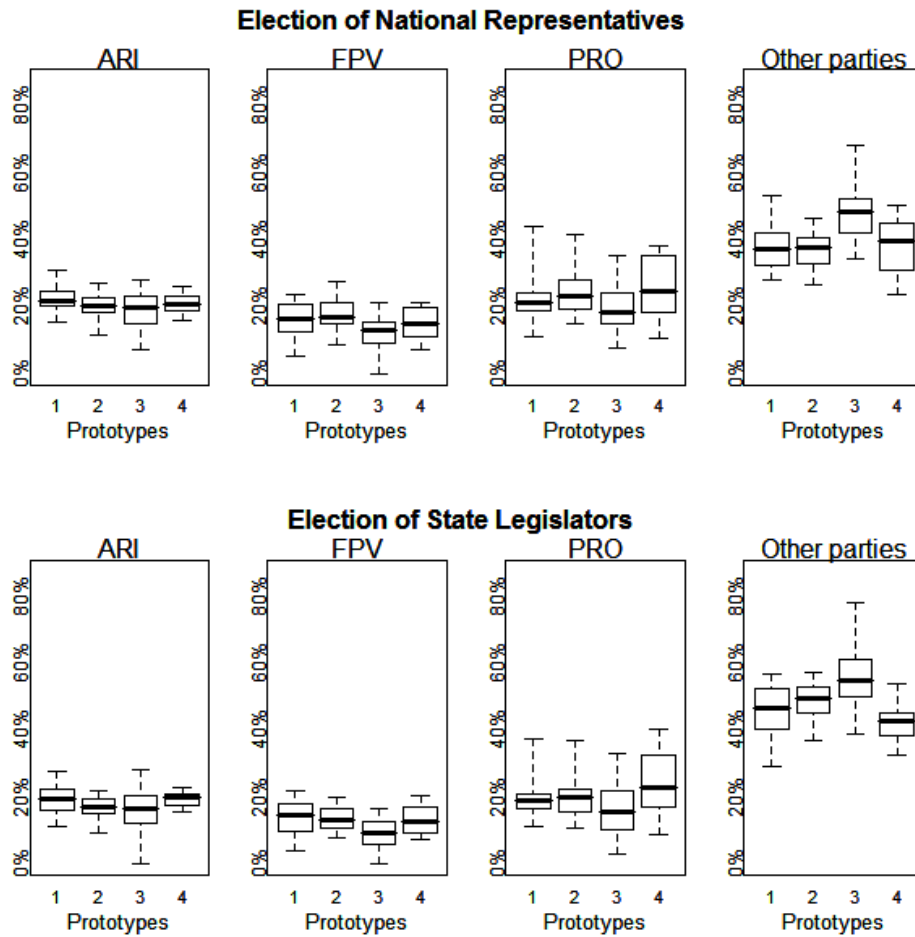


Figure 1: Distribution of the support for the parties under each prototype²³

²³ The thick horizontal lines correspond to the median vote-shares of the parties under each prototype. The rectangles correspond to the 50% interval, and the outer thin lines to the 95% intervals.

4 Estimating the Effect of E-Voting Technologies on Election Outcomes

While the data presented in the previous section reveals some interesting differences in voters' electoral behavior across voting devices, it does not allow us to assess the impact of the different technologies and ballot designs on the voter choice after accounting for the effect of socio-demographic and attitudinal variables. Controlling for these predictors might be relevant in order to estimate the causal effect of the e-voting devices on voters' choice and election outcomes [GH07], given that not all of the four prototypes were used in all the districts analyzed²⁴.

As our data includes the individual level votes for all the participants in the pilot, we can analyze the aggregate electoral and survey data from 128 voting stations defined by crossing each of the precincts with the e-voting devices²⁵. Our dependent variable is the vote-share of ARI, FPV, PRO and Other parties in the election for National representatives and State legislators in each of the voting stations, where the category "Other parties" comprises all the remaining parties in both races²⁶. The independent variables used in the analysis are defined at the voting station level and include: the mean Education level; the mean level of *Political Information*; *Interest in politics*; the mean level of participants' *Use of Technology*; *Perceived Difficulty of E-Voting*; and four variables measuring the percentage of participants who found their preferred party searching by *Party Name*, by *Party Logo*, by *Party Number*, or by *Candidate Name*. Additional details and descriptive statistics for these variables are provided in Appendix III of this paper's supplementary materials.

In order to estimate the causal effect of different voting technologies on the expected support for the parties competing in 2005, we implemented a multinomial-logistic model for the multinomial probabilities of support for ARI, FPV and PRO, with "Other parties" as the baseline category [Co05]. The probabilities of support for the parties are modelled as functions of the voting station covariates described above. In addition, in order to account for the cluster sampling scheme used in the experiment and to allow for unobserved heterogeneity across voting stations and for potential correlation in the election results across prototypes and precincts, we include zero-mean random effects for the two non-nested factors [Co05], [GH07]. The model was fit by MCMC Gibbs sampling methods [CS92]. The main advantage of using Bayesian estimation is that it allows obtaining arbitrarily precise approximations to the posterior densities, without relying on large-sample theory [Ja04].

²⁴ See footnote 3.

²⁵ Although the individual vote variable can be retrieved from each prototype's logs, privacy considerations prevented us from linking the individual vote with the individual survey data. Combining the information from the logs and the surveys, we have data from 128 out of the 139 possible voting stations, after dropping 924 individual observations with missing values from our analysis.

²⁶ "Other parties" includes 26 smaller parties in the election for National representatives and 37 parties in the election for the State Legislature.

In order to evaluate the model fit, we used posterior predictive simulations to assess the model’s ability to reproduce the overdispersion present in the data, comparing the Pearson statistic computed from the observed data with that computed using replicates sampled from the model [Co05]. Additional details about the model specification, the estimation procedure and robustness checks are provided in Appendix IV of the supplementary materials.

5 Empirical Results

Table 3 reports the posterior means and standard deviations for the fixed effects for the two elections under analysis. The model satisfactorily replicates the overdispersion in the data, with values of $P(\chi_{Rep}^2 > \chi_{Obs}^2)$ close to 0.5 for both elections [Co05].²⁷

| Parameter | Election of National representatives | | | Election of State legislators | | |
|----------------------------------|---|--------------------|--------------------|----------------------------------|-------------------|-------------------|
| | ARI | FPV | PRO | ARI | FPV | PRO |
| Education | 0.10 (0.14) | -0.23*** (0.09) | 0.29** (0.12) | 0.14 (0.10) | -0.23** (0.11) | 0.29* (0.15) |
| Political information | 0.54* (0.32) | 0.27 (0.33) | -0.36 (0.34) | 0.70** (0.30) | -0.01 (0.33) | -0.09 (0.33) |
| Interest in Politics | -0.15 (0.19) | 0.41* (0.21) | 0.24 (0.20) | -0.09 (0.19) | 0.44* (0.22) | 0.51*** (0.19) |
| Use of Technology | 0.05 (0.16) | 0.10 (0.17) | 0.25 (0.17) | 0.01 (0.16) | 0.33* (0.18) | 0.22 (0.16) |
| Assessment of E-Voting | 0.19 (0.43) | 0.34 (0.35) | 0.19 (0.36) | 0.36 (0.40) | 0.05 (0.50) | -0.16 (0.37) |
| Search by Party Name | -0.54** (0.26) | -0.18 (0.28) | -0.44* (0.26) | -0.11 (0.27) | -0.59** (0.31) | -0.29 (0.27) |
| Search by Party Logo | 0.01 (0.31) | 0.02 (0.34) | 0.24 (0.33) | -0.05 (0.32) | 0.18 (0.35) | 0.45 (0.34) |
| Search by Party Number | -0.06 (0.32) | 0.77** (0.35) | 0.43 (0.34) | -0.21 (0.33) | 0.52 (0.39) | 0.12 (0.33) |
| Search by Candidate Name | -0.39 (0.25) | -0.06 (0.25) | -0.73*** (0.27) | -0.07 (0.24) | 0.05 (0.28) | -0.47* (0.27) |
| Intercept | -1.13 (1.44) | -1.03 (0.68) | -2.73** (1.09) | -2.48** (1.05) | -0.77 (1.15) | -3.44** (1.31) |
| N | 128 | | | 128 | | |
| $P(\chi_{Rep}^2 > \chi_{Obs}^2)$ | 0.42 | | | 0.57 | | |

Table 3: Estimated posterior means and standard deviations for the fixed effects (Standard deviation in parenthesis; significance levels: *** 0.01, ** 0.05, *0.1)

²⁷ χ_{Obs}^2 is the usual Pearson statistic computed from the observed data, and χ_{Rep}^2 is using the replicates sampled from the model. See Appendix IV in the supplementary materials.

The results in Table 3 reveal some interesting differences regarding the effect of several covariates on the relative support for the three largest parties. For instance, in the two elections analyzed, the votes for *Propuesta Republicana* (PRO) increased in voting stations with higher average levels of education, while they decreased for *Frente para la Victoria* (FPV). In contrast, higher average levels of political interest were associated with higher support for FPV. This result is consistent with prior research that emphasizes class and education effects among non-Peronist voters [CM04]. Regarding the effect of the different information cues used by participants when casting their vote, the support for FPV in the more visible race increased with the percentage of voters relying on the official party number. On the other hand, the vote for ARI and PRO was negatively related to the percentage of participants using the name of the party in the election for National representatives, while there is a negative relationship between *Search by Party Name* and the support for FPV in the less visible election. The vote for PRO was also negatively associated by the percentage of voters basing their choice on the first candidate's name in both congressional elections.

The main focus of our analysis, however, lies in the effect of the different voting technologies on the support for the competing parties across elections. Figure 2 presents the posterior means and confidence intervals of the prototype effects for each of the parties in both elections.

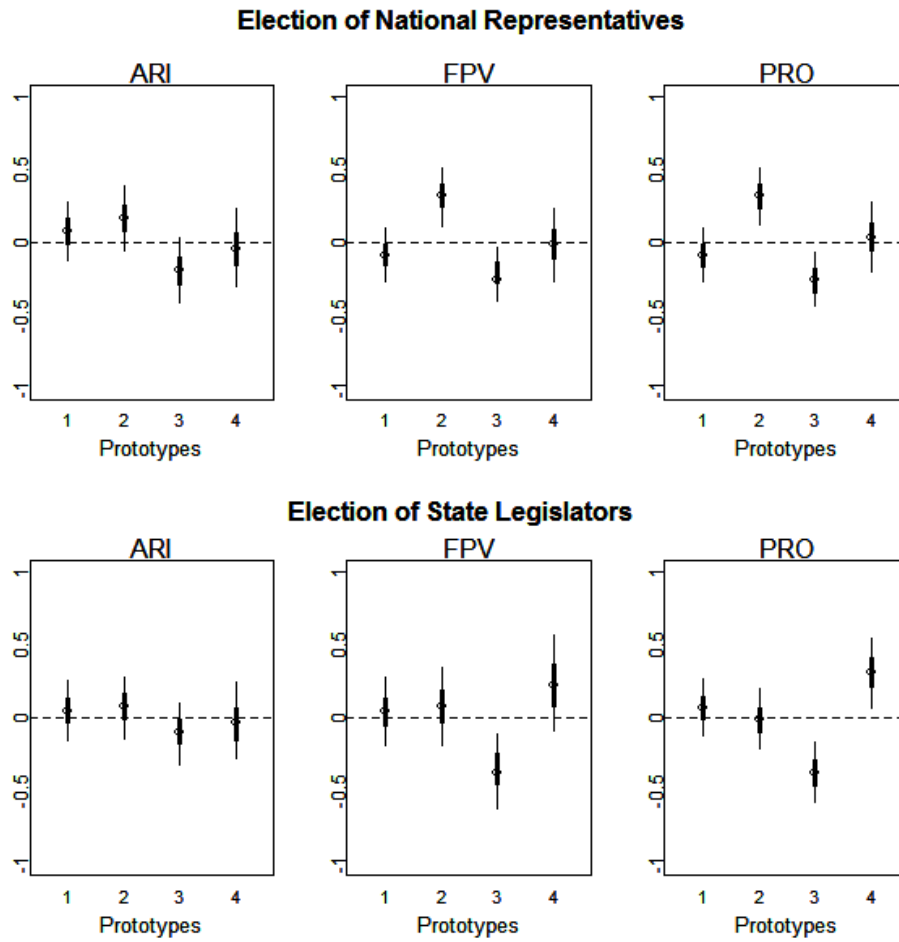


Figure 2: Prototype random coefficients for both congressional elections²⁸

²⁸ The center dots correspond to the point estimates of the prototype effects, the thicker lines to the 50% confidence interval, and the thinner lines to the 90% confidence interval.

These results indicate that different voting devices have potential influences on electoral outcomes after controlling for socio-demographic and behavioural variables. The effect of the voting technologies and the associated ballot designs varied considerably across parties and races. For instance, while the Optical Scan device with separate ballots (*Prototype 3*) had a significantly negative effect on the votes for FPV and PRO in both congressional elections, the touch-screen DRE device (*Prototype 2*) had the opposite effect, raising the support for FPV and PRO in the election for national representatives, although not in the election for state legislators. As mentioned above, the name of the first candidate of each party figured prominently on the screen of *Prototype 2*, and more than half of the participants using this device cast their vote based on this information. Hence, a possible interpretation of this result is that, while the first candidates of FPV and PRO, Bielsa and Macri, were renowned figures who were easily identifiable by voters, participants generally did not recognize the candidates running for the local legislature of any of the competing parties [CEP07]. Thus, the relative advantage obtained by FPV and PRO in the more salient election disappeared in the less visible race. Interestingly, however, the results reported in Table 3 show that the percentage of respondents using the first candidate's name had no systematic effect on the support for FPV in either of the races, while it had a negative impact on the vote for PRO. This indicates that the prototype-effects might be capturing additional sources of variability in the dependent variables, beyond that explained by the aggregate survey data.

Table 4 complements the information presented in Figure 2, reporting the mean posterior and 50% and 90% confidence intervals of the pairwise differences in the probabilities of supporting each party across prototypes. After controlling for other factors, the support for the largest parties tends to be higher for the two DRE devices than for *Prototype 3*, although the differences between *Prototype 1* and *3* are not statistically significant at the usual confidence levels. In contrast, in the cases of FPV and PRO, there are significant differences between their support for *Prototypes 2* and *3*: the touch-screen DRE device leads to an increase of 3.8 and 6.3 percentage points in their vote-shares, respectively, in the election for National representatives, and of 2.7 and 5.3 percentage points in the election for state legislators; these differences are significant at the 0.01 level. As shown in Figure 2, in the more visible race, these differences stem both from an increase in the support for FPV and PRO induced by *Prototype 2* and a reduction of their support for *Prototype 3*. In contrast, the results in the election for state legislators are entirely driven by the higher support for the smaller parties under the OS device with separate ballots. In fact, the relative support for the smaller parties tends to be consistently higher with *Prototype 3* in both races: in the national representative election, the vote-share of the minor parties is 11 percentage points higher under *Prototype 3 vis a vis Prototype 2*, while in the state legislature election their vote with this prototype is systematically higher when compared against all the other voting devices. Also, in the national election, the relative support for the smaller parties is lower with *Prototype 2* than *Prototype 1*. Hence, in the more visible race, the touch-screen DRE device consistently favours the parties with more renowned candidates, to the detriment of the smaller ones.

| | Pairwise comparisons | π^{ARI} | π^{FPV} | π^{PRO} | π^{OTHER} |
|--------------------------------------|----------------------|---------------------|----------------------|-----------------------|------------------------|
| Election of National representatives | Prototypes 1-2 | 2.1 (-4.2, 8.7) | -3.6 (-8.4, 1.0) | -5.2 (-10.9, 0.4) | 6.6 (0.8, 12.4) |
| | Prototypes 1-3 | 3.4 (-3.2, 9.9) | 0.2 (-4.0, 4.4) | 1.2 (-4.6, 2.1) | -4.8 (-10.8, 1.7) |
| | Prototypes 1-4 | 2.9 (-0.4, 6.0) | -1.0 (-4.3, 1.9) | -2.4 (-6.0, 1.0) | 0.5 (-3.6, 4.3) |
| | Prototypes 2-3 | 1.3 (-0.5, 3.3) | 3.8 (2.1, 5.7) | 6.3 (4.4, 8.3) | -11.0 (-13.7, -9.2) |
| | Prototypes 2-4 | 0.7 (-6.9, 8.0) | 2.6 (-3.3, 8.3) | 2.7 (-4.2, 9.4) | -6.1 (-13.0, 1.0) |
| | Prototypes 3-4 | -0.5 (-7.7, 6.5) | -1.2 (-6.3, 4.9) | -3.6 (-9.8, 2.4) | 5.3 (-2.1, 13.4) |
| Election of State legislators | Prototypes 1-2 | -0.6 (-5.4, 5.1) | -0.55 (-5.5, 4.6) | 1.5 (-4.2, 6.9) | -0.4 (-7.7, 6.5) |
| | Prototypes 1-3 | -0.2 (-5.3, 5.2) | 2.7 (-1.5, 7.4) | 5.3 (-0.1, 10.4) | -7.8 (-15.1, -0.8) |
| | Prototypes 1-4 | 2.5 (-0.5, 5.4) | -1.7 (-5.0, 1.4) | -4.0 (-7.8, -0.3) | 3.1 (-0.9, 7.2) |
| | Prototypes 2-3 | 0.4 (-1.4, 2.2) | 3.3 (1.8, 4.9) | 3.8 (1.9, 5.7) | -7.5 (-9.8, -5.1) |
| | Prototypes 2-4 | 3.1 (-2.8, 8.7) | -1.1 (-7.8, 5.2) | -5.5 (-12.2, 1.5) | 3.5 (-4.6, 12.3) |
| | Prototypes 3-4 | 2.7 (-3.0, 8.0) | -4.4 (-10.6, 1.1) | -9.3 (-15.6, -3.1) | 11.0 (2.8, 19.5) |

Table 4: Pairwise differences in the probability of support for each party across prototypes in percentage points (90% confidence intervals in parenthesis)

These results provide strong evidence in support of the hypothesis that alternative voting technologies may have substantive influence on the support for different parties. The relevant question thus becomes: how would the election outcomes vary under different voting technologies? In order to answer this question, we estimate the expected electoral outcome assuming only one prototype had been used in each voting-station, while holding all the remaining variables constant. Table 5 reports the expected election outcomes in both races for each of the four prototypes and compares them to the actual results in the experiment.

The evidence indicates that different voting technologies would in fact have led to quite different election results. For instance, if *Prototype 1* had been used in all voting stations, ARI would have had the highest expected support in the election for national representatives, rather than the actual winner, PRO. ARI would also have had the highest expected support in the election for state legislators under *Prototype 3*. In contrast, the vote-shares of PRO and FPV in the national election would have been maximized under *Prototype 2*, increasing their support at the expense of ARI and, especially, of the smallest parties. In the less visible race, however, the advantage enjoyed by PRO and FPV under the touch-screen DRE device would have virtually vanished. Finally, the expected support for minor parties in both races would have increased by almost 6 percentage points under *Prototype 3* with respect to the actual results in the experiment. Thus, the choice among different e-voting technologies could have had substantive effects on the election results.

| | ARI | FPV | PRO | Other Parties |
|----------------------------------|-------|-------|-------|---------------|
| Election of N. Representatives | | | | |
| Prototype 1 | 22.77 | 14.52 | 21.59 | 41.12 |
| Prototype 2 | 20.64 | 18.13 | 26.74 | 34.49 |
| Prototype 3 | 19.36 | 14.33 | 20.40 | 45.91 |
| Prototype 4 | 19.89 | 15.52 | 23.99 | 40.60 |
| Actual outcome in the experiment | 21.03 | 15.58 | 23.16 | 40.24 |
| Election of S. Legislators | | | | |
| Prototype 1 | 18.00 | 12.97 | 21.87 | 47.16 |
| Prototype 2 | 18.57 | 13.52 | 20.38 | 47.53 |
| Prototype 3 | 18.16 | 10.25 | 16.59 | 55.00 |
| Prototype 4 | 15.47 | 14.64 | 25.84 | 44.05 |
| Actual outcome in the experiment | 18.04 | 12.31 | 20.43 | 49.22 |

Table 5: Expected and actual election outcomes in percentage points

6 Concluding Remarks

Multiparty races impose substantial demands on voters, who have to gather enough information to be able to distinguish between the positions of the different parties before the elections and to identify their preferred choice at the polls. Using data from a large-scale e-vote experiment in Buenos Aires, we present the first study on the impact of different electronic voting systems on election outcomes in multi-party races. Our results indicate that different devices have considerable influence on the relative support for different parties across races, after controlling for relevant socio-demographic and behavioural predictors. In contrast to studies on this topic examining two-party elections in the U.S., most of which have found that the impact of alternative voting technologies on election outcomes is quite small [CS07], [HW07], our findings show that this effect might be large enough to potentially affect the election results. In this sense, our results are in line with the findings of [RS06], indicating that amount and the form in which information is presented to voters by different e-voting technologies might have a considerable influence on voting behavior in multi-party elections.

The evidence presented in this paper is particularly significant in view of the increasing trend towards electronic voting and the growing number of countries moving from traditional paper ballots to electronic voting systems. In many of these countries, political parties have repeatedly expressed concerns about the possibility of being systematically disadvantaged by the new voting technologies²⁹. Our results suggest that this might actually be the case, rather than just a myth fuelled by politicians, and raises the possibility that some voting technologies may in fact shape the electoral outcomes, rather than merely recording voters' preferred choices.

References

- [Ab02] Abadie, A.: "Bootstrap Test for Distributional Treatment Effect in Instrumental Variable Models". *Journal of the American Statistical Association*, 97(457), 2002, pp. 284-292.
- [Ag02] Agresti, A.: *Categorical Data Analysis*. New Jersey: John Wiley & Sons, 2002.
- [AH08] Alvarez, R.; Hall, T.: *Electronic Elections: The Perils and Promises of Digital Democracy*. Princeton, NJ: Princeton University Press, 2008.
- [AS05] Ansolabehre, S.; Stewart, C.: "Residual Votes Attributable to Technology". *Journal of Politics*, 67(2), 2005, pp. 365-389.
- [CEP07] Calvo, E.; Escolar, M.; Pomares, J.: "Ballot Design and Split Ticket Voting in Multiparty Systems: experimental evidence on information effects and vote choice." Unpublished manuscript, 2007.
- [CM04] Calvo, E.; Murillo, M.: "Who Delivers? Partisan Clients in the Argentine Electoral Market." *American Journal of Political Science*, 48(4), 2004, pp. 742-757.
- [CM07] Card, D.; Moretti, E.: "Does Voting Technology Affect Election Outcomes? Touch-screen Voting and the 2004 Presidential Election". *Review of Economics and Statistics*, 89 (4), 2007, pp. 660-673.
- [CG92] Casella, G.; George, E.: "Explaining the Gibbs Sampler". *The American Statistician*, 46(3), 1992, pp. 167-174.
- [Co05] Congdon, P.: *Bayesian Models for Categorical Data*. New York: John Wiley & Sons, 2005.
- [GH07] Gelman, A.; Hill, J.: *Data Analysis Using Regression and Multilevel / Hierarchical Models*. New York: Cambridge University Press, 2007.
- [HW07] Herron, M.; Wand, J.: "Assessing partisan bias in voting technology: The case of the 2004 New Hampshire recount". *Electoral Studies*, 26(2), 2007, pp. 247-261.
- [Ja04] Jackman, S.: "Bayesian Analysis for Political Research". *Annual Review of Political Science*, 7, 2004, pp. 483-505.
- [LS98] Loughin, T.; Scherer, P.: "Testing for Association in Contingency Tables with Multiple Column Responses". *Biometrics*, 54(2), 1998, pp. 630-637.
- [RS06] Reynolds, A.; Steenbergen, M.: "How the world votes: the political consequences of ballot design, innovation and manipulation." *Electoral Studies*, 25(3), 2006, pp. 570-598.
- [S04] Stewart, C.: "The Reliability of Electronic Voting Machines in Georgia". Working Paper 20, Caltech/MIT Voting Technology Project, 2004.
- [Wa04] Wand, J.: "Evaluating Voting Technologies: 2004 New Hampshire Democratic Primary. Technical Report, Stanford University, 2004.
- [Wo55] Wolf, B.: "On estimating the relation between blood group and disease." *Annals of Human Genetics*, 19, 1955, pp. 251-253.

²⁹ For instance, several French parties expressed such concerns during the 2007 Presidential election, the first time electronic voting machines were used for a presidential election in the country (Le Figaro, 04/18/2007).

Assessing Internet Voting as an Early Voting Reform in the United States

Alicia Kolar Prevost

American University
4400 Massachusetts Avenue NW
Washington, DC20016
Alicia.prevost@american.edu

Abstract: Recent research on convenience voting reforms in the United States has found that programs designed to make voting easier have not succeeded in boosting turnout, and have even had the unintended consequence of exacerbating the demographic biases that already exist in the electorate by encouraging votes among those who were most likely to vote anyway but who were inconvenienced by going to the polls on election day. Using public voting records and a unique dataset of Internet voters in the 2004 Michigan Democratic Presidential primary, this paper offers new evidence that Internet voting benefits two groups of people: young voters and people who vote infrequently. Like previous research on voting reforms, I also find evidence that Internet voting does not draw new voters into the electorate. I discuss the implications of these findings for the future of early voting reforms in general and Internet voting in particular.

1 Introduction

Americans routinely use the Internet for banking, commerce, social networking, and even paying taxes, but they have not been able to use the Internet for voting in elections for public office. At a time when Internet use is widespread and voting systems are being reassessed in nearly every state, and when Internet voting has been successfully tested in European countries at the local and even national level, why has Internet voting not been introduced in state administered elections in the US? Although state and local election administrators have not embarked on tests of Internet voting, state political parties have used Internet voting in two binding state-wide elections. These trials, held in 2000 in Arizona and 2004 in Michigan, can provide important information about the feasibility of Internet voting in future elections in the US. Before state election administrators can plan online voting trials, we must have a better understanding of the online elections that have already occurred in the US. This paper offers a better understanding of how Internet voting affects turnout among different demographic groups.

Recent studies of voting reforms have found that programs designed to make voting easier have had only small positive effects on turnout and have had the unintended consequence of exacerbating the demographic biases that already exist in the electorate [Be05; Tr04]. Convenience voting reforms such as vote-by-mail, no-excuse absentee voting, and in-person early voting have been shown to encourage votes among those voters who were most likely to cast a ballot anyway but were inconvenienced by having to go to the polls on election day. Internet voting is the newest innovation among these early voting reforms. However, there have been few opportunities to study Internet voting as an early voting reform in the United States. Findings from academic studies of Internet voting in Arizona in 2000 and Michigan in 2004 have been mixed on the effect Internet voting has on turnout among certain demographic groups [AN01; PS08].

Using public voting records and a unique dataset of individuals who participated in the 2004 Michigan Democratic Presidential primary, this paper examines the claims that Internet voting specifically and early voting reforms in general may only benefit those who were most likely to vote anyway. This research builds on previous studies of the effects of Internet voting as an early voting reform by offering an examination of voters at the individual level and incorporating voting history as an indicator of future voting behavior. I find that young people and people who vote infrequently benefit most from Internet voting. I also find that income is positively related to voting online, but race and education were not significant predictors of voting on the Internet.

This research adds to the body of knowledge on voting behavior by introducing new evidence on the effects of Internet voting as an early voting reform. This paper also incorporates the use of state voter files as an alternative to more traditional data sources for studying the effects of voting reforms on voter turnout. Similar research that uses public voting records includes Berinsky, Burns and Traugott [BBT01], in which the authors obtain individual vote history and confirm self-reported voting behavior from county records for a group of survey respondents. Public voting archives are readily available in most states, and are used regularly by political operatives, but seem to be rarely used by political scientists. Since the effects of voting reforms are often very small, it may be necessary to examine these reforms at the individual level, as Berinsky, Burns and Traugott argue [BBT01].

I begin with a review of the research on early voting reforms in general and the limited trails of online voting in the US. I then summarize the details of the unique dataset that I employ, including information about the 2004 Michigan Democratic primary, and describe the methods that I will use to evaluate Internet voting. Finally, I present the results of a multinomial logit regression model and discuss the implications of these findings for the future of Internet voting as an early voting reform.

2 Literature Review

2.1 Poor Marks for Voting Reforms

In recent years, political science research on reforms to make voting easier has been nearly unanimous in concluding that the reforms have not met their stated goals of increasing turnout and improving the representativeness of the electorate. Paul Gronke's overview of voting reforms argues that scholarly consensus has been reached on this point: "Early voting does not increase turnout by bringing new voters into the system. What it does is encourage regular voters to participate in lower intensity contests that they might otherwise skip" [Gr04]. Berinsky [Be05] and Traugott [Tr04] offer similar reviews of the political science literature on voting reforms with the same conclusion: that voting reforms have not achieved the goals that the reformers had in mind, and in fact the demographic representativeness of the electorate is actually worsened by easy voting reforms since "more of the same" voters – that is, highly educated, older, and richer voters – are even more likely to turn out using easy voting methods.

Berinsky [Be05] reviews the literature on voting reforms and concludes that they have had "perverse consequences" in that they have encouraged the people who were most likely to vote anyway (those who have higher incomes and are more educated) but were inconvenienced by going to a polling place on election day. Traugott [Tr04] argues that electoral reform has failed because it has not achieved the goals of substantial increases in turnout or greater socioeconomic diversity in the electorate. These findings are important because they show that groups who have always been underrepresented in the electorate – the poor, people without college degrees, and young adults – may become an even smaller percentage of the electorate, as easy voting reforms encourage more voters with higher incomes and more education to turn out, and mail balloting encourages more older voters to turn out. In addition, these findings might also bolster the arguments of policy makers who are opposed to expanding early voting options. Given the potential implications of these findings for policy makers and election administrators, it is important that analyses of voting reforms be conducted with the best evidence available and at the lowest level of aggregation possible in order to make inferences about the effects on individual voters. However, much of the empirical research on voting reforms has relied on evidence that might not be generalizable to individual voters. Previous studies have used survey data [NR01], exit polls [SG97], and aggregate data [AN01; Gi02]; all of which are problematic for making generalizations about individual voters. Although these studies have contributed important findings about the effects of early voting reforms, it is important to recognize the possible limitations of using aggregate data or unverified survey responses to make public policy decisions. Telephone surveys are increasingly unreliable because of the high no-response rate, and respondents tend to over-report turnout [TK79]. Exit polls only survey voters (by definition they leave out the non-voters who are not at the polls), and aggregating voter turnout data at high levels makes it difficult to make inferences about individual voters.

Studies of Internet voting use self-reported telephone survey responses [So01], or turnout aggregated at the county level [Gi02; AN01], which is a high level of aggregation and therefore not an accurate estimator of individual-level information. One of the strongest arguments against Internet voting is that it is biased against racial and ethnic minorities and citizens of lower socioeconomic status, since these groups have less access to the Internet. This claim has largely been supported by the existing academic literature on Internet voting, including the finding that the decrease in turnout was five times as great for non-white voters in the Internet voting election in Arizona [AN01]. However, the authors of that study use data and demographic variables (including race) aggregated at the county level. Since there are only 15 counties in the state of Arizona, this is a particularly high level of aggregation. Another study of Internet voting that uses individual level information about voters in the 2004 Michigan primary found that race was not a strong predictor of choosing Internet over mail voting, but it was a factor in the choice of applying to vote early [PS08].

The analysis conducted in this paper extends the research of Prevost and Schaffner [PS08], which examined the pool of voters who participated in the 2004 Michigan Democratic primary to see if there were differences in the demographic characteristics of those who voted on the Internet, by mail, or in-person. Prevost and Schaffner [PS08] found that voters in predominately African American zip codes were somewhat less likely to vote on the Internet than voters in predominately white zip codes, but not by margins as large as some critics of Internet voting suggested. The authors also found that young people were most likely to take advantage of Internet voting, while older voters were more likely to take advantage of voting by mail.

2.2 Individual Voting History and the Likelihood of Voting

State voter files can show the relationship between voting history and the use of easy voting methods. The theory that infrequent or first time voters can be enticed into the electorate by easy voting reforms can be tested empirically using public voting records. Berinsky, Burns, and Traugott develop a duration model to see if individual vote history has an effect on whether voters will participate in Oregon's vote-by-mail system [BBT01]. They find that voting-by-mail encourages occasional voters who are older, well educated, and those with higher levels of interest in the campaign. They also find that habitual non-voters are not drawn into the electorate by the easy vote-by-mail system.

Given that voter history has an effect on future voting behavior, Berinsky [Be05] proposes a two-part conception of the electorate, in which he considers both the stimulation of new or infrequent voters and the retention of other voters from election to election. He contends that electoral reforms will have a greater effect on the retention of voters than on the stimulation of new voters. Berinsky reasons that electoral reforms “increase the propensity of likely voters to consistently turnout by smoothing over the idiosyncrasies that cause engaged citizens to sometimes miss casting their votes in particular elections” [Be05: 477]. He suggests that to properly observe the effects of voting reforms on the composition of the electorate, we should analyze individual-level data over time to see if easy voting methods are used by regular voters (retention) or infrequent voters (stimulation). However, the only research he cites that uses individual-level data over time is a study of voting by mail in Oregon [BBT01].

Other empirical research supports the claim that those who have voted previously are more likely to vote in the future. Green et al [GGS03] find that voting in one election substantially increases the likelihood of voting in a subsequent election. The authors find voter history to have a greater effect than education and age in predicting whether an individual will turn out to vote. Using a randomized field experiment, they find that voting in 1998 increased the probability of voting in 1999 by 46.7 percentage points [GGS03: 547]. These findings suggest that vote history is an important variable in any model predicting voting behavior, but it has rarely been used in political science studies of voting behavior. Two exceptions where individual voting history has been used are Plutzer [Pl02] and Berinsky, Burns and Traugott [BBT01]. Using panel data spanning several decades, Plutzer finds that voting (and non-voting) is “habitual” – once a person starts voting she is likely to continue doing so [Pl02]. Using individual level voting history from public voting records, I analyze the effects of voting history on the propensity to use Internet voting as an early voting method.

3 Description of the 2004 Michigan Democratic Presidential Primary

The 2004 Democratic presidential nominating contest in Michigan has been called a caucus, a firehouse primary, and a party-run primary. The Democratic National Committee (DNC) officially defined it as a party-run primary, because it had many features of a primary, including an option for absentee voting, so it is referred to as a primary in this paper. The contest had some features of a caucus, including the fact that ballots cast were not secret. This feature allowed the Michigan Democratic Party (MDP), which administered the election, to circumvent many of the security concerns associated with Internet voting, since it allowed each voter to be assigned a unique identification and PIN number. In order to participate in the party-run primary, an individual could either apply for an absentee ballot or vote in person on election day. The absentee ballot application could be accessed on the MDP website, and several presidential campaigns also distributed them to supporters. The application could then be completed online, or printed and sent by mail or fax to the MDP. Once the application was received by MDP staff, it was checked against the state voter file for accuracy, so a person applying for an absentee ballot had to be a registered voter in the state. Alternatively, a person could decide on election day to vote in person at a caucus location without having taken any prior action.

In many ways, the Michigan Internet ballot was much like a traditional absentee ballot that a voter would send in a secrecy envelope to prevent election workers from seeing for whom a particular individual is voting. Media reports of the Michigan primary did not mention voters being concerned with privacy violations. It may be the case that voters who choose to vote absentee have come to accept that there is a possibility that an election worker will see their vote choice, and that is an acceptable cost given the benefit of being able to vote early or from home. 162,929 voters participated in the 2004 Michigan Democratic primary. 28.4% voted by Internet, 14.5% voted by traditional mail-in absentee, and 57.1% voted in-person at a caucus location on election day.

Michigan does not require a voter to declare a party affiliation when registering to vote. One implication of this is that the state has an open primary system – a voter can take a ballot for either party's primary, which means that Republicans can vote in Democratic primaries, and vice versa. This violates the rules of the Democratic National Committee, and so the Democratic party in Michigan has been forced to administer party-run primaries or caucuses for its presidential nominating contests.

4 Data and Methods

Two datasets serve as the empirical evidence for this analysis: the Michigan Qualified Voter File and turnout data from the 2004 Michigan Democratic Primary. The Michigan Voter File is publicly available from the Michigan Secretary of State. It contains individual-level information about the voting behavior of each of the approximately 7 million voters who are currently registered in the state, including name, address, gender, date of birth, and voting history for every state administered election. However, since the 2004 Democratic Primary was a party-run election, which was administered by the state Democratic party, voter history information for this election is not included on the state voter file.

Turnout data from the 2004 Michigan Democratic primary was provided by the MDP. It contains individual level-information for the approximately 162,000 voters who participated, including name, address, and choice of voting method: Internet, mail, or in-person. Ideally, the data from the 2004 Michigan Democratic primary would be compared to only Democrats on the state voter file, in order to make inferences about who participated in the 2004 Caucus and who was eligible to participate (since only Democrats were supposed to participate, according to MDP guidelines for voting in the primary, although a small number of self-identified Republicans and independents participated). However, since there is no party affiliation on the state voter file, there is no easy way to determine which voters are Democrats. To account for this, and to simulate a measure of party affiliation, I include a control variable in the model that measures the vote for Gore in 2000 by each voter's state house district (adjusted for the 2002 round of redistricting).

The full state voter file contains close to seven million voters, which was too large a dataset for any computer or statistical package in my department to handle. To overcome the lack of computing power, I generated a random sample of one million voters from the state voter file. Although the accuracy of the analysis might be marginally better if I were able to examine all of the 162,000 voters in the Michigan primary in the context of all eligible or likely voters in the state, a sample of one million is still many times larger than any other similar study of the effects of voting reforms. After merging the turnout data from the 2004 Democratic primary with the sample, there are 16,906 voters in the sample who participated in the 2004 primary. Table 1 includes summary statistics of the sample. The distribution of choice of voting method in the 2004 primary among voters in the sample is similar to the distribution of choice of voting methods among the entire population of primary voters.

| Variable | Frequency | % of sample |
|---|-----------|-------------|
| 2004 Michigan Democratic Primary ¹ | 16,906 | 1.7 |
| In-person | 9,181 | 0.94 |
| Internet | 4,972 | 0.51 |
| Mail | 2,753 | 0.28 |
| Gender ² | | |
| Women | 514,813 | 53.6 |
| Men | 446,590 | 46.4 |
| Age ² | | |
| 18-35 | 296,103 | 30.8 |
| 36-50 | 306,693 | 32.0 |
| 51-65 | 214,634 | 22.3 |
| 66 and over | 139,766 | 14.5 |
| Education ³ | | |
| 0-25% college degree in zip code | 487,500 | 50.71 |
| 26-50% college degree in zip code | 389,583 | 40.52 |
| 51-75% college degree in zip code | 75,963 | 7.90 |
| 76% or more college degree in zip code | 8,444 | 0.88 |
| Race ³ | | |
| 0-25% Black in zip code | 823,502 | 85.66 |
| 26-50% Black in zip code | 34,769 | 3.62 |
| 51-75% Black in zip code | 31,649 | 3.29 |
| 76% or more Black in zip code | 67,603 | 7.03 |

N = 961,403 ⁴

Table 1: Descriptive Statistics for Random Sample of One Million Voters taken from the Michigan Qualified Voter File

¹2004 Michigan Democratic Primary participation data is from the Michigan Democratic Party.

²Gender and age variables are from the Michigan Qualified Voter File.

³Education and race variables are from the 2000 US Census, aggregated at the zip code level and assigned to each voter according to the voter's zip code.

⁴Final sample size is less than one million because some observations were dropped due to missing demographic data.

The individual-level data provided by the Michigan voter file and the MDP include each voter's name, address, zip code, date of birth, gender, voting history in state-run elections, and whether and by what method they participated in the 2004 primary. The demographic variables I am interested in are not easily available at the individual level. As a substitute for individual-level indicators of race, income, and education, I collected Census data aggregated at the zip code level, and assigned a measure to each voter based on their zip code of residence. Although aggregating at the zip code level is not a perfect substitute for individual-level measures, which are often available with survey data, the zip-code level is a relatively small level of aggregation compared to congressional district level or county level that have been used in other studies of voter turnout. The zip-code level has been used regularly in health research [GBN96] and it may also be a particularly good substitute in Michigan, which has been noted for its high level of racial segregation [DK00]. Still, it is important to highlight the point that the measures for race, education, and income in this study are aggregate level measures and should not be interpreted as substitutes for individual-level measures. Future extensions of this research could include Census data at a lower level of aggregation, such as the block level, since the dataset includes each voter's full address. This could add to the validity of the findings on the relationship between demographic characteristics and the use of Internet voting.

Instead of using a duration model to explain the relationship between voting history and the effectiveness of early voting reforms, as Berinsky, Burns and Traugott do [BBT01], this paper operationalizes voting history as a series of dummy variables. Table 2 summarizes the characteristics of each category of voting history.

| | In-Person | Internet | Mail | Abstain |
|--|------------------|-----------------|-------------|----------------|
| Nonvoter (voted in no previous elections since 1998) | 1,079 (61) | 464 (26) | 216 (13) | 423,374 |
| Infrequent voter (voted in 1 general but no primaries) | 7,766 (54) | 4,273 (30) | 2,432 (17) | 402,568 |
| Occasional voter (voted in at least 1 primary) | 6,786 (54) | 3,542 (28) | 2,197 (18) | 239,571 |
| Regular voter (voted in last 3 elections) | 5,733 (54) | 2,986 (28) | 1,943 (18) | 160,342 |
| Absentee voter (voted absentee in at least one election since 1998) | 3,126 (46) | 2,025 (30) | 1,573 (23) | 152,790 |

Source: Vote history is from the Michigan Qualified Voter File and choice of voting method (In-Person, Internet, or Mail) is from the Michigan Democratic Party.

Note: Number in parentheses is the percent of people participating in the 2004 Michigan Democratic Primary who voted by each method.

Table 2: Voting History by Choice of Voting Method in the 2004 Michigan Democratic Presidential Primary

As shown in table 2, a “nonvoter” in this analysis is someone who did not vote in any of the following elections; the 1998 primary and general election, the 2000 primary and general election, and the 2002 primary and general election. An “infrequent” voter is defined as someone who voted in one general election but no primaries. An “occasional” voter is someone who voted in at least one primary election, and a “regular” voter is someone who voted in each of the most previous three elections before the 2004 primary.

The dependent variable in the turnout model is the decision to vote in the 2004 Democratic caucus, either by Internet, mail, in-person on election day, or to abstain. Since it is a categorical dependent variable with no particular order to the categories, multinomial logit is the appropriate estimator. The independent variables of interest are voting history, age, gender, education, income, and race. Based on the findings of Alvarez and Nagler [AN01] I expect to find that as the percentage of white residents increases in a zip code, the likelihood of voting by Internet should also increase. I also expect that as median income and percent of residents with a college degree increases, the percentage of Internet voters should increase. As the age of the voter increases, I expect the likelihood to vote by Internet to decrease and the likelihood to vote by mail to increase.

Based on the findings of Gerber et al [GGS03], I expect regular voters to be more likely to participate in the 2004 primary, and that regular voters will be more likely to vote by early voting methods. Based on the findings of Berinsky, Burns and Traugott [BBT01] I expect to find that either infrequent or occasional voters will be the most likely to take advantage of Internet and mail voting, but that nonvoters will not take advantage of these easy voting methods, either because they are habitual non-voters, because they have not been mobilized by parties or candidates [RH93; OI96], or because they did not have the foresight to apply for an absentee ballot [PS08].

5 Results

| | Entire Random Sample of 1 million voters taken from the Michigan Voter File (N=961,403) | | | | | | Voters in sample who participated in the 2004 Michigan Democratic Primary (N=16,906) | | | |
|--|---|--------|--------------------------------|--------|----------------------------|--------|--|--------|---------------------------|--------|
| | <i>In Person vs. not voting</i> | | <i>Internet vs. not voting</i> | | <i>Mail vs. not voting</i> | | <i>Internet vs. in person</i> | | <i>Mail vs. in person</i> | |
| | | | | | | | | | | |
| Age of Voter ¹ | .023* | (.001) | .013* | (.002) | .041* | (.003) | -.006** | (.003) | .025* | (.004) |
| Median Income ² | -.014* | (.001) | -.003 | (.001) | -.008* | (.001) | .013* | (.001) | .007* | (.002) |
| Percent College Educated ² | .034* | (.002) | .038 | (.001) | .029* | (.004) | .004 | (.003) | -.005 | (.004) |
| Percent Black ² | .003* | (.001) | -.0002 | (.001) | .003 | (.002) | -.003 | (.002) | -.001 | (.002) |
| Female ¹ | -.046** | (.021) | -.146* | (.029) | .138* | (.039) | -.120* | (.036) | .210* | (.045) |
| 2000 Gore Vote ³ | 1.63* | (.103) | 1.72* | (.130) | 1.56* | (.182) | .196 | (.188) | .032 | (.232) |
| Non-voter ⁴ | .476* | (.066) | -.109 | (.083) | .171 | (.125) | -.560* | (.106) | -.482* | (.142) |
| Infrequent voter ⁴ | 2.51* | (.124) | 2.61* | (.169) | 2.01* | (.255) | .719* | (.213) | -.652** | (.304) |
| Occasional voter ⁴ | 1.52* | (.032) | 1.39* | (.038) | 1.56* | (.061) | -.133* | (.051) | .034 | (.069) |
| Regular Voter (suppressed category) ⁴ | | | | | | | | | | |
| Age X infrequent | -.018* | (.002) | -.029* | (.002) | -.017* | (.003) | -.020* | (.003) | .001 | (.004) |
| Education X infrequent | -.008* | (.001) | -.001 | (.002) | .002 | (.004) | .006 | (.003) | .009** | (.004) |
| Black X infrequent | -.008 | (.002) | -.003 | (.001) | -.001 | (.002) | -.004** | (.002) | .000 | (.002) |
| Constant | -.786* | (.089) | -9.22* | (.172) | -11.2* | (.259) | -.759* | (.222) | -2.73* | (.309) |
| Pseudo R ² | 0.126 | | | | | | .048 | | | |

* $p < .01$ ** $p < .05$

Note: 2004 Michigan Democratic Primary participation data is from the Michigan Democratic Party.

Table 3: Likelihood of voting in the 2004 Democratic caucus by Internet, mail, or in-person, compared to not voting – Multinomial Logit Regression Coefficients and Standard Errors

¹Gender and age variables are from the Michigan Qualified Voter File.

²Education and race variables are from the 2000 US Census, aggregated at the zip code level and assigned to each voter according to the voter's zip code.

³2000 Presidential vote by State House District provided by Brian F. Schaffner.

⁴Voting history is from the Michigan Qualified Voter File. "Nonvoter" is someone who did not participate in any elections archived on the voter file since 1998; "Infrequent voter" is someone who participated in one general election but no primaries since 1998; "Occasional voter" is someone who participated in at least one primary election; and "Regular voter" is someone who participated in each of the last three state-wide elections before the 2004 primary.

Table 3 displays the results of two multinomial logit models. The first model includes the entire sample of one million voters; the second includes only the voters in the sample who participated in the 2004 Michigan primary. The first model uses “did not vote” as the base comparison category, since a large majority of voters in the full sample did not participate in the 2004 primary. The second model uses “voted in person” as the base category, since the majority of participants in the 2004 primary voted in person on election day.

In both models, the effects of age, income, gender, and all categories of voting history are significant at the .01 level. The interpretation of the findings that follows will focus on the second model, since I am mostly interested in voters who participated in the 2004 primary. As expected, the median income in a voter’s zip code is significant and positively related to voting early. As income increases, the likelihood of voting early either by Internet or mail increases. The relationship between income and the likelihood of voting by Internet, mail, or in person, holding other variables in the model at their means, is displayed in Figure 1.

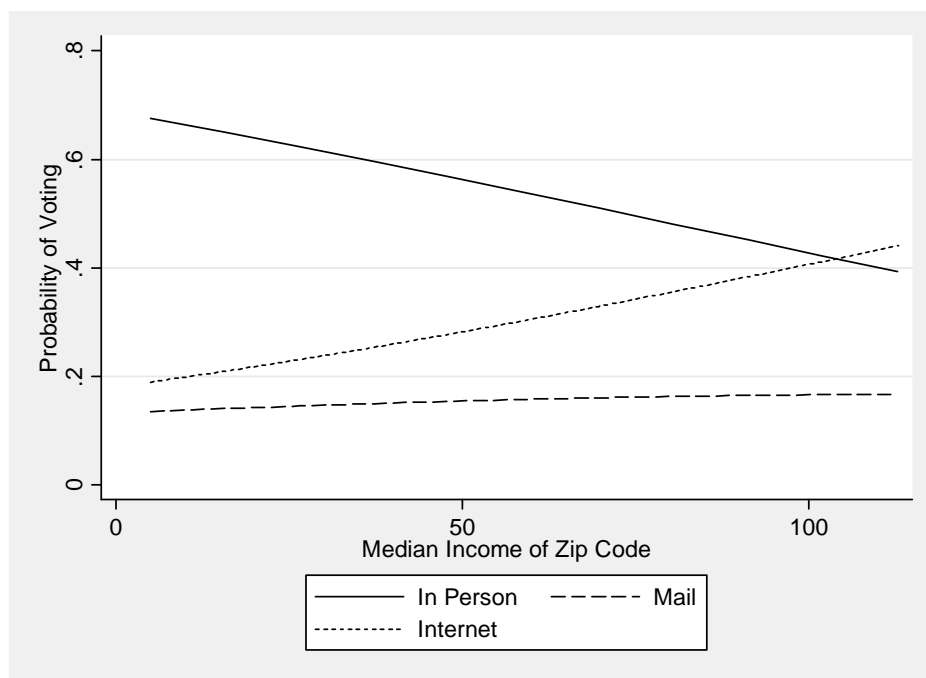


Figure 1: Probability of Voting by Internet, Mail, or In Person by the Median Income in the Voter’s Zip Code

Also as expected, as a voter's age increases, he is more likely to choose voting by mail and less likely to choose Internet voting. This result is shown in Figure 2. As a voter's age increases, the likelihood of choosing to vote by mail increases substantially, while the likelihood of voting by Internet or in person decreases at a more gradual rate. The effect of age on the likelihood to vote by Internet may not be surprising to young people, who are probably the most comfortable out any age group with using the Internet, but it is important for the study of early voting reforms. Other studies of early voting reforms, especially voting by mail, have found that older voters are more likely to benefit from early voting reforms. This research shows that young voters benefit from the option to vote on the Internet.

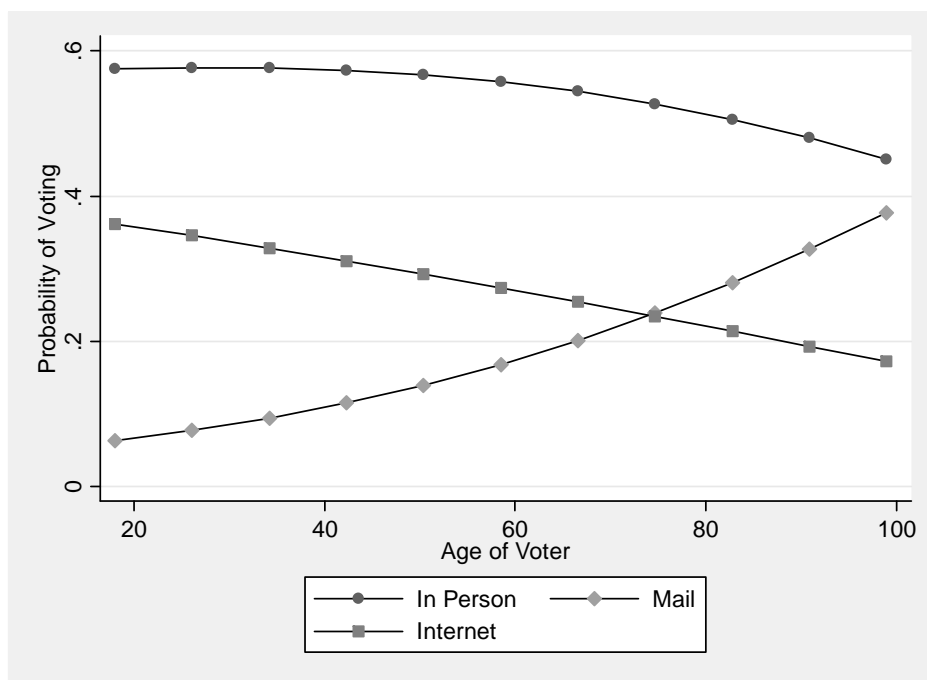


Figure 2: Probability of Voting by Internet, Mail, or In-Person by Age of Voter

The dummy variables for nonvoter, infrequent voter, and occasional voter are statistically significant at the .01 level in both models (regular voter is the suppressed category). As expected, being designated as a “nonvoter” was strongly and negatively related to voting on the Internet or by mail in the second model. Being an “infrequent” voter (one who voted in one general election but no primaries) was strongly and positively related to voting on the Internet, but strongly and negatively related to voting by mail, when controlling for other factors in the model. On the other hand, being an “occasional” voter (one who had voted in at least one primary) was positively related to voting by mail but negatively related to voting by Internet, controlling for other factors in the model. These findings are similar to those of Berinsky, Burns, and Traugott [BBT01], who found that individuals who voted sporadically were more likely to benefit from Oregon’s vote-by-mail program. This model goes further to show that there is a difference between levels of frequency of voting. Infrequent voters were more likely to benefit from Internet voting, but occasional voters were more likely to benefit from mail voting. Figure 3 shows the predicted probabilities across the different categories of vote history for low and high values of a voter’s age.

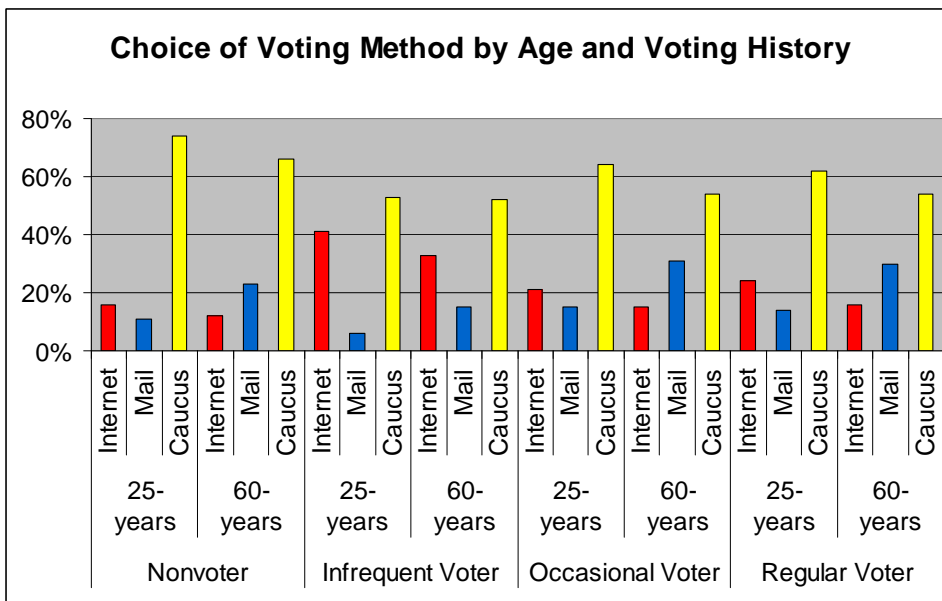


Figure 3: Predicting Choice of Voting Method for Voters Who Participated in the 2004 Michigan Democratic Primary, by Voter’s Age and Individual Voting History

Younger voters in almost every category of voting history were more likely than older voters to choose Internet voting, and older voters were more likely to choose mail voting in almost every category. The only category in which both younger and older voters were more likely to choose Internet voting was for infrequent voters. For infrequent voters, 25 year olds were 41% likely to vote on the Internet and only 6% likely to vote by mail, and 60 year olds were 33% likely to vote by Internet and 15% likely to vote by mail. Although I expected to find that young voters would be more likely to choose Internet voting, I did not expect older voters to choose Internet voting over mail voting. This unexpected finding suggests that for future applications of this research, the composition of the voting history categories should be tested for robustness. The limits of time and computing power prevented this research from testing any additional models. It is also clear from Figure 2 that voting in person was the most popular choice across all categories of age and voting history, and that nonvoters – those who had not participated in any previous elections since 1998 – were the most likely to vote in person on election day.

Two of the variables of interest, race and education, are not significant in the second model. In the first model, education is significant for the decision to vote in person versus not voting, but it is not significant for the choice to vote by Internet versus not voting. Race is only significant in the first model for the decision to vote in person versus not voting, but the effect is small. Both variables reach significance when they are interacted with voting history, which suggests that it is the combination of voting history and these demographic variables that has an effect on voting choice, but even here the effect is small. An infrequent voter living in a zip code that is 80% black has a 34% likelihood of voting on the Internet and a 13% likelihood of voting by mail, compared to an infrequent voter living in a zip code that is 20% black who is just one percentage point more likely to vote on the Internet and has the same likelihood of voting by mail.

6 Conclusion

This research shows that Internet voting as an early voting reform helps bring two groups into the electorate who might not otherwise have voted: young people and people who were infrequent voters. These findings are important for policy makers and election administrators to consider when evaluating new voting reforms, since they provide evidence that Internet voting can be effective at bringing young voters into the electorate. They are also important in light of the recent research on voting reforms, which have been almost unanimous in their findings that no new groups of voters are drawn into the electorate.

Since voting history has been shown to be an important predictor of future voting behavior, new studies of the effects of voting reforms on individual voters must include information about voting history. State voter registration files should be utilized by political scientists, as they are used by political professionals, to inform predictions and explanations about voting behavior and the effects of early voting reforms. The Help America Vote Act of 2002 has helped states streamline their voter registration databases, and these advances should aid political scientists in obtaining state voting archives that are suitable for research purposes.

Several state legislatures have proposed an expansion of no-excuse absentee mail programs, and some states are even considering adoption of all vote-by-mail systems like Oregon's. According to electiononline.org, a non-partisan election reform advocacy organization, there is legislation currently pending in 19 states to expand mail absentee voting programs. This research suggests that states should also consider implementing Internet voting as an absentee voting method, if the goal of reformers is to encourage voting among young people. This research also suggests that a switch to all mail voting programs could actually decrease turnout among young voters.

Of course there are many concerns about Internet voting that are not addressed in this paper, including security concerns that some scholars suggest are insurmountable in large-turnout public elections [Ca00]. However, I believe the implications for young voters are so important that more experiments with Internet voting as an early voting method should be tried. Alvarez and Hall agree that more controlled experiments with Internet voting should be designed and implemented in order to learn more about the effects on turnout among demographic groups and the potential security risks [AH04]. As an early voting method, Internet voting can be implemented in a way that is very similar to a traditional absentee ballot, as it was in the 2004 Michigan primary. The important distinction for young voters is that instead of going to a post office, voters go to a website to vote, and in this election that seems to have made a difference.

Appendix

Dependent Variable

Participation in the 2004 Michigan 4 categories, coded:

Democratic Presidential Primary 0 = Did not vote

1 = Voted in person

2 = Voted by Internet

3 = Voted by Mail

Explanatory Variables

Age Voter's age in years, taken from the birth year listed on the Michigan Qualified Voter File.

Gender Coded 0 for Male and 1 for Female, taken from the Michigan Voter File.

Income Median income in the voter's zip code of residence, in thousands, taken from the 2000 Census.

Education Percent college educated in the voter's zip code of residence, taken from the 2000 Census.

Race Percent African American in the voter's zip code of residence, taken from the 2000 Census.

Zip Code Voter's zip code of residence.

2000 Gore vote: Percent of the vote for Al Gore in 2000 by State House district, adjusted for the 2002 state legislative redistricting, provided by Brian F. Schaffner of American University.

Vote History Variables

Vote history data is from the Michigan Qualified Voter File and includes information for the following elections: 1998 primary and general, 2000 primary and general, 2002 primary and general.

Nonvoter: Coded 1 for individuals who did not participate in any of the elections taken from the state voter file; coded 0 otherwise.

Infrequent voter Coded 1 for individuals who participated in at least 1 general election but no primaries; coded 0 otherwise.

Occasional voter Coded 1 for individuals who participated in at least 1 primary election; coded 0 otherwise.

Regular voter Coded 1 for individuals who participated in all of the last 3 elections (the 2002 general and primary and the 2000 general); coded 0 otherwise.

References

- [AH04] Alvarez, R. M.; Hall, T.: *Point, Click, and Vote: The Future of Internet Voting*. Washington, DC: Brookings Institution Press, 2004.
- [AN01] Alvarez, R. M.; Nagler, J.: The Likely Consequences of Internet Voting for Political Representation. *Loyola Law Review*, 34, 2001; pp.1115-1153.
- [Be05] Berinsky, A.: The Perverse Consequences of Electoral Reform in the United States. *American Politics Research* 33, 2005; pp. 471-491.
- [BBT01] Berinsky, A.; Burns, N.; Traugott, M.: Who Votes By Mail? A Dynamic Model of the Individual Level Consequences of Voting-By-Mail Systems. *Public Opinion Quarterly* 65, 2001; pp.178-197.
- [Ca00] California Internet Voting Task Force Report: 2000. Retrieved on May 1, 2008, from <http://www.sos.ca.gov/executive/ivote/>
- [DK00] Darden, J.; Kamel, S.: Black Residential Segregation in the City and Suburbs of Detroit: Does Socioeconomic Status Matter? *Journal of Urban Affairs* 22, 2000; pp. 1-13.
- [GGS03] Gerber, A.; Green, D.; Shachar, R.: Voting May Be Habit-Forming: Evidence from a Randomized Field Experiment. *American Journal of Political Science* 47, 2003; pp. 540-550.
- [GBN96] Geronimus, A.; Bound, J.; Neidert, L.: On the Validity of Using Census Geocode Characteristics to Proxy Individual Socioeconomic Characteristics. *Journal of the American Statistical Association* 91, 1996; pp. 529-537.
- [Gi02] Gibson, R.: Elections Online: Assessing Internet Voting in Light of the Arizona Democratic Primary. *Political Science Quarterly* 116, 2002; pp. 561-583.
- [Gr04] Gronke, P.: Early Voting Reforms and American Elections. Paper presented at the 2004 Annual Meeting of the American Political Science Association.
- [NR01] Neeley, G.; Richardson, L.: Who is Early Voting? An Individual Level Examination. *The Social Science Journal* 38, 2001; pp. 381-392.
- [OI96] Oliver, E.: The Effects of Eligibility Restrictions and Party Activity on Absentee Voting and Overall Turnout." *American Journal of Political Science*, 40, 1996; pp. 498-513.
- [PI02] Plutzer, E.: Becoming a Habitual Voter: Inertia, Re-sources, and Growth in Young Adulthood. *American Political Science Review* 96, 2002; pp. 41-56.
- [PS08] Prevost, A.; Schaffner, B.: Digital Divide or Just Another Absentee Ballot? Evaluating Internet Voting in the 2004 Michigan Democratic Primary." *American Politics Review*, forthcoming, 2008.
- [RH93] Rosenstone, S.; Hansen, J.: *Mobilization, Participation, and Democracy in America*. New York: MacMillan Publishing Company, 1993.
- [So04] Solop, F.: Digital Democracy Comes of Age: Internet Voting and the 2000 Arizona Democratic Primary Election. *PS: Political Science and Politics* 34, 2001; pp. 289-293.
- [SG97] Stein, R.; Garcia-Monet. P.: Voting Early but Not Often. *Social Science Quarterly* 78, 1997; pp. 657-671.
- [TK79] Traugott, M.; Katosh, J.: Response Validity in Surveys of Voting Behavior. *Public Opinion Quarterly* 43, 1979; pp. 359-377
- [Tr04] Traugott, M.: Why Electoral Reform Has Failed: If You Build It, Will They Come?" In (A.N. Crigler, M. R. Just, and E. McCaffery): *Rethinking the Vote: The Politics and Prospects of American Election Reform*. New York" Oxford University Press.

Session 3: Legal & Procedural Issues of E-Voting

A Methodology for Assessing Procedural Security: A Case Study in E-Voting

Komminist Weldemariam^{1,2}, Adolfo Villafiorita¹

¹Fondazione Bruno Kessler
Center for Scientific and Technological Research (fbk-irst)
Sommarive 18 I-38050 Povo (TN) – Italy
[_{sisai|adolfo}@fbk.eu](mailto:{sisai|adolfo}@fbk.eu)

²DISI, University of Trento
Sommarive 14 I-38100 Povo (TN) – Italy
weldemar@disi.unitn.it

Abstract: This paper presents a methodology for procedural security analysis in order to analyze and eventually try to make elections more secure. Our approach is based on modelling the electoral procedures in the form of business process models (which we write in a strict simplified subset of UML), systematically translate the models into executable formal specifications, and analyze the specifications against security properties. We believe such an analysis to be essential to identifying the limits of the current procedures (i.e. undetected attacks) and to identify more precisely under what hypotheses we can guarantee secure elections. This paper presents the approach and demonstrates with an example taken from the e-Voting procedures enacted within the ProVotE project, current trial of the Italian legislation.

1 Introduction

The organization of elections in Italy involves various offices of the Public Administration and private contractors, has a time-span of months, and has strict security and traceability requirements. Sensibility by citizens and politicians is very high, and litigation over, e.g., implementation of procedures and validity of results are not uncommon. The Autonomous Province of Trento who has autonomy over local election is evaluating the switch to e-voting and, to that extent, is sponsoring the ProVotE project [VF06].

The switch to electronic elections in Italy, however, is a long and difficult process that requires extreme attention, including a thorough understanding of the limits of the risks associated to the procedures or to the combination of the procedures and systems chosen for voting. (See, e.g., [ALRL04; Mya05; FM06; MFMP07; BLRS06; LKK+03; Ale04] for a discussion of security risks associated to the usage of ICT systems and elections.)

We are approaching the problem by reasoning about the procedures and controls that regulate the usage of e-voting systems. We do so by providing formal models of the procedures, by "injecting" threats in such models and by analyzing, through the help of model checker, the effects of such threats. We believe such an analysis to be essential to, first, identifying the security boundaries— that is the conditions under which procedures can be carried out securely and, secondly, devise a set of requirements, to be applied both at the organizational level and on the (software) systems used to make systems and system processes secure. In particular, the violation of security properties could provide clues about a sequence of actions that an adversary uses to construct attacks before or during the execution of procedures.

The main contribution of this paper is twofold. On one hand we are tackling the problem at the procedural level —namely, we are trying to understand weaknesses and strengths of the procedures regulating an election, in order to analyze possible attacks and their effects on the electoral system, and, more specifically, possible attacks and threats that can be realistically carried out on the e-voting machines. On the other hand, we are interested in devising techniques and tools to analyze security threats at the organizational/procedural level, and eventually make comparison between as-is and to-be election system procedures.

This paper refines and extends the work presented in [WVM07], and it is structured as follows. In the next chapter we explain the ProVotE project scopes under which this work has been developed. In Chapter 3, we describe the context of procedural security in detail. In Chapter 4, we describe our methodology for procedural security analysis and illustrate the approach with an example in Chapter 5. Finally, in Chapter 6, conclusions drawn from this work are discussed.

2 The ProVotE Project and Motivations

ProVotE [VF06], a project sponsored by Provincia Autonoma di Trento (PAT), has the goal of ensuring a smooth transition to e-voting in Trentino, eliminating risks of digital divide and providing technological solutions which support, with legal value, the phases ranging from voting to the publication of the elected candidates.

The project includes partners from the public administration (PAT, Regione Trentino/Alto-Adige, Consorzio dei Comuni Trentini, Comune di Trento, IPRASE), research centers and academia (FBK, Faculty of Sociology of the University of Trento, Fondazione Graphitech), and local industries (Informatica Trentina). The technological solution (both software and some hardware components) has been developed in house, providing integration with some commercial components.

The project is multi-phased and is organized in various lines of activities that strictly interact (see also [VF06; CBF+06] for more details).

The first phase had the goal of testing prototypes, evaluating acceptance by citizens, ease of use, and some organizational aspects. Verification of the results achieved in the first phase was conducted through four different trials (between 2005 and 2006) held during local elections. Participation to the first phase has been quite high: about 10,000 citizens took part in the experimentation³⁰.

During the second phase of the project we used the electronic systems in two elections, with legal value. The first election was the election of student representatives in a local high school and it involved 1,298 students. The second election — conducted in the towns of Campolongo al Torre and Tapogliano in Friuli-Venezia Giulia (November 2007), a neighboring region with autonomy similar to that of PAT — was a poll to unify the two municipalities; 561 people used the system.

For the third phase of the project, which could lead to a large-scale introduction of the new voting system, aspects related to procedures, logistics, and organization become more relevant, as they will serve both as the basis for the deployment of the solution and for the definition of the laws that will govern the electronic election.

With respect to scope, population, and participation, ProVotE is among the largest, if not the largest, e-voting project in Italy.

3 The Context of Procedural Security Analysis

Procedural security deals with the identification, modelling, establishment, and enforcement of security policies about the procedures that regulate the usage of a system and system processes.

The situation is depicted in Figure 1. *Our target of evaluation* is a complex organization setting in which procedures transform and elaborate *assets*, which may not necessarily be just digital assets (like, e.g., paper documents are also sensitive assets). The procedures and the organization are meant to add value to the assets and high desire to protect them from attacks, which can either come from external sources or from insiders.

³⁰ Detailed results of all the experimentations and elections conducted within the ProVotE project are available on the Internet at: <http://www.provincia.tn.it/elezioni> and <http://referendum2007.regione.fvg.it/index.html>.

In particular, we distinguish the following kind of attacks:

1. *Attacks on digital assets* (item 1 and item 3 in Figure 1). These attacks are meant to alter one or more of the digital assets of an organization. Attacks can either be carried out from external sources (the environment) or from internal sources. Opportunities for attacks are determined by the organizational setting and by the security provided by the digital systems.

2. *Attacks on other kinds of assets* (item 2 and item 4 in Figure 1). These attacks are meant to alter one or more of the non-digital assets of an organization. Attacks can either be carried out from external sources (the environment) or from internal sources. Opportunities for attacks are determined by the organizational settings only.

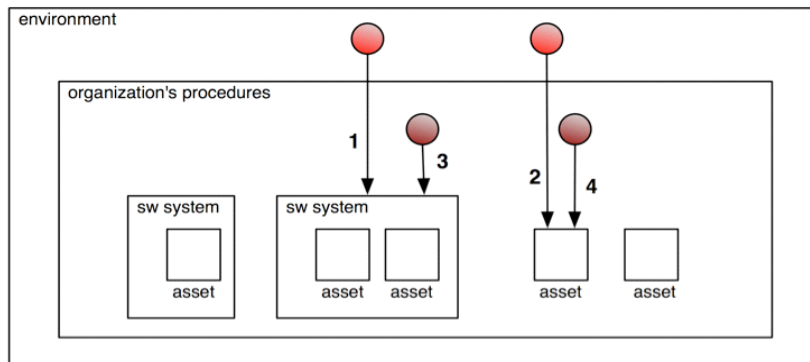


Figure 1: Procedural security Analysis.

Security assessment usually focuses on understanding items 1 and 3, namely, types and effects of attacks on (software) systems. In order to address the scenario depicted above in a systematic and tool-supported way, we *lift* the security assessment at the organizational level and we call *procedural security* analysis the usage of techniques and tools to understand the impact and effects of *procedural threats*, namely courses of actions that can take place during the execution of the procedures and which are meant to alter the assets manipulated by procedures in an unlawful way.

4 A Methodology for Procedural Security Analysis

We developed a precise methodology to perform formal procedural security analysis, based on the following steps (see also Figure 2):

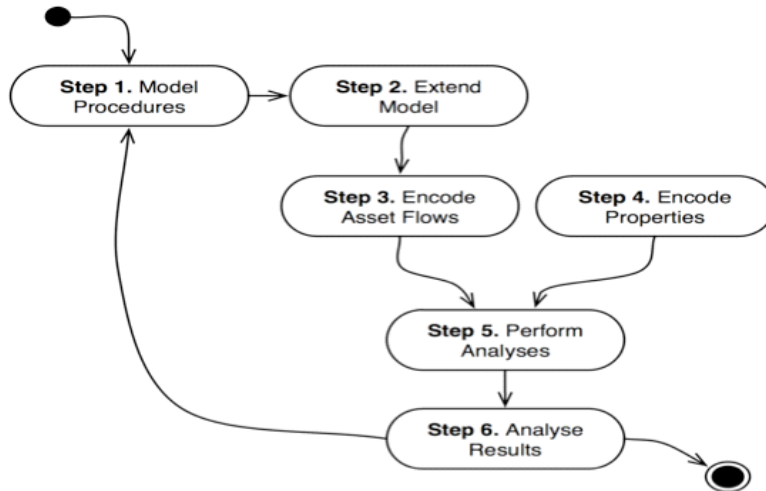


Figure 2: The process of formal procedural security.

1. ***Provide (business) models of the procedures under evaluation.*** The starting point is a model that describes the process or the processes to be analyzed (Step 1 of Figure 2). In order to ease the task of translating the models into executable asset-flows, we defined and stuck to a subset of the UML activity diagrams. This allows us to describe the concepts like asset, processes, and accessory information (such as, location) in a strict and defined way. So far we managed to provide UML models of the electoral procedures in place in the Autonomous Province of Trento and in Regione Friuli Venezia Giulia. We use Visual Paradigm³¹ as our reference-modelling tool. See some previous works [Man03; Mat06; Cia07] for more details about the notation, tool support, and the model themselves.

³¹ <http://www.visual-paradigm.com/>

2. **Inject Threat actions into the model.** We generate, from the models defined at the previous step, what we call *extended model* (Step 2 of Figure 2). The extended model is generated by “injecting” asset-threats in the nominal flow of the procedures. Thus, in the extended model, not only assets are modified according to what the procedures define, but they can also be transformed by the (random) execution of one or more threat actions. The possible impact of threats depends upon the injection strategy that is chosen. The most general strategy is that of injecting all possible threats at all possible steps of the process (the model checker will take care of “pruning” useless threats, namely threats which do not lead to any successful attack). The construction of the extended model, whose generation can be automated, is currently performed by hand.

3. **Encode the Asset Flows.** From the extended models defined at the previous step we derive the asset flows of each asset manipulated by the procedures (Step 3 of Figure 2). Asset flows are represented in the NuSMV input language. The NuSMV model of the asset flows is based on the definition of “program counters” that ensure that procedures are executed according to the specifications, and by defining one module per asset with one state variable per asset-feature. The state variables encode how features change during the execution of the procedures. Accessory information, such as actors responsible for the different activities, can be used, e.g., to enrich the language used to express security properties. The necessity of modelling actors’ roles in NuSMV depends upon the target of the security analysis. Note that from the list of activities executed to carry out, e.g., an attack, we can derive the list of actors involved, simply by looking at the UML activity diagrams.

4. **Specify Security Properties to Check.** The specifications of the desired (procedural) security properties, namely, the security goals that have to be satisfied, are then encoded using LTL/CTL formulas (Step 4 of Figure 2), which then (together with the model) are given as input to NuSMV.

5. **Perform Analysis.** We finally run the model checker to perform the analyses (Step 5 of Figure 2). Counterexamples of security properties encode the sequence of actions that have to be executed in order to carry out an attack on an asset.

6. **Analyze Results.** The last step is analyzing the obtained results (Step 6 of Figure 2). Counterexamples are used to achieve the following two goals. First, they allow to understand what are the hypotheses and conditions under which a given security goal is achieved or breached. Second, they provide information to try and modify the existing procedures, so that security breaches are taken care of. Analogously to what happens in safety analysis when analyzing, e.g., the loss of critical functions, enhancing the procedures results in reducing the probability of an attack or making the attack more complex, rather than eliminating it [Mar07].

5 A Case Study Example

Modelling Asset-flow, Step 1. Figure 3 shows a fragment of the procedure that is followed during project trials for the transfer of election results from polling stations to Electoral Office. The diagram abstracts away those details that are irrelevant for the sake of presentation, e.g. details related to the alternative modelling choices for carrying out the data transfer process are omitted. We also hide some actors' responsibilities by collapsing, e.g. Secretary, Scrutinizers, them into a single actor. See in [Vol07] for detail strategies of data transfer process and how the alternative choices are modelled.

The diagram illustrates (see Figure 3), after the election, the Section President (one of the Poll Officers) deactivates the voting machines, extracts (from the voting machine) printed votes, the USB key with the results, and other artifacts, and prepares a package containing votes and various reports, to be delivered to the Electoral Office. Electronic data are transmitted through a VPN and the USB key with the electronic results delivered to the Electoral office via a “messenger” (e.g. a police officer).

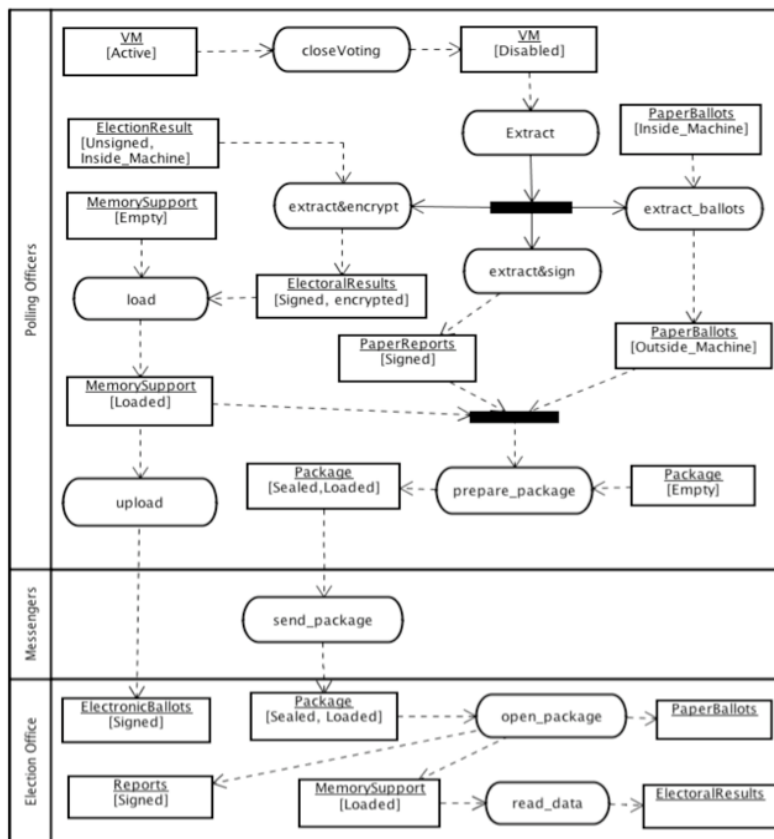


Figure 3: An example of asset flow.

Threat Injection, Step 2. The next step is *injecting*, that is, extending the model with threat actions and generate the *extended model*. Figure 4 shows some examples of threat-actions injected into the nominal model of Figure 3. In the extended model, threat actions are marked with the stereotype “threat-action”. Impact of the attacks depend upon the asset they target and the position, in the procedure, where the attack take place.

For instance, replacing the results of a polling station in a USB key has no effect after the result have been generated. (On the other hand it may change the results of the election if performed before the results have been computed.)

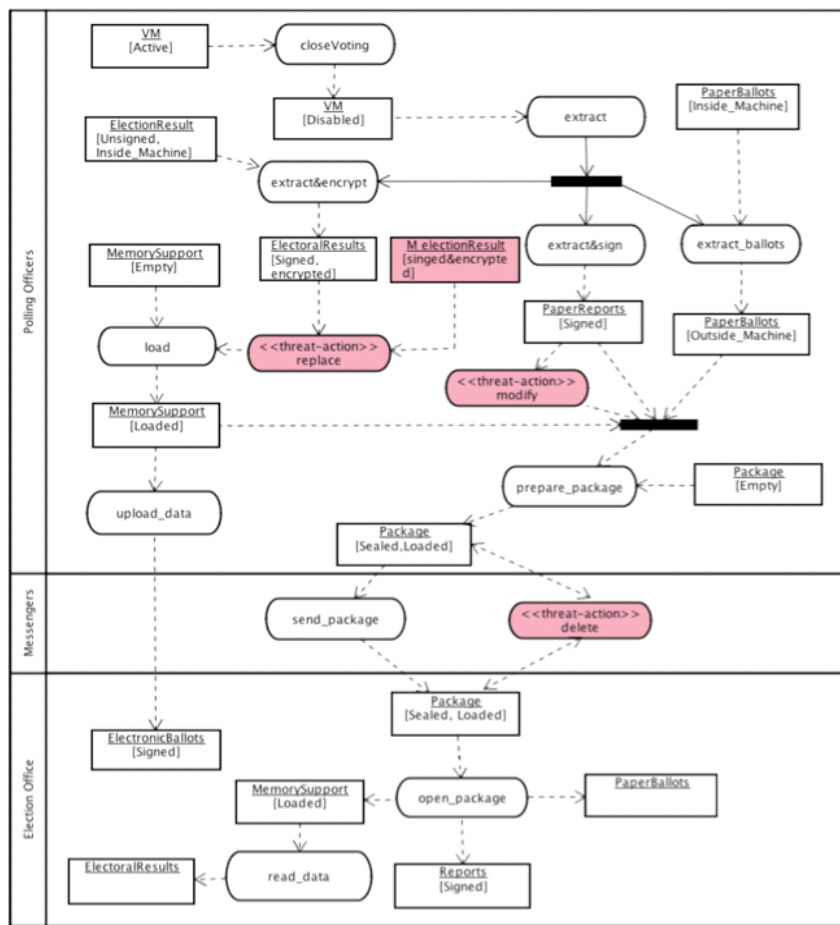


Figure 4: An example of extended model.

Asset-Flow encoding, Step 3. Below we show a snippet of the code that defines the asset type *electionResult* and some of its feature variables, named *state* (the states in which the *electionResult* can be) and the content (the qualitative value of the *electionResult* can be).

```
MODULE electionResult ( ... )
VAR
state    : {plain,unsigned,signed,signed_&_encrypted};
content  : {null,data,signed_&_encrypted_data,garbage};
```

The evolution of assets' properties is encoded using state machines, which are encoded in NuSMV with the *next* construct (which specifies the value of a variable at step $n+1$, given the value at step n). Below, for instance, we show a piece of NuSMV code that illustrates how the content variable of *electionResult* asset changes:

```
init(content) := null;
next(content) := case
pc.pc = closeVoting && next(pc.pc) = extract_&_encrypt : data;
content = data && pc.pc = extract_&_encrypt && state = signed: signed_&_encrypted_data;
[...]
```

Threat injection (model extension) corresponds to augmenting the state machine of the asset flow with new transitions (e.g., adding a transition that leads to a *garbage* state of *content*) corresponding to the execution of threat actions. The triggering of a threat action is "monitored" through boolean variables that are set to true when the action takes place, as illustrate by the following pieces of code:

```
next(can_malElectionRes) := case
(malElectionRes && pc.mpc = replaceElectionRes &&
next(electionResult.content) = malEnSignedData) || [...] :1;
1: can_malElectionRes;
esac;
```

Note that in the codes above we have left some detail specification (such as location) for the matter of presentation purposes. Analogously, the remaining asset flows and model extension encodings can be encoded.

Specify Security Properties and Perform Analysis, Step 4 & 5. We use temporal logic formulas to represent the properties of interest and model check them using the NuSMV tool. In particular, security properties are specified using LTL/CTL logic language. LTL is used to reason on the computational path scenarios of an asset (e.g., what can happen as asset travels along different locations), while CTL to reason about the existence of specific states (e.g., is there any particular state in which an asset can be altered in an undesired way).

Among the property classes we are interested in is that of verifying a property about "*Safe transfer of election result.*" A desirable property, for instance, that we want to specify and analyze can be described in plain text as: "*It is never the case that election officials receive modified election data before computing the final result.*" This property is expressed in CTL formula as:

```
AG !(ElectionResult.can_garbage && ElectionResult.location = electoralOffice)
```

We give the above property to NuSMV tool to check that the property holds. However, the tool generates a counter-example showing the violation of the given property. Upon analyzing the generated counter-example, the election result is replaced (i.e., a replace attack is in place) following the introduction of a wrong election data into the asset flow, which, in turn, causes wrong delivery of election result to the electoral office. Among the possible scenarios that we analyzed, at some time a malicious election data is introduced while poll officer is preparing the data to transfer to electoral office. At the same time, an attacker implements replace attack before loading the memory support.

6 Related Work

Various approaches (for specifying, modelling, analyzing, and assessing security) have been proposed in the past and proven useful for zeroing the security lacks of the analyzed systems (see, for instance, [FM06; BDL+03; VWW06; Wim05]).

To our knowledge, however, formal procedural security analysis is quite an un-explored area. The work closest in spirit to ours can be found in [XM04, XM05], where the authors argue the need for procedural security in electronic elections and provide various examples of procedural risks occurred during trials in the UK; in [LKK+03, XM06] where the authors highlight the importance of defining roles and responsibilities in e-voting and in [Ale05] where the need for applying business process re-engineering to the electoral process is emphasized. Our focus, however, is on the technical machinery to automate analyses.

Volha et al. [Vol07] presents an approach to reason on security properties of the to-be models (which are derived from *as-is* model) in order to evaluate procedural alternatives in e-voting systems using Tropos.

Finally, Alexander et al. in [PKKU04] also highlighted a comprehensive way of overviewing attacks against sensible assets in all stages of e-voting.

7 Conclusion

In this paper we presented a methodology to perform procedural security analysis based on explicit reasoning on asset-flows — notably, by building a model to describe the nominal procedures implementation, enriching this model with possible threat actions, and encoding the extended model to suit for model checking techniques which, in turn, allows to reason on different aspects of the procedures such as, the "actor-play-role" principle and some reachability analysis for some undesired state of an asset. Among the advantages of our approach, the possibility of getting a better comprehension of the effect and impact of combined attacks to the assets of an election.

The model checker runs that were made on the current version of the specification have not revealed much interesting results though seemed useful; therefore, much work needs to be done in order to see if the model can be fully verified or if any interesting results can be uncovered. Moreover, we need to consolidate our approach and provide guidelines that can be incorporated in the Common Criteria [cc07], both methodologically and in a tool supported way to automate the analysis.

References

- [Ale04] Alexandros Xenakis and Ann Macintosh. Levels of Difficulty in Introducing e-Voting. *Electronic Government*, 3183/2004, November 05 2004. LNCS, Springer.
- [Ale05] Alexandros Xenakis and Ann Macintosh. Using Business Process Re-engineering (BPR) for the Effective Administration of Electronic Voting. *The Electronic Journal of e-Government*, 3(2), 2005.
- [ALRL04] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*, 01(1):11–33, 2004.
- [BCP+02] P. Bertoli, A. Cimatti, M. Pistore, M. Roveri, and P. Traverso. NuSMV 2: An Open Source Tool for Symbolic Model Checking. In *Proceeding of International Conference on Computer-Aided Verification*, 2002.
- [BDL+03] David Basin, Jürgen Doser, and Torsten Lodderstedt. Model Driven Security for Process-Oriented Systems. In *SACMAT '03: Proceedings of the eighth ACM symposium on Access control models and technologies*, pages 100–109, New York, NY, USA, 2003. ACM.
- [BLRS06] J W. Bryans, B Littlewood, P Y. A. Ryan, and L Strigini. E-Voting: Dependability Requirements and Design for Dependability. *ARES '06: Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)*, 0:988–995, 2006.
- [CBF+06] Letizia Caporusso, Carlo Buzzi, Giolo Fele, Pierangelo Peri, and Francesca Sartori. Transition to Electronic Voting and Citizen Participation. In Robert Krimmer, editor, *Electronic Voting*, volume 86 of LNI, pages 191–200. GI, 2006.
- [cc07] Common Criteria. 2007. <http://www.commoncriteriaportal.org/>.
- [Cia07] Aaron Ciaghi. From Laws to Models: Tools and Methodologies. Master's thesis, University of Trento, Italy, 2006-2007. In Italian.

- [FM06] Igor Nai Fovino and Marcelo Masera. Through the Description of Attacks: A Multidimensional View. In *Computer Safety, Reliability, and Security*, 25th International Conference, SAFECOMP 2006, Gdansk, Poland, September 27-29, 2006, Proceedings, pages 15–28, 2006.
- [LKK+03] Costas Lambrinouidakis, Spyros Kokolakis, Maria Karyda, Vasilis Tsoumas, Dimitris Gritzalis, and Sokratis Katsikas. Electronic Voting Systems: Security Implications of the Administrative Workflow. In *DEXA '03: Proceedings of the 14th International Workshop on Database and Expert Systems Applications*, page 467, Washington, DC, USA, 2003. IEEE Computer Society.
- [Man03] Andrea Mattioli. From Processes to Information Systems: Tools for Sharing Models. Master's thesis, University of Trento, Italy, 2002-2003. (In Italian)
- [Mar07] Marco Bozzano and Adolfo Villafiorita. The FSAP/NuSMV-SASafetyAnalysisPlatform. *Int. J. Software Tools Technology Transfer*, 9(1):5–24, 2007.
- [Mat06] Andrea Mattioli. Analysis of Processes in the Context of Electronic Election. Master's thesis, University of Trento, Italy, 2005-2006. (In Italian)
- [MFMP07] Daniel Mellado, Eduardo Fernández-Medina, and Mario Piattini. A Common Criteria Based Security Requirements Engineering Process for the Development of Secure Information Systems. *Comput. Stand. Interfaces*, 29(2):244–253, 2007.
- [Mya05] Myagmar, S. and Lee, A. and Yurcik, W. Threat Modelling as a Basis for Security Requirements. In *StorageSS '05: Proceedings of the 2005 ACM workshop on Storage security and survivability*, pages 94–102., New York, NY, USA, 2005. ACM Press.
- [PKKU04] Alexander Prosser, Robert Kofler, Robert Krimmer, and Martin Karl Unger. Security Assets in E-Voting. In *Electronic Voting in Europe*, pages 171–180, 2004.
- [VF06] Adolfo Villafiorita and Giorgia Fasanelli. Transitioning to e-Voting: the ProVote Project and the Trentino's Experience. In *EGOV-06*, Krakow, Poland, 2006.
- [Vol07] Volha Bryl, Fabiano Dalpiaz, Roberta Ferrario, Andrea Mattioli and Adolfo Villafiorita. Evaluating Procedural Alternatives. A Case Study in e-Voting. *Proceedings of MET-TEG07*, 2007. An extended version has been published as a Technical Report DIT-07- 005, Informatica e Telecomunicazioni, University of Trento.
- [VWW06] Monika Vetterling, Guido Wimmel, and Alexander Wisspeintner. A Graphical Approach to Risk Identification, Motivated by Empirical Investigations. *Lecture Notes in Computer Science*, pages 574–588, Thursday, November 23 2006.
- [Wim05] Guido Oliver Wimmel. Model-Based Development of Security-Critical Systems. PhD thesis, German umlauts Institut für Informatik der Technischen Universität München, February 2005.
- [WVM07] Komminist Weldemariam, Adolfo Villafiorita, and Andrea Mattioli. Assessing Procedural Risks and Threats in e-Voting: Challenges and an Approach. In Ammar Alkassar and Melanie Volkamer, editors, *VOTE-ID*, volume 4896 of *Lecture Notes in Computer Science*, pages 38–49. Springer, 2007.
- [XM04] Alexandros Xenakis and Ann Macintosh. Procedural Security Analysis of Electronic Voting. In *ICEC '04: Proceedings of the 6th international conference on Electronic commerce*, pages 541–546, New York, NY, USA, 2004. ACM Press.
- [XM05] Alexandros Xenakis and Ann Macintosh. Procedural Security and Social Acceptance in E-Voting. In *HICSS '05: Proceedings of the Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) - Track 5*, page 118.1, Washington, DC, USA, 2005. IEEE Computer Society.
- [XM06] Alexandros Xenakis and Ann Macintosh. A Generic Re-engineering Methodology for the Organized Redesign of the Electoral Process to an E-electoral Process. In *Electronic Voting*, pages 119–130, 2006.

Secure Remote Voter Registration

Victor Morales-Rocha¹, Jordi Puiggali¹, Miguel Soriano²

¹Scytl Secure Electronic Voting
Tuset 20 1-7 Barcelona, Spain
[_{victor.morales|jordi.puiggali}@scytl.com](mailto:{victor.morales|jordi.puiggali}@scytl.com)

²Technical University of Catalonia
Department of Telematics Engineering
Jordi Girona 1-3 Barcelona, Spain
soriano@entel.upc.edu

Abstract: Voter registration is an important issue in election processes. In order to protect the election accuracy, it is necessary to have an accurate electoral roll of eligible voters. The electoral roll is usually constructed by means of a voter registration system that compiles voter data either in person or remotely. Current solutions for remote voter registration lack effective methods to prevent impersonation, multiple registrations and alterations on voter information. In this paper we propose a remote voter registration scheme that increases the accuracy of the current systems. In this scheme the voter identification is carried out by means of some biometric systems. Biometrics is also used to prevent impersonation, detect multiple registrations from the same person and protect from alterations of the registration information.

1 Introduction

Lately, there has been an increasing interest to improve the efficiency in the election processes, which has resulted in a wide range of proposals for new election systems. Most of the proposals have been focused in voting and tallying stages, giving least interest to voter registration stage.

Voter registration is the process of collecting the voters' data in order to constitute an electoral roll. Because of the fact that the electoral roll determines if a voter has the right to cast a vote during the voting stage, it has to be formed in an efficient way. Even when voting and tallying stages have the greatest security level, a deficient voter registration system can facilitate fraud practices that can even affect the accuracy of the election.

Voter registration is conventionally carried out face to face with the registration authority. However, since many voters are residing abroad during an election process, it has been necessary to have new methods to collect, remotely and in a secure manner, the information of such voters. As in most of the remote transactions, current remote voter registration systems face some security problems. These problems are mainly related to the inability to accurately verify the identity of the voter, which can facilitate impersonation or multiple registrations by the same voter with different data [El07].

In this paper we propose a remote voter registration scheme, in which some biometric systems play an important role to protect the accuracy of the electoral roll. Biometric systems have already been considered in electronic voting in the voting phase, e.g. [Ho07]. However, they have not been extensively used in the voting or in the registration phase.

It is important to note that sometimes voter registration is related to the voter credential generation process. Some authors have made proposals about this subject [Ac04, Kr07, Sc06]. However, in the context of this paper, voter registration is related to the creation of the electoral roll.

Section 2 presents a panorama of the current voter registration systems, as well as an analysis of biometrics and how these can be applied to improve the voter registration process. In section 3, our proposal is described. Section 4 concludes by emphasizing the advantages that our proposal gives to the remote voter registration process.

2 Voter Registration

2.1 Current Voter Registration Systems

Nowadays, in some countries like The United States [Fv08] or United Kingdom [El08] it is common to carry out remote voter registration. These methods allow the voter to fill out his or her own paper registration form remotely (e.g., at home) and return this form to the registration officers by using a delivery channel or optionally attending in person to a registration site. Registration forms are usually available to voters through postal delivery or downloading them from the network. In both cases voters fill out handwritten sign and return the forms to the registration officers using a postal delivery or any other alternative channels such as fax or e-mail (attaching a scanned copy of the filled form) [Fv08]. Furthermore, there are countries [De06] introducing the use of web interfaces to allow voters to fill out the registration form online, speeding up the remote acquisition of voter registration information.

After sending the registration form, if a voter wishes to verify that the registration has been received by the registration officers, he or she can contact them through e-mail or a phone call.

In the cases previously described, the identification of the voter is done by one or the combination of the following techniques: the verification of personal information of the voter and the verification of some physical characteristics of the voter. The first technique consists of registration officers checking to see if the voter included in the form some personal information that it is also stored in the voter register. Some examples could be the date of birth, the social security number or any other familiar information (e.g., mothers' maiden name, etc.). The problem with using such information for identifying the voter is that this information could be available in other databases (e.g., the member database of a social club) or could be known by people close to the voter. Therefore, it could be easy to impersonate a voter in the registration process just using this information.

The second technique consists of requiring verifying the identity of the voter based on checking some voter personal characteristics, such as a handwriting signature stamped on the form or the face or fingerprint of the voter against an image or template contained in some identity card or database. Face recognition requires the physical presence of the voter and therefore, it is not suitable for a real remote voter registration. However, handwriting recognition is the usual way implemented by remote registration and therefore the main one considered in this paper. In any case, the accuracy of this second technique of voter identification is based on the ability of the registration officers to validate the voter authentication data. Considering that most of these officers are not handwriting or physiognomy experts, we cannot expect high levels of accuracy.

Furthermore, current remote voter registration methods do not check if the same person has filled out more than a registration form by using the names of different valid voters. That is, using handwriting signatures as a reference, the verification process is based on looking for similarities between the signature on the form and a pre-existing signature. Therefore, detecting a person filling out more than one registration form signed with different signatures could be unfeasible for a registration officer. In this case, registration officers must have the ability to extract the identity of a person from the handwriting signature instead of looking for similarities. It is important to mention that registration officers usually do not have a pre-existing signature of the voter. Therefore, the signature contained in the registration form is only used to create a temporary database of signatures that will be used to identify the voters during the vote casting process. For example, in the case of postal voting, the voter signature stored during the registration process is compared against the signature contained in the postal envelope to detect if the vote has been cast by the legitimate voter.

Finally, in addition to identification accuracy, there are additional problems in current remote registration scheme. The contents of the registration form can be altered after the voter has sent this form. Furthermore, the handwriting signature on the form can be re-used by an attacker to fill out a different registration form. This problem lies in the fact that handwriting signatures (as well as face recognition) are not bound to the contents of the register. Therefore, any change in the contents of the registration form or the re-use of a valid handwriting signature in a different form cannot be detected by simply verifying the signature.

Summarizing, current voter registration systems face the following problems:

- Accuracy to validate the voter identity;
- Prevention of multiple registers by voters; and
- Integrity of voter registration information.

To increase the accuracy of remote registration process, we propose the combination of biometric systems and cryptographic functions. Below we analyze which are the improvements of adding both techniques in remote registration process.

2.2 Accuracy on Biometric Systems

In some way, the voter registration systems previously described are based on the use of biometrics. Registration officers usually verify some physical characteristics that uniquely identify the voter, such as a picture (facial identification) or the signature of the voter. However, one of the main issues of this identification is the accuracy on the process, since not all the registration officers are, for example, handwriting or physiological experts. In this sense, we propose the use of biometric systems to help registration officers to improve the accuracy of voter identification. However, are all the biometrics systems suitable for a remote voter registration?

Biometric systems are electronic systems specialized on identifying a user by means of processing unique physiological or behavioural characteristic of the user. Biometrics systems are classified based on the unique characteristic of the user that is used for the identification, for instance: DNA, face, fingerprint, iris, palmprint, retina, writing/signature and voice. However, the accuracy on the different biometric system is not the same, since each of the biometric characteristics processed has advantages and disadvantages.

A good biometric characteristic must fulfil some requirements [JR04]:

- Universality- Each individual should have the characteristic.
- Uniqueness- How well the characteristic makes different two individuals.
- Permanence- How well the characteristic endures over time.
- Collectability- Ease of acquiring the characteristic.
- Performance- Refers to the speed and accuracy of recognition as well as the resources required to do it (cost).
- Acceptability. It indicates the level of acceptance of people to use the characteristic.
- Robustness. It reflects the level of resistance against fraudulent methods attempting to mislead the system.

In our analysis, we considered an additional requirement for remote voter registration: the biometric system must be remotely available for most of the voters. Therefore, the acquisition of the biometric information must be supported using standard means or devices. This reduces the number of potential candidates to handwriting signatures and voice biometrics, since these allow biometric information to be acquired by means of scanning the signature written in the paper registration form or a voice recording made from a standard telephone. About handwriting biometrics, there are two distinct techniques, namely on-line and off-line handwriting. Besides the shape of the signature, on-line signatures take into account other aspects such as pen timing, pressure or writing trajectory. However, we do not consider on-line signatures a good candidate, since it requires voters to have available a digital-pad for acquiring a writing of a text (e.g., the signature of the voter). Therefore we will focus on off-line signatures.

Using pre-existing biometric systems comparative analysis [JR04, Ti06] and taking fingerprint biometrics as reference, the proposed biometrics systems fulfil the requirements previously introduced as follows (L=Low, M=Medium and H=High).

| Biometrics | Universality | Uniqueness | Permanence | Collectability | Performance | Acceptability | Robustness |
|--------------------|---------------------|-------------------|-------------------|-----------------------|--------------------|----------------------|-------------------|
| Fingerprint | H | H | H | M | H | M | M |
| Off-line Signature | M | M | L | H | L | H | L |
| Voice | M | M | M | H | M | H | L |

Table 1. Comparison of three example biometric systems

From this comparison we can conclude that off-line signatures and voice biometrics are not as robust as fingerprint biometrics systems. However, the introduction of voice biometrics could improve the current systems based on handwriting signatures.

Another important aspect of performance on biometrics is the accuracy of the identification process. There are three parameters that can help to determine in a quantitative manner such accuracy:

- *False rejection rate (FRR)*. It is the percentage of eligible user requesting access declared by the system as non-eligible;
- *False acceptance rate (FAR)*. It is the percentage of non-eligible access attempts identified as valid users.
- *Equal error rate (ERR)*. The point at which FRR and FAR are the same.

Additional comparative analysis of the same biometrics systems used in Table 1, provide the following measures from the accuracy point of view.

| Biometrics | FRR | FAR | EER | References |
|--------------------|------------|------------|------------|-------------------|
| Fingerprint | 2.2% | 2.2% | 2.2% | [Ca06], [Bi06] |
| Signature off-line | 10-30 % | 10-30% | 10-30% | [KSX04], [YJX07] |
| Voice | 5-10% | 2-5% | 6% | [Re05], [PM04] |

Table 2. Accuracy performance of biometric systems

Based on the values shown in table 2, fingerprints are again, the best positioned biometric characteristic. However, as we will explain in the definition of our proposal, fingerprints do not give any advantage over the current solutions on remote registration environment. Furthermore, voice biometrics behave better than handwriting signatures. The values for voice have been obtained by using a telephone communication [Re05].

2.3 Preventing Multiple Registration on Biometric Systems

Another issue detected during the study of the current remote registration systems is the capacity to detect multiple registers from the same voter. To analyze how biometric systems can manage this issue, we considered the two main operation contexts implemented by biometric systems for user authentication: verification and identification.

Verification. In this context, the system verifies a user identity by comparing the given biometric data with a template stored in the system database. To start the comparison, the user gives a personal ID or username known by the system. The system then retrieves the template related to such user and carries out a one-to-one comparison. That way it is possible to determine if a user is who she claims to be.

Identification. In this context, the user does not need a personal ID or username. Based on the biometric characteristic given by the user, the system has to identify if such characteristic corresponds to one stored in its database. In this case, a one-to-n comparison is carried out.

Based on the operation of both contexts, we can identify that current remote voter registration methods only use the verification context; registration officers use voter personal information to retrieve the signature stored in their database for the comparison. However, using a biometric system in the identification context, the signature of the register could be checked against the complete database of signatures stored. Then, in case the same voter attempts to register more than once using different personal information, she will be detected. Therefore, the use of an identification context prevents multiple registrations by voter.

2.4 Binding Biometrics and Contents

Finally, in order to overcome the feasibility of an attacker changing the contents of a registration form, or separating such contents from the voter identification element, it is necessary to get a link between the contents of the registration form and the voter identification element.

Nowadays, a usual method to protect information is the digital signature. A digital signature protects the information from alterations and binds such information to its author. However, digital signatures have important logistic problems, for example it is necessary for a PKI to generate and provide users with digital certificates.

On the other hand, despite the advantages that biometrics can give to the identification or verification aspects, not all the biometric techniques provide a bind between the biometric characteristic and the contents of a message. For example, in the comparisons presented, fingerprint is considered the most efficient biometric in the values scale given. However, neither fingerprints nor signatures, are usable for binding the contents. In both cases the contents of a message can be manipulated and this cannot be detected by means of the fingerprint or signature.

We have evaluated how to take advantage from the most usable biometrics to carry out the voter registration process in a more effective way. The main idea, as we already have mentioned, is to bind the contents of the registration form to the identification element (i.e. the biometric characteristic). Table 3 shows a new element (hand-writing) and a new requirement (content binding). The handwriting element is added as an extension of signature. Handwriting refers to the unique characteristics that an individual possesses in his or her writing. The new requirement added in table 3 refers to the ability to bind the contents, in our case registration information, to the biometric characteristic. Note that both signature and writing have the same values in the initial compared requirements. However, writing biometrics as well as voice possesses that peculiar characteristic, which is the binding that can give between the biometric characteristic and the contents of the message. In the proposal, we take advantage of such binding to improve the current registration systems.

| Biometrics | Universality | Uniqueness | Permanence | Collectability | Performance | Acceptability | Robustness | Content binding |
|--------------------|---------------------|-------------------|-------------------|-----------------------|--------------------|----------------------|-------------------|------------------------|
| Fingerprint | H | H | H | M | H | M | M | No |
| Signature off-line | M | M | L | H | L | H | L | No |
| Handwriting | M | M | L | H | L | H | L | Yes |
| Voice | H | M | M | H | M | H | L | Yes |

Table 3. An extended comparison of biometric characteristics

3. Proposal

This proposal carries out a remote voter registration in a secure way. It protects from alterations the contents of the voter registration information by binding such information to the voter identity. This is reached by means of combining biometrics and cryptographic techniques that do not require a public key infrastructure. It consists of creating a kind of biometric digital signature. That means a biometric characteristic that can give at the same time both authentication and integrity to the contents.

The scenario for the application of the scheme is a voter registration over Internet. However, other application scenarios are currently possible.

In this scheme, four participants are necessary during the voter registration process: a citizen requesting to be a voter, a registration module, a validation module and the registration officer.

Voter- The voter provides her personal data in order to generate the registration information. The voter also will collaborate to generate a registration proof based on both, her biometric characteristic and the registration information.

Registration module- This module is used to enter the voter registration information and generate an integrity proof of such registration information.

Validation module- The registration proof is generated by means of this module. Such proof is generated with the biometric information provided by the voter.

Registration officers- The registration officers receive the voter register information and carry out some validation processes.

The scheme is divided in two main stages:

- Introduction of the voter registration information and protection of the integrity
- Generation and validation of a registration proof

Based on this division the scheme behaves as follows.

3.1 Introduction of the Voter Registration Information and Protection of the Integrity

The voter connects to the Web site of the Registration Module by means of a secure and encrypted channel, e.g. SSL. The Web site provides a registration form. The voter fills out the registration form with his or her required personal data. Once the registration form is completed, an integrity proof is generated by the Registration Module. Such integrity proof is a cryptographic hash function of the registration information provided by the voter.

The integrity proof is then represented in a format that can be legible by the voter, for instance, a base-32 notation [RFC06]. We selected base-32 notation instead of others available notations (e.g., base-64) for usability reasons: it uses a reduced set of characters focused on minimizing interpretation mistakes. For example, the number 0 is not included in the representation set to prevent being confused by the letter “O.”

This representation is shown to the voter by means of the same communication channel. Figure 1 shows the interaction between the voter and the Registration Module to carry out the remote registration and get the integrity proof.

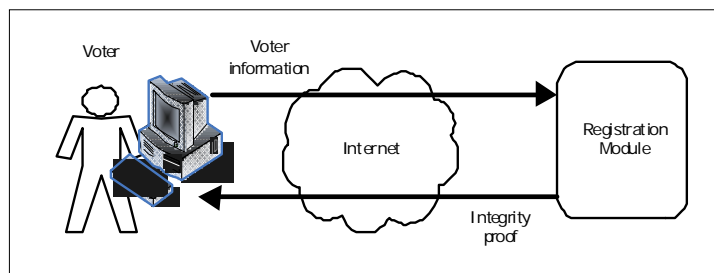


Figure 1: Interaction between Voter and Registration Module

In order to get the integrity proof it is used as a combination of MD5 and SHA1 hash functions. The latest is used in its MAC implementation. This combination is conceived with the aim of preventing collisions between the digest messages, such as was found in the last years for MD5 [Ha04, K105, Wa05, WY05] and for SHA1 [Wa05, WY05]. The integrity proof generation is then as follows:

1. Get a digest k from the registration information M_i :

$$K = \text{MD5} [M_i]$$

2. Use k as a key to get a HMAC-SHA1 from the same registration information M_i :

$$H = \text{HMAC-SHA1} [M_i, K]$$

The resultant H is the integrity proof.

Using a combination of MD5 and HMAC-SHA1, the probability to have a collision decreases significantly. An attacker needs to find a coincidence of collision for the same text on both systems. In addition, we are reducing the probability of these collisions without increasing the size of the digest that remains the same as a SHA1 (160 bits).

Since H is based on an HMAC-SHA1, it is 160 bits long, i.e. 2^{160} different digests. Therefore, a base-32 notation (which is 2^5) allows a representation of SHA1 in 32 characters. These 32 characters can be shown to the voter in six groups of five characters plus the two remaining ones. However, the integrity proof H can be truncated in order to give a higher usability. For example, taking only the first 20 characters, they can be shown in five groups of four characters or four groups of five characters, which is usable enough.

To prevent reply attacks, each form has a unique number. Therefore, two forms with the same contents will always have different integrity proofs.

Finally, the form with the voter register information and integrity proof is sent to the registration officers. This can be done by posting the on-line registration form or by printing and sending it by a postal service. The preferred option is using an on-line channel, since it allows the implementation of cryptographic techniques that cannot be applied on a postal delivery (e.g., encryption of the information). The received information is stored by the registration officers pending for further validation.

3.2 Generation and Validation of a Registration Proof

The second stage is the generation of a registration proof and the validation of the registration information. Based on the previous analysis, we will use a voice biometric system in this stage.

The voter carries out a communication with the Validation Module. This communication is done by means of a phone call. Then the voter is asked to give the integrity proof. He or she speaks the proof previously shown by the Registration Module, i.e. the groups of characters that represent the integrity proof. By doing this process, the voice of the voter is bound to the contents of the registration information. This is called the registration proof. The registration proof is then stored by the Validation Module. Figure 2 shows the interaction between the voter and the Validation Module in order to generate the registration proof.

The registration proof protects the integrity of the registration information. Any change in the registration information causes the registration proof to not correspond to the contents of the registration information. The registration proof also binds the contents of the registration information to the author, that is, the voter who provides his or her personal information.

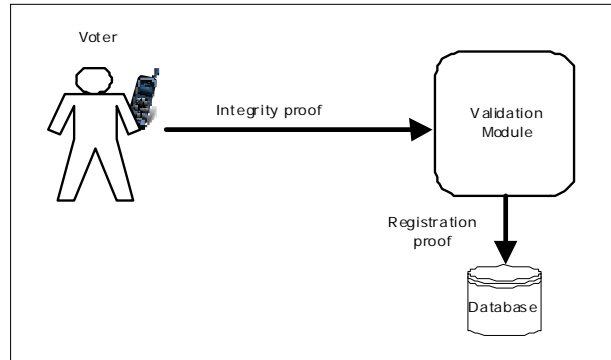


Figure 2: Interaction between Voter and Validation Module

The interaction between the voter and the Validation Module includes, besides the speech of the integrity proof, other dynamic data in order to prevent reply attacks in which an attacker could use a pre-recorded voice of a voter. Such dynamic data could consist of a challenge to the voter who has to repeat a word or a set of words said by the Validation Module. That way, the Validation Module can be sure that the integrity proof is being spoken by a person who is on the other side of the communication line and not by a pre-recorded or automatic process.

Once the registration officers have recorded the validation proof, they can start the validation process.

The validation process facilitates the detection of people who attempt to create more than one record. It is possible to compare the voice of a voter who is validating a new registration with the set of voices previously recorded. That way, a person attempting to create a bogus or an additional record will be rejected, and the registration information associated with the proof provided by such a person will be identified as invalid. Therefore, the probability of impersonation is low. This verification is not necessarily carried out on-line but it can be made after the registration process.

Since any attempt at creating bogus records can be detected through the validation process, the scheme does not require a previous database with the recorded voice of voters. However, for future registrations, the previous records can be used in order to validate the voice of the voter who is making the new record.

An additional validation consists on checking the voter registration information against the associated registration proof. This check will consist on verifying if the integrity proofs match. That means, if the hash of the voter registration form has the same value as the one recorded as part of the registration proof.

If registration proofs and voter registration records pass all the validations, election officers can accept the voter registration information of the voter. If any of the validations fail, the voter registration form and corresponding registration proof can be classified as non-validated records. Therefore, registration officers can implement additional manual checks or contact the voter for checking the process if required.

In a subsequent voting stage, it could be possible to use the registration proof to verify that the person who is voting is the same who created the registration information by checking his or her voice.

Our scheme can be also used as a means to activate the voter credentials once they have been received by the voter. This is usable if the voter credentials are sent to voters by remote means. In such cases, there is the risk that voter credentials are received or intercepted by a third person. The activation technique prevents somebody using the voter credentials instead of the legitimate voter. The activation is carried out by means of an activation code, which is enclosed to the voter credentials. The voter has to call and say the activation code to the registration authority and then a process of comparison between the activation voice and the voice recorded during the registration process is carried out. If the activation voice is the corresponding one, then the voter credentials are validated and authorized to participate in the election. That way, an illegitimate use of the voter credentials is prevented.

Another possible scenario in which our voter registration process can be applied is by using handwriting biometrics instead of voice. The first part of the process (generation of the registration information and integrity proof) could be the same as the previously described, that is, through Internet. The second part of the process (generation of the integrity proof) is carried by the voter by writing by hand the representation of the integrity proof. That way, the registration proof binds the contents of the registration information with the handwriting biometrics of the voter. The handwriting of the integrity proof is carried out in a form provided by the election authority. Once filled out by the voter with the hand-written integrity proof, this form is sent to the election authority by means of postal mail. The sending can be also by electronic means such as fax or e-mail. In the case of electronic sending, the form has to be previously converted to a digital format by scanning it. Even when the verification of a writing text is as difficult as the signature verification, the advantage of the writing text respect to the signature is that it can do the linking to the contents as we have explained before.

4 Conclusions

Current remote voter registration systems have important issues that can facilitate voter impersonation. These issues are mainly voter identification accuracy, multiple registrations from the same person and voter registration information integrity. In this paper we proposed the use of biometrics systems to increase the voter identification accuracy of voters that make a remote registration. In addition, operating on an identification context, biometrics systems can automate the detection of multi registrations made by the same person. Finally, we identified and proposed some biometrics methods, such as handwriting and voice biometrics that can also bind the registration information to the voter identity. Combining this later feature with the use of cryptographic algorithms, such as hash functions, we also provided a way to protect the integrity of voter registration information that can be suitable to implement in current environments.

References

- [Ac04] Acquisti, A: Receipt-free homomorphic elections and write-in ballots, Cryptology ePrint Archive, Report 2004/105, <http://eprint.iacr.org/>, 2004.
- [Bi06] Biometric System Laboratory - University of Bologna: "FVC2006: The Fourth International Fingerprint Verification Competition," 2006. Available at <http://bias.csr.unibo.it/fvc2006/default.asp>.
- [Ca06] Cappelli, R. et. al.: Performance evaluation of fingerprint verification systems. IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 1, pp. 3–18, January 2006.
- [De06] Department of Defense U.S., Report on IVAS 2006, As Required by Section 596 of the National Defense Authorization Act for Fiscal Year 2007, December 2006.
- [El07] Election Law Blog. The Extremely Weak Evidence of Voter Fraud in Crawford, the Indiana Voter ID Case. May, 2007. Available at <http://electionlawblog.org/archives/008378.html>
- [El08] Electoral Commission' website to register to vote. Available online at <http://www.aboutmyvote.co.uk/register/CitzSelect.cfm?officeID=214&CFID=12799012&CFTOKEN=71181288>
- [Fv08] FVAP Voting Assistance Guide. Available online at <http://www.fvap.gov/pubs/vag.html#ch3>
- [Ha04] Hawkes, P. et. al.: MD5 collision, October 2004. Available at <http://eprint.iacr.org/2004/264>.
- [Ho07] Hof, S.: E-Voting and Biometric Systems? Electronic Voting in Europe. pp. 63-72. 2004.
- [JR04] Jain, A.; Ross, A.; Prabhakar, S: An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No.1, pp. 4-20, January 2004.
- [Kl05] Klima, V.: Finding MD5 collisions on a notebook PC using multi-message modifications. In International Scientific Conference Security and Protection of Information, May 2005.
- [Kr07] Krivoruchko, T: Robust Coercion-Resistant Registration for Remote E-Voting, Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE 2007), 2007.

- [KSX04] Kalera, M.; Srihari, S.; Xu, A.: Offline signature verification and identification using distance statistics. *International Journal of Pattern Recognition and Artificial Intelligence*, Vol. 18, No. 7 pp. 1339-1360. 2004.
- [PM04] Przybocki, M.; Martin, A.: NIST, Speaker Recognition Evaluation Chronicles. In *Odyssey: The Speaker and Language Recognition Workshop*, pp. 12–22. Toledo, Spain, May 2004.
- [Re05] Reynolds, D. et. al.: The 2004 MIT Lincoln laboratory speaker recognition system, in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing*, Philadelphia, PA, March 2005.
- [RFC06] RFC 4648. October 2006. Available at <http://tools.ietf.org/html/rfc4648#section-6>
- [Sc06] Schweisgut, J: Coercion-resistant electronic elections with observer, 2nd International Workshop on Electronic Voting, Bregenz, August 2006.
- [Ti06] Tiltont, C.: The Role of Biometrics in enterprise Security. Dell Power Solutions. 2006. Available online at <http://www.dell.com/downloads/global/power/ps1q06-20050132-Tilton-OE.pdf>.
- [Wa05] Wang, X. et. al.: Cryptanalysis of the hash functions MD4 and RIPEMD. In *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Aarhus, Denmark, May 22-26, 2005, *Proceedings (2005)*, vol. 3494 of *Lecture Notes in Computer Science*, Springer, pp. 1-18.
- [WY05] Wang, X.; Yu, H.: How to break MD5 and other hash functions. In *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Aarhus, Denmark, May 22-26, 2005, *Proceedings (2005)*, vol. 3494 of *Lecture Notes in Computer Science*, Springer, pp. 19-35.
- [YJX07] Yu, Q.; Jianzhuang, L.; Xiaou T.: Offline Signature Verification Using Online Handwriting Registration. *Computer Vision and Pattern Recognition, CVPR '07. IEEE Conference on*. pp. 1-8. June 2007.

Long-term Retention in E-Voting – Legal Requirements and Technical Implementation

Rotraud Gitter¹, Lucie Langer², Susanne Okunick³, Zoi Opitz-Talidou¹

¹Universität Kassel
– provet –
Wilhelmshöher Allee 64-66
34119 Kassel, Germany
[r.gitter | z.talidou}@uni-kassel.de](mailto:{r.gitter|z.talidou}@uni-kassel.de)

²Technische Universität Darmstadt
Cryptography and Computeralgebra
Hochschulstraße 10
64289 Darmstadt, Germany
emailadresse@autor1
langer@cdc.informatik.tu-darmstadt.de

³pawisda systems GmbH
Robert-Koch-Straße 9
64331 Weiterstadt, Germany
susanne.okunick@pawisda.de

Abstract: Legally binding elections require retention of specified election data such as balloting material. This applies to paper-based as well as electronic elections. However, in Germany, legal requirements on retention in e-voting have not been issued so far. Based on the German legal framework for governmental as well as non-governmental paper-based elections, we give recommendations on long-term retention in e-voting, applying our results to a state-of-the-art e-voting scheme. We also review technical measures to meet the security requirements of long-term retention in e-voting.

1 Introduction

In the context of governmental actions and democratic elections especially, secure long-term storage is an important issue. Strict regulations apply here and compliance with these obligations must be documented as a proof of correct process implementation. Turning to e-government and e-voting in particular, new challenges have to be faced in this area: While the classical paper-based form of documentation just needs to be stored in a safe place once and for all, long-term retention of electronic data truly is a long-term task. Electronic data can easily be changed, therefore issues like integrity and authenticity must be addressed. Furthermore, due to hardware and software obsolescence, difficulties in terms of readability emerge.

With respect to democratic elections, the ballots must be retained over a specific period (usually several years) to allow recounting in case of contestations. Hence, for legally binding elections there exist legal obligations regarding long-term retention. This applies to common paper-based as well as electronic elections. But unlike the paper-based variant, legal regulations for remote electronic elections have not yet been issued in general. In its recommendation on legal, operational and technical standards for e-voting [Cou04], the Council of Europe states that “the e-voting system shall maintain the availability and integrity of the electronic ballot box,” which means that “the information kept in the electronic ballot box must be securely saved for as long as this is necessary to permit any recount or legal challenge or for the period after the election required by the electoral process in the member state in question” [Cou04, Standard No. 99]. Concrete measures are a matter for national legislature. The German Informatics Society (Gesellschaft für Informatik – GI) has developed a catalogue of requirements for online elections in non-governmental organizations [Ges05], presuming that there exist no regulations regarding long-term retention of election results. At the same time, the GI as well as the German Research Foundation (Deutsche Forschungsgemeinschaft – DFG) have adopted their own regulations for online elections, which comprise also regulations regarding long-term retention of election records (cf. [Ges04], [Deu06]).

The different issues of long-term retention in general have been addressed by a lot of research projects. The projects nestor [nes] and PADI [PAD] brought together and made available competences and information regarding technical, organizational, and legal aspects of long-term archiving. InterPARES [Int] is a major international research initiative that aims at developing the knowledge necessary to provide policies, strategies and standards capable of ensuring the longevity and trusted authenticity of digital material. In Germany the DOMEA concept [DOM] defines requirements for document management and electronic archiving in e-government. The long-term conservation of electronically signed documents has been addressed by the European Telecommunications Standards Institute [ETS03] and the projects ArchiSig [Arc] and TransiDoc [Tra]. The LTANS group [LTA] brings forward the standardization in this area. However, long-term retention in the context of e-voting has not yet been addressed before and the question as to which data should be retained is unanswered. [VK06] focuses on the challenge of providing everlasting privacy for online elections that, at the same time, are based on cryptosystems that may be broken at some point in the future. But to the best of our knowledge, long-term retention in the case of electronic elections has not yet been studied thoroughly before.

Our paper is structured as follows. In Section 2 we review the regulations for paper-based elections in Germany and transfer them to online voting, providing legal requirements regarding long-term retention of election data in e-voting. In Section 3 we apply our results to a state-of-the-art e-voting protocol and evaluate which data must be retained in particular to meet the legal requirements we have derived. Following a more technical approach, we report on specific requirements regarding retention in e-voting in Section 4: Which security objectives must be achieved? Which measures should therefore be applied? We also provide concrete recommendations regarding the technical implementation, referring to the protocol we have analyzed in Section 3. Concluding remarks are given in Section 5.

2 Legal Framework

In the following we analyze the legal regulations that apply to selected election types in Germany, reaching from governmental elections for democratic decision-making to non-governmental elections in civil society.

2.1 Legal Requirements for Conventional, Paper-based Elections

Parliament.

Elections of the German Bundestag take place every four years [Sch98]. They are subject to the Federal Electoral Law (Bundeswahlgesetz – BWG) and specified by the Federal Election Ordinance (Bundeswahlordnung – BWO), which contains provisions for documentation and safekeeping of the election material. According to Art. 72 BWO, the election board has to keep a record of the election process, the vote counting and the election results. Discarded ballot papers must be enclosed in the record as well as envelopes and polling cards whose validity has been questioned. The record has to be approved and signed by the members of the election board. All documents are handed over to the municipality hereafter. The municipal authorities have to retain the election documents for a period determined by Art. 90 BWO. Protection against unauthorized access must be ensured. The following election documents have to be retained for six months, as long as no scrutiny procedure is pending and no law enforcement authority needs to investigate regulatory offences: the electoral roll, the polling card register, the register of invalid polling cards, and the register of persons (for example in hospitals or monasteries) who according to Art. 29 (1) BWO, were allowed to vote by a moving election board; furthermore, the form letters containing the signatures assisting the nomination of candidates. All the other documents such as voting papers, voting envelopes, and the documents of the postal vote have to be retained in accordance with Art. 90 (3) BWO for the whole legislative period of the Bundestag, until 60 days before the elections of a new Bundestag.

The longest retaining period for elections documents amounts to four years. This period may be extended if pursuant to Art. 49 BWG scrutiny procedures are pending or when regulatory offences (see Art. 107-108e StGB) need to be investigated by the law enforcement authorities. Consequently, the appropriate election documents may be needed for a period of longer than four years to be used as evidence material for the hearing or the proceedings.

Works Council.

Elections of the works council are held every four years. The election process is governed by Art. 7-20 of the German Works Constitution Act (Betriebsverfassungsgesetzes – BetrVG) and, in detail, determined by a special election ordinance (Wahlordnung – WO). Documentation requirements are stipulated in Art. 18 BetrVG, Art. 16 and 19 WO. According to Art. 18 (3) BetrVG the election board has to establish a record of the election process subsequently to the termination of the election. The record must contain the total of the ballot envelopes handed in, the total of valid and invalid votes, the number of valid votes for every list of candidates, the distribution of seats to the lists, the names of the elected candidates, and finally, any incidents or matters that might affect the validity of the election. The record must be signed by the chairman and at least one different member of the election board (*writing requirement*). According to Art. 19 BetrVG an election may be contested if any of the essential rules regarding the right to vote, eligibility or the electoral procedure have been infringed and no subsequent correction has been made. In this case only infringements that verifiably could not have altered or influenced the election results will not affect the validity of the election. As a rule, contestations must be filed within two weeks of the announcement of the election results.

However, severe infringements exceptionally may be claimed even hereafter, whereupon the election result might be declared void at any time. Art. 19 WO therefore stipulates that the newly elected works council has to retain all relevant election documents at least until the end of its term of office. These documents are, in addition to the record of the election board, any other documents in the broadest sense that might be relevant in case of election contest: for example ballots, announcements of the election board and the envelopes of late postal votes that were not counted.

Governing Boards of Social Security Institutions.

Elections of the governing boards of the social pension funds as well as for the health, nursing and accident insurances take place every six years. The election process is governed by Art. 43 et sqq. of the Social Security Code (SGB IV) and by the special Electoral Ordinance for that sector (SVWO). According to Art. 91 SVWO there is a general obligation to retain the election documents for the whole term of office of the governing boards. However, the voter's election pass, the ballot papers, the ballot envelopes and the postal voting envelopes can be discarded if the election is not contested one month after the announcement of the final results (see Art. 57 (3) SGB IV). In case of an election contest, these documents have to be retained for at least two months after the court decision has become legally binding, as far as no special reasons demand further retaining.

Executive Committee of an Association.

The executive committee of an association is elected at the annual general membership meeting [Kur04]. The election procedure is organized pursuant to the provisions of Art. 28 et seq. of the German Civil Code (BGB), if the articles of association do not stipulate something else (Art. 40 BGB). Details of the electoral procedure, for example the voting principles, the eligibility requirements, or the modality of the election performance, may be regulated according to the discretion of the body setting down a separate voting statute of the association [Rei07].

On the association level, elections have already been carried out electronically: The German Informatics Society as well as the German Research Foundation have issued their own e-voting statutes (cf. [Ges04], [Deu06]). Both of them comprise provisions concerning the retention of electronic election documents and the voting software which provide for a retention period according to the term of office of the executive committee, i.e. two and four years, respectively.

2.2 Obligations for Documentation and Retention in E-Voting

Legal rules governing elections demand a thorough documentation of the election process and the retrieval of the results. Even if it is not explicitly stipulated (as for the elections of the executive committee of an association), a preservation of these documents is necessary to prove the dual process of the election and the correct calculation of results. As a rule these documents should be stored at least for the term of office of the elected body. E-Voting systems must provide for an appropriate electronic documentation to prove the compliance with basic voting principles. The election host therefore must be able to demonstrate how the technical or organizational processes which could alter or influence the election results work in general and if the system functions properly. For this purpose the election host must be able to prove the security of the relevant components and applications of the voting system. The tallying process must be verifiable and hence repeatable. Thus, in particular the number of cast and counted ballots – including the number of valid and invalid ballots – must be documented, as well as logging files that can exclude any manipulation of the system. It should be possible to recount the election results by a trustworthy counting program. If legal norms require paper-based documentation (e.g. for the record of the election board), printouts can be generated and signed by the responsible authority. According to German law, it is also possible to replace the handwritten signature by a qualified electronic signature. In any case, qualified signatures should be used to provide for the integrity and authenticity of the electronic documentation [Siga].

3 Implementing Legal Requirements: A Concrete Example

In the following, we apply our results regarding legal stipulations on long-term retention to the e-voting scheme designed by Juels, Catalano, and Jakobsson (JCJ) [JCJ05]. First we give a short description of the protocol. Hereafter we investigate which of the occurring data must be retained in order to meet the legal requirements we have identified in Section 2.

3.1 Protocol Description

The scheme proposed by JCJ was the first one to offer coercion-resistance, which means that a voter cannot be forced to abstain from voting or to vote in a particular way. In effect, a potential adversary cannot learn whether the coerced voter complied with his demand. To achieve this, the JCJ scheme is designed such that the identity of the voter remains hidden during vote-casting and validity of the ballot is verified by blind comparison against an electoral roll. For this, secret anonymous credentials are distributed among the voters during registration phase. These credentials serve two purposes: Firstly, they are employed for authentication and authorization of the voters. Secondly, they mark a “free” vote in the sense that this vote indeed expresses the voter’s will; if a voter wants the vote to be accounted, she includes her valid credential. If she casts the vote under coercion, she attaches an invalid credential. The coercer is not able to distinguish invalid credentials from valid ones and hence cannot know if the voter has complied with his demand. Since multiple voting is allowed, the voter can hereafter cast a valid vote. In the end, only the latest vote with a valid credential is accounted in the tallying process.

Registration.

The identity and eligibility of each voter is first verified by the registration authority. Upon successful verification, voter v_i receives a unique valid credential σ_i from the registration authority over an untappable channel. An encrypted version S_i of this credential is published on the bulletin board. At the end of registration phase, the electoral roll L contains all valid encrypted credentials alongside the plaintext names of registered voters and is signed by the registration authority. The registration authority is assumed to be trustworthy, but can also prove to a voter that σ_i is authentic, i.e. that S_i is a valid encryption of σ_i . However, it must be assumed that the registration authority does not leak credentials to an adversary.

Voting.

The registration authority publishes an integrity-protected candidate list C . For voting, the voter v_i casts a ballot over an anonymous channel. The ballot comprises the following parts:

1. A probabilistic encryption of the chosen candidate c_j , hereafter referred to as the *vote*
2. A probabilistic encryption of the voter's credential σ_i
3. A non-interactive zero-knowledge proof (cf. [BSMP91]) that c_j is in C
4. A non-interactive zero-knowledge proof of knowledge of σ_i and c_j

Voter v_i encrypts her valid credential σ_i if she wants her vote to be accounted, otherwise she encrypts a fake credential σ_i' . The proof that c_j indeed marks a valid candidate is necessary since casting write-in votes could compromise coercion-resistance. Knowledge of σ_i and c_j must be proved to prevent replay-attacks by simply re-encrypting votes that have already been cast.

Tallying.

1. Proof checking. The tallying authority first checks that all proofs included in each ballot are correct. Ballots containing invalid proofs are discarded. For all the remaining ballots, let A_1 denote the list of encrypted votes and B_1 the list of encrypted credentials.

2. Duplicate removal. Next, the tallying authority removes ballots with credential duplicates via plaintext equivalence test (see [JJ00]). Only the latest credentials in B_1 are kept, resulting in a weeded list B_2 . The ciphertexts in A_1 , which correspond to duplicate credentials are also removed, resulting in a weeded list A_2 . Now there is no more than one vote per given credential.

3. Mixing. The list of encrypted votes as well as the list of encrypted credentials is mixed using the same, secret permutation.

4. Validity checking. The credentials from B_2 are compared with the ones in L via plaintext equivalence test, eliminating those which do not correspond to valid credentials in L . The corresponding invalid votes from A_2 are eliminated as well. Let A_3 and B_3 denote the final lists. These now correspond to authentic ballots cast freely by eligible voters with no more than one vote per voter.

5. Vote counting. Finally the votes in A_3 are decrypted and tallied.

3.2 Meeting Legal Requirements

We now investigate which data should be retained in order to meet the legal obligations specified in 2.2. Here we only specify *which* data is to be stored. Comments on the question *how* this should be done will be given in Section 4.

First of all, the list L is to be kept; it denotes the eligible voters and contains their valid, encrypted credentials. Furthermore, the list C should be stored since it contains the names of the candidates including unique identifiers used for vote-casting.

Let N denote the total number of ballots cast in the election. This value includes also multiple ballots cast by single voters under valid as well as invalid credentials. In 2.2 we have stated that the number of cast and counted ballots – including the number of valid and invalid ballots – must be documented. Hence, we first have to determine what “invalid” votes actually are with regard to the analyzed voting scheme. As mentioned before, for the JCJ scheme to remain coercion-resistant, it is excluded that voters cast write-in votes, which means that they vote for candidates that are not on list C and hence are invalid. This implies that voters cannot cast invalid votes, i.e. ballots that have been invalidated by the content of the vote and not by using an invalid credential. A ballot can thus only be invalid for one of the following reasons:

- (a) It contains an invalid proof
- (b) It has been cast under a valid credential, which was later on re-used to vote
- (c) It was cast under an invalid credential

The number of ballots corresponding to these categories are the following:

- (a) $N - |B_1|$ (see phase 1 of the tallying procedure)
- (b) $|B_1| - |B_2|$ (see phase 2 of the tallying procedure)
- (c) $|B_2| - |B_3|$ (see phase 4 of the tallying procedure)

According to 2.2 the retrieval of the election result shall be documented, which includes also ballots that have been declared invalid. In particular, ballots that contain invalid proofs and hence are to be discarded in phase 1 of the tallying procedure should not be deleted but rather kept for retention and just eliminated from the tally. For being able to exclude replay attacks, the valid proofs of knowledge of the tallied votes should be kept as well.

Subtracting the number of invalid ballots specified above from the total of N ballots gives $N - (N - |B_1| + |B_1| - |B_2| + |B_2| - |B_3|) = |B_3|$ valid ballots. This is no surprise since B_3 contains the valid, unique credentials under which votes have been cast. This list should be retained, as it must be verifiable that only eligible voters have cast a ballot.

Re-tallying of the votes requires retaining list A_3 since it contains encrypted votes, which correspond to the valid, unique credentials in B_3 .

Besides protocol-specific data we have just considered, additional material must be retained. According to the legal stipulations, it must be provable that the system functions properly and no manipulations have been performed. System auditing files as well as logging files of intrusion detection systems in use should therefore be retained in addition to the material specified above.

4 Technical Implementation of Long-Term Retention

In this section we address the technical realization of long-term retention. First we appoint the technical requirements for electronic and electronically signed voting material to meet legal obligations. Next we outline suitable technical protection methods. Finally we apply the results to the scheme proposed by JCJ, which we have introduced in Section 3.

4.1 Requirements for E-Voting

General requirements for the technical implementation of long-term retention are specified in [RFDJ07] and [WPB07]. In the following these requirements are transferred to e-voting:

Integrity. Any kind of retention is targeted at preserving the integrity of a document, i.e. preserving it as it originally has been created. Undetected modification or deletion of any election document, in particular the electronic ballots, must be prevented. Integrity – and hence the whole election – is compromised otherwise.

Authenticity. The authenticity of the documents must be preserved to keep the originator of the document identifiable. In case of electronic elections, special attention must be paid to the task of ensuring authenticity of the ballots (e.g. confirmed by a validating authority) on the one hand while providing for strict anonymity of the vote on the other hand.

Completeness. Since the whole election process has to be documented, the connection of the single election documents should be preserved.

Confidentiality. Voting material containing personal data of the voters must be protected against unauthorized knowledge. For instance the voter's signature includes the voter's certificate, which may contain sensitive personal data of the voter.

Negotiability. A document is negotiable if it is possible to transfer it if from one system to another without losing the possibility to check the characteristics of the document, for example, its integrity. In case of contestations, the evidential voting material has to be presented before the court without any quality loss.

Readability. The voting documents have to be readable, i.e. hardware to access the stored data must be available as well as software to interpret and present it. We assume that permanent availability of the voting data during the retention period is not required.

4.2 Technical Protection Methods

In the following, we present existing technical protection methods and evaluate them on the basis of the requirements defined above. The protection methods are divided into the following categories according to [RFDJ07]:

System-oriented. Data access is controlled by a technical system. By configuring the archiving system accordingly, access is restricted to certain components or persons. An example is write protection on a file system defining groups with reading and writing privileges.

Medium-oriented. This category includes storage media for which the overwriting or manipulating of the stored information is not possible, e.g. WORM (write once read many) or other non-rewritable media.

Document-oriented. This comprises technologies to preserve documents against unauthorized extraction of content and undetected modifications, for example encryption and qualified signatures.

In [RFDJ07] some protection methods out of every category are evaluated. At this point we pick up this evaluation and work out recommendations for the retention of e-voting documents.

Using Qualified Signatures.

As mentioned in Section 2 qualified signatures should be used to provide provability of the integrity and authenticity of the election documentation. A qualified signature proves that the data has not been modified and ensures that the originator of the signed document can be identified.

Signatures are also a suitable method to ensure completeness and negotiability. Completeness may be guaranteed by pooling all voting documents and signing this collection. Furthermore, a signed document is negotiable because any third person is able to verify the signature and thus prove the integrity and authenticity of the document. In contrast to signatures, system-oriented methods limit the negotiability of a document: An unsigned document protected by access control in a given system loses this protection when given to a third party. The third party is not able to verify the integrity of the document and has to trust the applied system or must verify its security.

Using Well-Known, Standardized Signature and Data Formats.

To ensure negotiability, accepted or standardized data formats should be used. If a rare and unknown format is used, the court will have to consult an expert opinion, which may cause great costs. Well-known or standardized signature formats are:

1. CMS (Cryptographic Message Standard) [Hou04]
2. XML signatures [ERS02]
3. PDF/A (ISO 19005-1:2005, this ISO standardization of the PDF/A specification includes the electronic signature)

General usage of standardized formats increases the probability that appropriate software is available and hence contributes to long-term readability.

Access Restriction During the Retention Period.

As previously mentioned, qualified signatures conserve the provability of signed documents, but they do not protect against modifications during the retention period. Therefore, additional protection methods are necessary. Suitable are non-rewritable media or system-oriented methods for the file system, document management systems or archive systems where the document is stored, e.g. access control software or a read-only mode for the documents. An alternative is the usage of any portable storage media as DVD or USB, which are deposited at a place accessible only by authorized persons. By access restriction the confidentiality of retained sensitive voting data can be achieved as well.

Redundant Data Management.

In general it is useful to hold the data redundant to safeguard against loss in case of unexpected impacts such as theft or fire. For this purpose, backups should be provided and kept in at a different place.

4.3 Long-Term Aspects

The retention period has great influence on the realization of retention since all technical protection methods are subject to an aging process and require an update. In the following we select long-term aspects important for e-voting.

Generally, obsolete archive systems and storage media have to be replaced by state-of-the-art technologies. During the replacing process data must not be modified or lost. We assume that currently available hardware that meets the minimal quality standard is durable for the expected retention time in e-voting.

In the case of electronic signatures, an aging process applies as well. After a certain time, the underlying cryptographic algorithms and parameters become insecure. Thus signatures lose their integrity and authenticity and hence their probative value. This process may be significant after six years and therefore concerns signed e-voting documents. In Germany, according to §6 of the Signature Act [Siga] and §17 of the Signature Ordinance [Sigb] electronic signatures have to be renewed by a new qualified electronic signature before the used algorithms lose their security suitability. In the concept of signature renewal the new signature is performed by a time stamp. A time stamp is issued by a time stamp service, which signs the document after adding a date. In the ArchiSig project [Arc] a concept has been developed in which a lot of documents are renewed by one time stamp [RS06]. At first the documents are merged in a hash tree in accordance with Merkle [Mer80]. Then a time stamp for the root hash value of the tree representing all documents is requested. This procedure is independent of document formats and more cost-efficient since qualified time stamps usually require a fee. The concept complies with the German and European Signature Law [Roß04]. The LTANS group [LTA] brings forward the standardization in this area, cf. [BPG07]. However, only few products exist which handle signature renewal.

E-Voting protocols such as the JCJ scheme mentioned in Section 3 usually employ encryption to ensure confidentiality. The aging process of cryptographic algorithms also influences the encrypted data. With the decreasing security suitability of the used algorithms, the encrypted document loses its confidentiality. Therefore additional measures should be taken during the retention period to ensure confidentiality.

4.4 Applying the Results to the JCJ Scheme

Finally, we briefly comment on long-term retention methods for the JCJ scheme discussed in Section 3.

While, for example the electoral roll L is supposed to be signed by the registration authority, most of the other data which is to be retained such as the lists A_3 and B_3 are a priori not signed. However, it is not sufficient to store the data unsigned since both data integrity and authenticity has to be provable before the court. Therefore it is inevitable to sign the material. Signing all lists including L by one authority additionally proves the completeness of the voting material. As recommended in Section 2, qualified signatures should be used.

To ensure negotiability, a non-proprietary format should be chosen for the lists. Otherwise the lists can only be interpreted and presented by appropriate proprietary software. To prove the compliance with essential voting rules, the security of the software must be examined. To ensure confidentiality, the encrypted credentials in the lists have to be protected against unauthorized access before the encryption parameters and algorithms become insecure.

5 Conclusion

Long-term retention is an important issue in e-government and e-voting in particular. Electronic elections can only become legally binding if legal obligations on long-term retention are met. We have transferred the legal regulations on paper-based elections in Germany to the scenario of online elections, providing guidelines for long-term retention in e-voting. Following an exemplary e-voting protocol we have analyzed which data must be retained concretely. We have also provided technical requirements for retaining voting documents and recommended technical protection methods. Our work shows that the requirements of long-term retention should be taken into account already when designing an e-voting protocol or selecting a scheme to be used for a practical implementation. We believe that we hereby contribute to building the foundations of e-voting and help advancing online elections, not only in Germany.

References

- [Arc] The ArchiSig Project. <http://www.archisig.de/>, last checked 26.02.2008.
- [BPG07] Ralf Brandner, Ulrich Pordesch, and Tobias Gondrom. Evidence Record Syntax (ERS). RFC, 4998, August 2007. <http://www.ietf.org/rfc/rfc4998.txt>, last checked 25.02.2008.
- [BSMP91] Manuel Blum, Alfredo De Santis, Silvio Micali, and Giuseppe Persiano. Noninteractive Zero-Knowledge. *SIAM J. Comput.*, 20(6):1084–1118, 1991.
- [Cou04] Council of Europe. Legal, operational and technical standards for e-voting. Recommendation Rec(2004)11, September 2004. http://www.coe.int/T/e/integrated_projects/democracy/02_Activities/02_e-voting/, last checked 13.02.2008.
- [Deu06] Deutsche Forschungsgemeinschaft. Wahlordnung für die Wahl der Mitglieder der Fachkollegien der Deutschen Forschungsgemeinschaft (DFG), 2006. http://www.dfg.de/forschungsfoerderung/formulare/download/70_01.pdf, last checked 25.02.2008.
- [DOM] DOMEA-Konzept. http://www.kbst.bund.de/cln_011/nn_836960/Content/Standards/Domea_Konzept/domea_node.html_nnn=true, last checked 28.02.2008.
- [ERS02] Donald Eastlake, Joseph Reagle, and David Solo. (Extensible Markup Language) XML-Signature Syntax and Processing. RFC, 3275, March 2002. <http://www.ietf.org/rfc/rfc3275.txt>, last checked 26.02.2008.
- [ETS03] ETSI TS 101 733 V1.5.1, 2003.
- [Ges04] Gesellschaft für Informatik. Ordnung der Wahlen und Abstimmungen, 2004. <http://www.gi-ev.de/fileadmin/redaktion/OWA/gi-owa.pdf>, last checked 24.02.2008.
- [Ges05] Gesellschaft für Informatik. GI-Anforderungen an Internetbasierte Vereinswahlen (“GI requirements for Internet based elections in non-governmental organizations”), August 2005. www.gi-ev.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf, last checked 13.02.2008.
- [Hou04] Russ Housley. Cryptographic Message Syntax (CMS). RFC, 3852, July 2004. <http://www.ietf.org/rfc/rfc3852.txt>, last checked 26.02.2008.
- [Int] The InterPARES Project. <http://www.interpares.org/>, last checked 25.02.2008.
- [JCJ05] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-Resistant Electronic Elections. In Vijay Atluri, Sabrina De Capitani di Vimercati, and Roger Dingledine, editors, WPES, pages 61–70. ACM, 2005.
- [JJ00] Markus Jakobsson and Ari Juels. Mix and Match: Secure Function Evaluation via Ciphertexts. In Tatsuaki Okamoto, editor, ASIACRYPT, volume 1976 of Lecture Notes in Computer Science, pages 162–177. Springer, 2000.
- [Kur04] Kurt Stöber. Handbuch zum Vereinsrecht. Otto Schmidt, München, 2004.
- [LTA] Long-Term Archive and Notary Services (Itans). <http://www.ietf.org/html.charters/ltans-charter.html>, last checked 26.02.2008.
- [Mer80] Ralph C. Merkle. Protocols for Public Key Cryptosystems. In IEEE Symposium on Security and Privacy, pages 122–134, 1980.
- [nes] nestor – The German Network of Expertise in Digital Long-Term Preservation. <http://www.langzeitarchivierung.de/index.php?newlang=eng>, last checked 28.02.2008.
- [PAD] PADI – Preserving Access to Digital Information. <http://www.nla.gov.au/padi/>, last checked 28.02.2008.
- [Rei07] Bernhard Reichert. Vereins- und Verbandsrecht. Luchterhand Verlag, 2007.

- [RFDJ07] Alexander Roßnagel, Stefanie Fischer-Dieskau, and Silke Jandt. Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente, August 2007. <http://www.bmwi.de>, last checked 25.02.2008.
- [Roß04] Alexander Roßnagel. Signaturgesetzkonformität des Standardisierungsvorschlags “Long-Term Conservation of Electronic Signatures” für die ISIS-MTT Spezifikation vom 30.6.2004, July 2004. http://www.teletrust.de/fileadmin/files/ag8_isis-mtt-gutachten-langzeitsig.pdf, last checked 28.02.2008.
- [RS06] Alexander Roßnagel and Paul Schmücker. Beweiskräftige elektronische Archivierung – Bieten elektronische Signaturen Rechtssicherheit? Economica Verlagsgruppe Hüthig Jehle Rehm GmbH, Heidelberg, 2006.
- [Sch98] Wolfgang Schreiber. Handbuch des Wahlrechts zum Deutschen Bundestag. 1998.
- [Siga] German Electronic Signature Act (Gesetzliche Rahmenbedingungen für elektronische Signaturen, SigG). http://bundesrecht.juris.de/sigg_2001/index.html, last checked 13.02.2008.
- [Sigb] German Electronic Signature Ordinance (Verordnung zur elektronischen Signatur, SigV). http://bundesrecht.juris.de/sigv_2001/index.html, last checked 13.02.2008.
- [Tra] Legally Secure Transformations of Signed Documents. <http://www.transidoc.de>, last checked 20.01.2008.
- [VK06] Melanie Volkamer and Robert Krimmer. Online-Wahlen und die Forderung nach zeitlich unbegrenzt geheimen Wahlen. Working Paper Series on Electronic Voting and Participation, 02/2006, 2006.
- [WPB07] Carl Wallace, Ulrich Pordesch, and Ralf Brandner. Long-Term Archive Service Requirements. RFC, 4810, March 2007. <http://www.ietf.org/rfc/rfc4810.txt>, last checked 25.02.2008.

Session 4: Comparison of E-Voting

The E-Voting Readiness Index

Robert Krimmer, Ronald Schuster

E-Voting.CC
Competence Center for Electronic Voting and Participation
Pyrkerlgasse 33/1/2, A-1190 Vienna, Austria
[r.krimmer | r.schuster}@e-voting.cc](mailto:{r.krimmer|r.schuster}@e-voting.cc)

Abstract: The goal of this study is to analyse and compare the environment for the introduction of E-Voting. To do so a contextual model is developed and then applied with the value benefit analysis to compare 31 countries including all EU member states, and Russia, Switzerland, United States and Venezuela.

1 Introduction

The use of information and communication technology (ICT) in the electoral process is continuously rising around the world. While most of the applications emerge in the back-office, hence the administration of the election like electronic electoral registers or mandate calculate, ICT is finally reaching the home of the voters.

As can be seen in international gatherings of E-Voting experts, the discussion around is led very actively. The use of E-Voting machines has taken up in many countries, the uses of E-Voting in remote elections is in contrast still small in size [KTV07].

So far there has been only one study by Leenes and Svensson which could not identify a unique trend for the adoption of E-Voting other than that it is dependant from the context [LeSv03].

In the following we will introduce the methodology and give some first findings of our study.

2 Methodology

For our analysis of the E-Voting context, we needed on the one hand the contextual model where we identified the necessary dimensions to be used, and on the other hand the methodology to assess the countries.

2.1 Contextual Model

For the development of a contextual model for E-Voting we could use previous work, namely the work by Leenes/Svenson [LeSv03] and Moosmann/Baumberger [MoBa03]. These were integrated in our first approach as described in [Krim04], where four dimensions were identified: the political, legal, technological and social dimensions. These factors constitute the national (macro) level in contrast to the process (micro) level for the concrete application under investigation. These dimensions were also broken down in subdimensions.

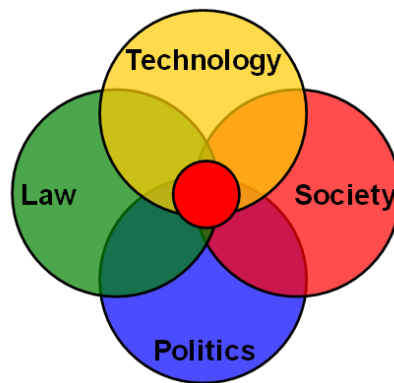


Figure 2: The Dimenions of E-Voting

We then extended this model using Pippa Norris's view [PiNo01, 11] where she distinguishes among three nested levels of analysis, as illustrated in figure 3. The national context, including the macro-level of technological, socioeconomic, and political environment, determines the diffusion of the Internet within each country. These three environments are similar to those from the previous model. The institutional context of the virtual political system provides the structure of opportunities mediating between citizens and the state, including the use of digital information and communication technologies by governments and civic society. Here the political process takes place. The individual or micro-level of resources and motivation determines who participates within the virtual political system. Norris' framework assumes that the national context, such as the process of technological diffusion, influences the development of the virtual political system. In turn, the core institutions of the political system available in the digital world provide the systematic context within individual citizens have opportunities to participate online. It is determined by the particular citizen, personal resources (time, money, skills) and their motivation to take advantage of these opportunities.

The final model consists of two levels to be explored:

- National level (Macro)
- Application level (Micro)

While the national level handles with E-Democracy environment in general, the level on project basis examines the application E-Voting. Regarding E-Democracy, the dimensions on the national view level which can be considered are divided as figure 3 shows:

- Information Society Context
- Political Context
- Legal Context Information

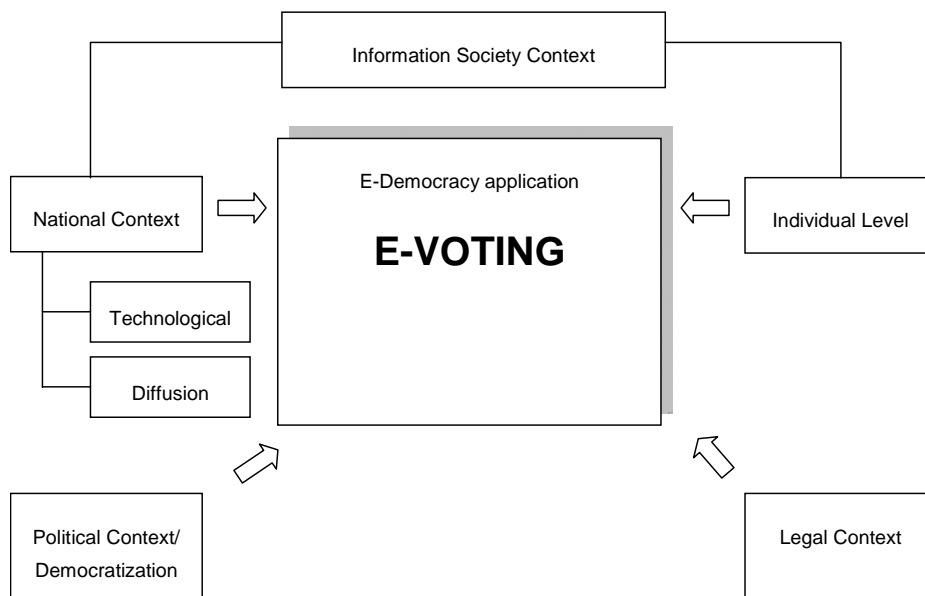


Figure 3: The E-Voting Readiness Index Contextual Model [RoSc07, 16]

The “information society context” is divided into “national context” and the “individual context” of the users whereby the latter is not considered in this work. The “national level” is further divided into “technological” and “diffusion”. In this dimension there are items like computer penetration, internet penetration to be measured as E-Democracy is an IT topic.

The “political context” considers the democratization of a country by measuring subdimensions like “institutional stability” or “stateness”. A stable democracy is necessary for the introduction of E-Democracy applications like E-Voting.

The “Legal Context” measures basics for democratic elections like election system or supplementary protocol for human rights that are required by a democracy.

Those dimensions that are relevant for E-Democracy have a great impact on a possible application like E-Voting. The result of the first stage “national view level” can be considered as an E-Democracy readiness scale.

The second stage to be measured is the application level with the application E-Voting that is influenced by the environment. This stage is divided into public and private projects to guarantee that individual experiences are not mixed with the development progress of the state and completes the E-Democracy readiness scale of the first stage to a complete E-Voting readiness scale.

For each of the dimensions numerous weighted indicators have been found that were grouped to weighted subdimension that are summed up to the dimensions. By summing up the weighted dimensions the E-Voting readiness can be explored.

The next table shows the dimensions and it’s subdimensions used.

| | E-Democracy Environment | | | Application E-Voting |
|---------------|---|---|--------------------------------------|-------------------------|
| DIMENSIONS | Information Society Context | Legal Context | Political Context | E-Voting Applicaton |
| SUBDIMENSIONS | Status of registers | Election System | Stateness | Public debate |
| | Status of eGovernment infrastructure | Supplementary protocol for human rights | Rule of law | Private elections |
| | Digital net infrastructure | Realization of Council of Europe recommendation | Stability of democratic institutions | Public elections |
| | Prices for the entrance to information and communication service and for the use of services | | Election system and turnout | |
| | Diffusion of information and communication services | | Political participation | |
| | Expenditures for information technologies and information and communication-referred services | | Political aims | |
| | Transaction penetration | | | |
| | Degree of the informatization in the public administration and of administrative expirations | | | |

Table 1: The Factors for the E-Voting Readiness Scale

2.2 Methodology

The requirement was to find a method that allows the analysis of different opportunities to reach a defined goal. Zangemeister's basic system of the value benefit analysis turned out to be useful setting up our methodology. He regards his method as analysis of a quantity of complex alternatives with the purpose of arranging the elements according to the preferences of the decision maker. Phases proposed are: (i) Definition of situation-relevant goals, (ii) description alternatives to reach a goal, (iii) a preference order of the alternatives due to the goals that have to be achieved. [Zang76, 45]

Using the value benefit analysis it becomes possible to include the non quantifiable use into an evaluation with and thus to eliminate the main difficulty creating costs using comparisons. We used the more specified approach from Stahlknecht and Hasenkamp [StHa05] who applied the value benefit analysis for assessing tenders in the IT-sector.

1. Listing and weighting of the criteria. The criteria relevant from the view of user are arranged and weighted proportionally. The sum of the weighting results in 100 percent.
2. Confrontation of the units of analysis. The units are confronted on the basis of the selected criteria.
3. Evaluation and scoring of the units of analysis. Each unit is evaluated regarding each criterion. The values are then multiplied according to the associated weights and the final values are added. Thus result into the individual utilizable value of the alternative.

We adapted this approach for our purposes as follows:

1. The superordinate goal is the development of the E-Voting readiness scale. In order to develop this scale, the relevant environmental dimensions must be identified (see 2.2).
2. Dimensions are divided into thematically matching subdimensions. These subdimensions contain the individual indicators. Each indicator is evaluated on a four-level scale, whereby alternative 1 describes the least favorable environment situation and therefore gets only 0,25 points and alternative 4 is the most favorable environment situation and gets 1 point.
3. Since the individual indicators do not have the same importance for the evaluation of a subdimension, these are weighted. The sum of the weighted criteria results in a number for the subdimension.
4. The subdimensions are weighted too as their contribution to the utilizable value for the dimensions are different. The sum of the weighted subdimensions is a number for the whole dimension expressing the utilizable value for the environment of the whole dimension.

5. Finally the different dimensions have to be weighted according to their importance of contribution to the E-Voting readiness. The sum of the weighted dimensions results in a number that expresses the E-Voting readiness.

The following figure represents this procedure.

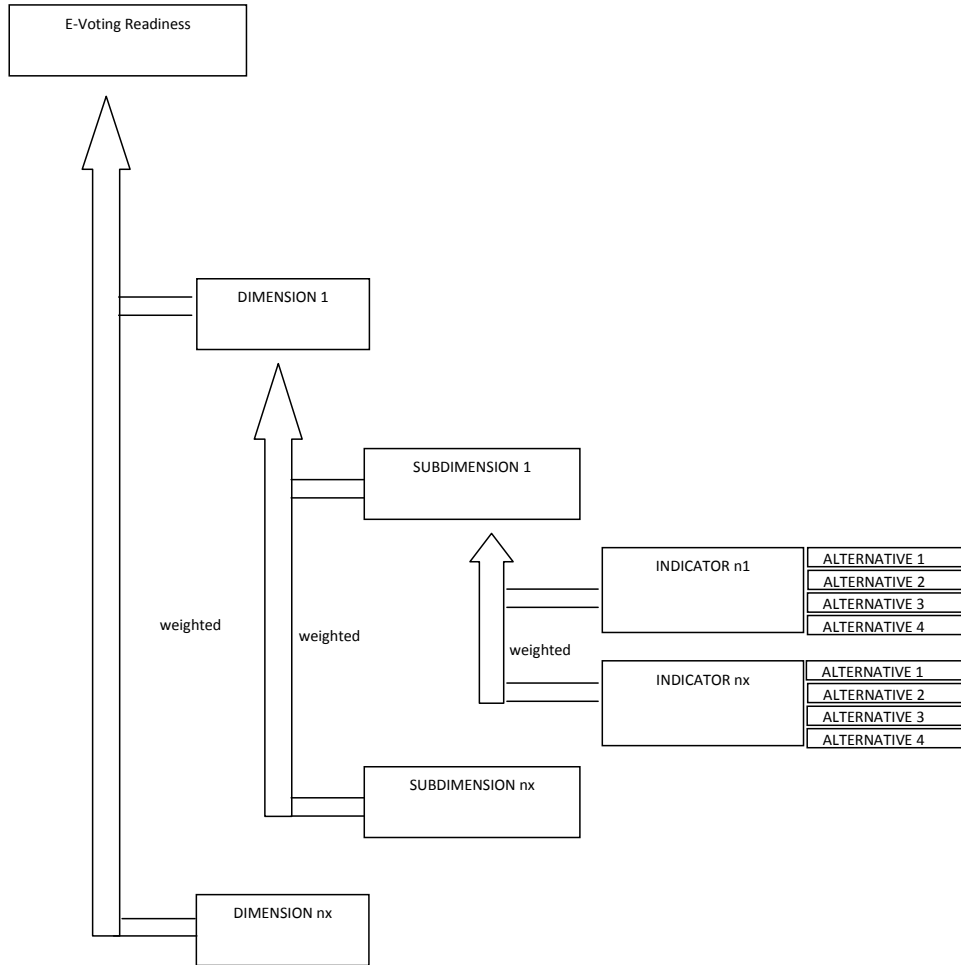


Figure 1: The Evaluation Procedure for the E-Voting Readiness Scale following the Value Benefit Analysis

3 Study

We used the above described methodology of a value benefit analysis together with the contextual model to answer our main question, which is to measure the progressiveness of countries in preparing the right context for E-Voting. To do so, we developed factors for each of the subdimensions to determine and measure the criteria. In the end we had 79 single factors (Political Context: 16, Legal Context: 10, Information Society Context: 29, E-Voting: 24). The next step was the weighting of the (sub) dimensions, and factors. We weighted the E-Voting with 40% and each of the three macro levels with 20%.

In the next step we identified 31 countries for the study. We included all 27 member states of the European Union, as well as relevant countries with E-Voting experiences where data was available: Russia, Switzerland, United States and Venezuela. The research team was extended by IT experts with native language skills and then used desktop research to collect the data and assessed the factors between 0,25 to 1.

As an example we will walk you through the process of classifying relevant dimensions with the example of Great Britain.

In order to be able to evaluate specific items we consulted research articles, press releases, experts and different sources in the World Wide Web. All data were collected twice. If we had divergences in data material we started further investigations.

The political context of Great Britain is well developed. Indicators evaluating the fields of constitutional state, stability of democratic institutions, political participation and political aims were scored at highest levels. We found restrictions in election turnout.

The legal context of Great Britain shows an excellent environment for E-Voting. We did not find any restrictions in the election system. There is no postal voting implemented, but advanced voting exists.

Concerning the IS context the major findings were: No citizen register is implemented. The voting register is organized de-central and electronically. Registration procedure for elections is the responsibility of government authorities. Digital signature is available. A Citizen card is considered to be introduced soon. E-Government standards are implemented. Indicators for penetration of computers, internet and mobile phones show values of 44.8 percent, 67 percent and 109 percent. Further internet transactions like online shopping and e-Government applications have been executed on a high level by citizens shortly below 40 percent. Just eight percent handle their finances electronically.

Great Britain tested all kinds of electronic voting: Voting machines, kiosk voting and I-Voting. There have been private electronic elections. Politically binding elections fulfill the comprehensive British experience: Voting machines in polling stations, kiosk voting and remote electronic voting.

The study resulted in the following weighted factors according to the four dimensions:

| | Political | Legal | InfSoc | E-Vote | Total |
|----------------|-----------|-------|--------|--------|-------|
| Austria | 19,58 | 14,20 | 14,04 | 12,13 | 59,96 |
| Belgium | 20,00 | 11,40 | 10,20 | 15,35 | 56,95 |
| Bulgaria | 15,33 | 8,40 | 4,17 | 1,47 | 29,37 |
| Cyprus | 14,58 | 8,40 | 5,19 | 0,00 | 28,17 |
| Czech Republic | 18,23 | 8,40 | 8,05 | 2,37 | 37,05 |
| Denmark | 20,00 | 17,00 | 8,99 | 8,55 | 54,54 |
| Estonia | 17,88 | 16,76 | 14,36 | 17,60 | 66,60 |
| Finland | 19,08 | 14,20 | 10,64 | 12,87 | 56,79 |
| France | 19,50 | 8,40 | 9,23 | 19,53 | 56,66 |
| Germany | 19,50 | 14,20 | 10,37 | 15,00 | 59,07 |
| Greece | 18,88 | 8,40 | 6,45 | 7,50 | 41,23 |
| Hungary | 19,00 | 8,40 | 9,41 | 2,50 | 39,31 |
| Ireland | 18,90 | 10,40 | 6,63 | 6,93 | 42,86 |
| Italy | 16,10 | 8,40 | 7,76 | 14,80 | 47,06 |
| Latvia | 18,00 | 8,40 | 4,76 | 3,47 | 34,63 |
| Lithuania | 17,00 | 8,40 | 5,23 | 5,47 | 36,10 |
| Luxembourg | 20,00 | 11,20 | 10,17 | 0,37 | 41,74 |
| Malta | 19,40 | 11,40 | 4,44 | 3,10 | 38,34 |
| Netherlands | 20,00 | 14,20 | 8,80 | 19,90 | 62,90 |
| Poland | 17,67 | 8,40 | 4,89 | 2,92 | 33,87 |
| Portugal | 19,00 | 11,20 | 7,92 | 14,92 | 53,04 |
| Romania | 15,38 | 8,40 | 4,97 | 5,13 | 33,88 |
| Russia | 13,57 | 8,40 | 5,61 | 10,30 | 37,88 |
| Slovakia | 15,27 | 16,30 | 6,07 | 6,57 | 44,20 |
| Slovenia | 19,00 | 11,20 | 6,01 | 4,35 | 40,56 |
| Spain | 18,08 | 8,40 | 9,44 | 17,43 | 53,36 |
| Sweden | 20,00 | 17,00 | 11,39 | 11,50 | 59,89 |
| Switzerland | 19,00 | 14,00 | 10,39 | 18,40 | 61,79 |
| United Kingdom | 19,15 | 11,50 | 8,60 | 31,35 | 70,60 |
| United States | 18,50 | 16,30 | 8,18 | 23,70 | 66,68 |
| Venezuela | 11,68 | 8,40 | 6,88 | 11,60 | 38,57 |

4 Conclusion

This project was an ambitious effort to the development of the contextual model and to collect the data. However the collected data and analysis will provide for a better understanding of the environment for E-Voting and in consequence it will benefit future research in the area. The future work will concentrate on finding significant relations between contextual factors and successful deployment of E-Voting.

References

- [PiNo01] Norris, P.: Digital Divide, Civic Engagement, Information Poverty and the Internet Worldwide, Cambridge University Press, Cambridge, 2001.
- [Krim04] Krimmer, R., Die Dimensionen der elektronischen Demokratie, in: Proceedings of IRIS 2004, Verlag Österreich, Salzburg 2004.
- [KTV07] Krimmer, R., Triessnig, S., Volkamer, V.: The Development of Remote E-Voting around the World: A Review of Roads and Directions. In: Alkassar, A., Volkamer, M.: VOTE-ID 07, Springer LNCS, 2007.
- [MoBa03] Moosmann, R., Baumberger, P.: E-Voting-Sicherheitskonzepte - eine vergleichende Studie (2003), Egovernment Präsenz, Zeitschrift des Institut für Wirtschaft und Verwaltung, Vol., 02, 2003.
- [RJSB03] Leenes, R., Svenson, J.: ICT in the Voting Process - A Report on 17 European Countries: University of Twente, 2003.
- [RoSc07] Schuster R.: Development of an e-Voting Readiness Scale, Diploma Thesis, Vienna, 2007.
- [StHa05] Stahlknecht P., Hasenkamp. U.: Einführung in die Wirtschaftsinformatik, (11th Ed.), Springer, Berlin – Heidelberg 2005.
- [Zang76] Zangemeister, C.: Nutzwertanalyse in der Systemtechnik, (4th Ed.), Wittmann, München, 1976.

Malfunction or Misfit: Comparing Requirements, Inputs, and Public Confidence Outcomes of E-Voting in the U.S. and Europe

E. John Sebes, Gregory A. Miller

Open Source Digital Voting Foundation
665 Lytton Ave., Palo Alto, CA, USA
<http://osdv.org>
{jsebes | gmiller}@osdv.org

Abstract: While European democracies are increasingly adopting e-voting technology – including remote voting via public networks – the e-voting experience in the U.S. has been one of disenchantment. The adoption of e-voting technology and outcomes in public confidence in elections processes and results are at significant variance between the U.S. and Europe. We argue that the causes of this variance are rooted in divergent inputs of political traditions that only loosely define systems requirements. In the case of the U.S., several factors, most notably balkanization of the elections processes, have led to the current situation where e-voting technology is a poor fit for unclear systems requirements that are only now becoming clearly understood. A comparative analysis of European and U.S. experiences is the basis for a solvable problem statement for the U.S. situation, together with a solution approach that is being attempted at present.

1 Introduction

Public confidence in the outcome of the use of digital voting technology (hereinafter referred to as “e-voting”) is very different in Europe as compared with the U.S. To take two of a great many examples, Swiss e-voting pilot projects [BB06] showed a dramatic increase in participation, via Web-based remote balloting, of habitual non-voters, while in the U.S. advocacy groups called for a return to non-electronic voting.

This striking difference is not merely a reflection of European technophilia and suspicious American technophobia. To understand what one might call “American e-voting dysfunction” we need to look at the American political tradition and the implicit technical and system requirements in our electoral process. We suggest a developmental model of five parts. Political traditions create often-inconsistent sets of elections process goals that create varying trust models, partially determining election system requirements, that are applied (or misapplied) to defining functional requirements for e-voting.

By comparing the U.S. and Europe in this developmental model, we can show how American e-voting dysfunction is as much a result of engineering misfit as it is of technical malfunctions—and indeed that the latter is a consequence of the former. This account of the technology misfit provides the framework for an approach to correcting e-voting dysfunction. This approach is a combination of developmental process, trust process, and functional fit. In addition to being a framework for the creation of sound e-voting systems, this combination is specifically designed to enable a public process of restoring voter confidence in e-voting as a beneficial (not merely neutral) component of an elections system.

2 From Political Traditions to Elections Process

Regarding elections and trust, the American political tradition in the 21st century is still very much based on experience in the 19th century, in at least these three regards: vote buying and coercion; polling-place election fraud; and election fraud in canvassing. Each of these concerns is not only a lasting concern in the American political tradition, but also a driver for formulation of present-day goals for election process, trust models, and system requirements for e-voting systems.

Vote buying and coercion are the most notable instances of voter fraud that are enabled by the lack of effective privacy for casting ballots. There are many historically documented forms [Ca05], but one example may suffice for purposes of comparison: the notorious role of the “precinct boss.” In the polling place of a politically corrupt precinct dominated by one political party, the role of a precinct boss was to observe each voter’s ballots to determine whether the voter voted in accordance with previous direction, and hence was eligible for reward or punishment.

Concerns over vote buying and coercion have historically been the drivers for the election process goal of the combination of privacy and anonymity in the voting process. More recently, these concerns have manifested in two ways concerning vote-by-mail. In one view, moving the balloting process away from the precinct polling place eliminates the opportunity for precinct-based organized, scalable (“wholesale”) coercion/bribery. In another view, large-scale mail voting enables coercion/bribery for a sufficiently large number of voters as to cast doubt on election result validity, especially in close elections. The latter appears to be the more prevalent position, though the actual incidence of this type of voter fraud is debated [MC03], particularly in the state of Oregon (state-wide vote by mail). As voluntary vote-by-mail participation in California has risen above 30%, it may be that parts of the American West are demonstrating a *wertewandel*, or mutation of values, concerning the link between privacy and coercion/bribery.

Vote-by-mail also shows a potential *wertewandel* concerning anonymity. Currently, a ballot is anonymous, but it may be enclosed in an envelope that identifies the voter. Identification is required to determine whether the putative voter is entitled to vote. This approach suggests that current voters may trust election officials not to correlate ballots and voters, despite their ability to do so.

Two other aspects of concern are forms of election fraud—one in the polling places (where access to ballots enables the insertion of spurious or fraudulent ballots); and the other as part of the canvassing process, where undesirable ballots are simply not counted. Many examples have been described [AB00] ranging from the canonical “stuffing the ballot box” to accidents in which a block of ballots is mislaid, invalidated, or simply not counted. Suspicions of fraud are raised when historical voting patterns indicate that the missing ballots could be expected to trend against the desire of elections officials.

These concerns essentially describe a lack of trust in elections officials and in the elected office-holders who have authority or influence over them. Perhaps the most notorious recent incident was in the Florida 2000 American Presidential race. Personal and partisan relationships among the Secretary of State (who had oversight of the elections), the Governor of the State, and the ultimate race winner (the Governor’s brother) permanently clouded election results. Although this and similar experiences sparked some excellent work on recommended election reforms [Ca02, Cr04], to date little work has been done to look at how e-voting technology can be trusted to support any of the suggested reforms.

2.1 Election Fraud and the Push to Automation

Election automation is perhaps the most striking and uniquely American result from a political tradition of high sensitivity to election fraud. In the late 19th century, states began using electro-mechanical voting machines that led to the lever machines that remained in wide use in some states as late as 2007. The main driver for adoption was the idea that the machines were more trustworthy by virtue of being less easily manipulated by elections officials to perform wholesale election fraud. This type of automation retained a great deal of public trust despite defects of low auditability, no ballot of reference, no paper trail, etc.

European countries certainly also have histories of election fraud, and real concern over how to structure elections to control it. However, the US may be unique in the degree of mistrust that creates a preference for automation over “pure manual” elections of hard-marked, hand-counted paper ballots.

2.2 Comparison of Election Goals

The elements of American political tradition drive a number of goals for elections processes: privacy of balloting; anonymity of balloting; minimization of distrust in both elected officials and elections officials; auditing and transparency of canvassing and other actions of elections officials. These goals in turn serve as drivers for trust models and systems requirements for e-voting. These goals – and how they define elections processes and technology – exist in marked contrast between the U.S. and many European countries, especially those that make greater use of e-voting. There are two distinct types of contrast: hearty adopters, and non-adopters of e-voting.

In the hearty adopter category are Estonia and parts of Switzerland. Many Swiss cantons have been encouraging vote-by-mail for some time in order to increase voter participation. Although, as noted above, vote-by-mail can create some concerns about anonymity and distrust of elections officials, neither of these values is as strongly held in the Swiss political tradition. Indeed, historically, non-anonymous town-square voting, e.g., a show of hands, was viewed as a traditional value for high-confidence elections.

Similarly, the anonymity concern over vote-by-mail seems largely absent, particularly with the extension to “Internet voting.” The high rate of participation in pilots, especially among habitual non-voters, shows a significant trust in elections officials’ proper use and dissemination of e-voting data. Anecdotal evidence from elections officials indicates pilot participants were not concerned about privacy, or at least correlation of voter identification and ballot. Participants in the pilot similarly trusted the technology involved, including the PCs, Web browsers, Web applications, the public Internet for communications, and Web application security standards for communication security. A similar set of values is indicated in the Estonian Internet voting experience, with the addition of increased reliance on technology for voting authentication and authorization.

In the non-adopter category are the Netherlands and Ireland. The Netherlands is notable for having effectively outlawed e-voting after nationwide adoption approached 100% in March 2006, with the vast majority of municipalities using the same election system. Shortly thereafter, a documented security issue of the system (described in [Gh07]) and public activism resulted in two government commission studies, the first of which reported that many safeguards thought to be essential to verifiable elections had been ignored because the new technology was not properly understood. The second commission’s report suggested the possible future use of open source systems for marking and counting paper ballots. The Dutch government acted to revoke its previous legal framework [Ne07] for defining voting machines for use in the Netherlands; subsequent elections have returned to manually counted paper ballots.

Ireland also conducts elections using manually counted paper ballots. The use of e-voting was seriously considered at one time, however. The Irish government created a Commission on Electronic Voting, which reported in 2004 that it could not recommend the use of an electronic system [Ce04]. Later work also failed to provide the basis for e-voting usage in Ireland, and the commission was dissolved in 2006. There seemed to be a lack of sufficient benefit for the cost and risk of e-voting. Although mitigation of electoral fraud was a potential benefit, it should by no means be taken as an indication of Irish indifference to the issue. Rather, Ireland’s rather infrequent (5 and 7 year terms mean that 2 years or more can go by between elections) and simple (often one measure and rarely more than five, each separately balloted) elections are subject to the structured process of manual counting with observation by the general public, and political party officials observing to perform independent counting. The structure and the avid observation may be related in part to the non-trivial method of tallying with Ireland’s form of the single transferable ballot.

By contrast, the American response to election fraud concerns has included the use of automation. While the particularly weighty American history (a political tradition of voter fraud, election fraud, corrupt elected officials and elections officials, often referred to *in toto* as “machine politics”) of fraud may be one factor, the much higher complexity and frequency of elections may contribute as well.

2.3 Election Complexity and the Push to Automation

American election officials may well look with envy on feasibly hand-counted single-contest ballots, with feasible public visibility of counting – even if they are proponents of e-voting. Election complexity arises partly from a more complex governmental structure than many European countries, resulting in more frequent elections with more contests. Yet some European countries have a similar degree of complexity of offices, and have not adopted e-voting – France is perhaps the best example.

Another fact in election complexity is the result of another form of balkanization, coupled with response to another legacy of American “machine politics” – cronyism, nepotism, patronage, and similar ways in which elected officials use their power of appointing government officials, for their own personal gain. This part of the American political tradition has led to a frequent practice of electing officials that in other times or in other jurisdictions were appointed. The balkanization effect arises from the fact that these locally elected offices are for jurisdictions that are not co-extensive with legislative or local jurisdictions. For example, some parts of a county will be in one school district or another; of the parts that are in one school district, one subset will be in a different water district. A not infrequent result is that in some counties, almost every voting place has a distinct ballot with a distinct set of contests. One anecdotal example: by the time the next President of the U.S. is elected, one author will have voted 4 times in 367 days for a total number of contests numbering at least 30 and likely over 40, in jurisdictions that include: multiple county offices and referenda, offices or referenda from at least 3 local jurisdictions (fire district, harbour district, coastal commission), state and federal offices, and all in a “light year” in which municipal offices, state executive officials, and federal senators are not up for election.

In short, a history of fraud has led to a desire to use automation to mitigate the vulnerability of pure manual paper-based elections, while a history of fraud and patronage has led to a high degree of complexity which elections officials are motivated to manage with automation. Pressure from both sides has encouraged automation in the U.S. for over a century, while public trust in the process has eroded in the more recent past. These two trends may help explain why the American election system is problematic regardless of automation, and in a way that drives automation without trust or even a central or consensual model for trust.

3 From Elections Process Goals to Trust Models

Derived from American political traditions, elections process goals in turn drive trust models for elections and for the reflection of them in a digital voting system. To properly understand e-voting trust models, two aspects of the previous statement are critical: the idea of plural models of trust, and a trend toward trust minimization.

First, the plurality of trust models is derived from a fundamental and critical aspect of U.S. elections systems—an aspect which might be called “balkanization.” That is, the U.S. Federal government delegates to states the responsibility for Federal elections. States delegate to county elections officials. Each county, therefore, represents a distinct elections body, making its own choices about election processes, with distinct but (typically) limited regulations or guidance from the state. Each state also makes its own elections laws and regulations within a minimal set of Federal requirements. Not only is there no central or standard regulation or guidance on how to conduct elections (and hence what trust properties an elections process should have), the number of variants is at least two orders of magnitude (dozens of counties in many of the 50 states) larger than in European countries with devolved Federal elections, e.g., Switzerland and France. At the far end of the spectrum are unitary democracies in which the central government regulates how municipalities conduct elections, and most contests are for either one level of local government, or for one legislative representative. In the Netherlands for example, it is not uncommon for an election to consist of just one contest.

We would also argue that current U.S. elections are conducted with a distinct default of mistrust, or at least a goal of minimizing trust and increasing transparency and public auditability. The trend seems to be increasingly in this direction, not only in the realm of public advocacy (particularly in the area of verifiable voting) and public opinion, but also of elected officials. For example, California’s Humboldt County is one of the counties in which the chief elections official is pursuing transparency by developing a system for capturing electronic images of all ballots and electronically publishing the set of images. At the state level, again in California, the office of the Secretary of State (regulating county elections officials’ activity) recently issued a set of guidelines for polling place physical security practices and for an auditable chain of custody of constrained data items—such as paper ballots and magnetic media—that record electronically cast ballots. Vigorously pursuing these guidelines, only three counties received cognizance of full compliance—and hence the full ability to utilize e-voting in the February 2008 election.

A third factor is complexity of government structure and oversight over elections. In the US, there is often a variety of partisan elected officials (at the local, county, and state levels) who can influence the way an election is conducted. Not only can election integrity appear to be affected by partisan officials, there is a sometimes complex array of such officials. Further compounding the complexity is that in cases of legal dispute, judicial officials may be notably publicly partisan, or may be elected judicial officials who may be seen as not neutral on issues of the election process. Of course, partisan politics also affects public trust in European elections as well. However, in the US, this trust factor is exacerbated by complexity and is combined with the other factors above.

These three characteristics contribute to the lack of a coherent model of trust in our elections process. A model of trust must consider what roles and operations are trusted with what constraints (e.g., in pursuit of anonymity), and associated controls and logging for auditability. Lacking a definitive trust model for an elections process, it is nearly impossible to derive the basis for trust in e-voting systems—systems that automate parts of the existing election process, much less systems that require modification of the existing process. This lack is greatly exacerbated by the range of trust attitudes, e.g., Oregon and California vs. states that attempt to regulate absentee voting.

3.1 Comparison of Elections Process Goals and Trust

European countries are certainly not uniform in centralization of elections functions or regulations over those functions, not even the countries making more extensive use of e-voting. However, some European voting jurisdictions—for example, the country of Estonia [MM05], or the Swiss cantons that implemented Internet-enabled remote voting—have been clear enough about the elections process and trust to be able to implement aggressive (by U.S. standards) e-voting systems with clear technical requirements. The key differentiator (by contrast with the U.S.) is the active role of the voting authorities (national or cantonal) in the implementation of remote voting.

A different contrast to the U.S. is offered by countries that have explicitly rejected e-voting. Irish experience (in selecting, acquiring, piloting, and studying an e-voting system) was driven by the central government empowered to set goals and empanel commissions to assess a system with respect to those goals. The Dutch experience was even more specific, with the central government creating specific regulations defining voting technology for use by municipalities. When it became apparent that the main e-voting system in use did not conform to regulations, and in addition had serious defects out of scope of the regulations, the Dutch government was empowered to retract the regulation (effectively barring e-voting) and empanel studies to recommend policies to be decided by the central government to regulate the entire country.

Both these types of experience could be said to be a successful outcome with e-voting, in that it became clear whether or not available e-voting technology met the goals for its use. The U.S., by contrast, has no such uniform outcome, or indeed any outcome that is stable for multiple election cycles. Unlike the hearty adopters, county elections offices and the offices of Secretaries of State have had low to no direct involvement in the implementation of e-voting systems and the processes that they automate. Rather, these many, many governmental organizations have acted in the role of a traditional consumer of packaged technology, selecting from a few vendors those systems that seemed to best meet state or local needs. One measure of the lack of positive outcome of this approach is the result of the review, performed for the Office of the Secretary of State of California, of all the polling-place and/or canvassing e-voting systems that had previously been certified by the Office for use in California. Reviewed systems were all de-certified, and only three systems re-certified for limited use for accessibility, with a proviso requiring significantly improved physical and procedural security methods and auditing [So03].

Although the grounds for rejection were mainly based on system security and information security considerations, the overarching question is how these systems came to be used in the first place. Further, how is it that in European experiences the systems used were deemed fit to meet their requirements for use, or specifically unfit? We hypothesize that the European experience was more successful because of the existence of a central body which had authority to define or review proposed requirements, the authority and ability to correlate product requirements with trust requirements; the ability to work with technology vendors to obtain e-voting systems that putatively [a] fit the trust model; and b] are a reasonably close fit to overall systems requirements; and the ability and authority to assess and decide whether systems were in fact fit for use in specific terms.

This combination may have enabled either a definitive rejection of e-voting, or a more multilateral and deliberate process of design, implementation and deployment ([Bo06] describes another such example) than is the typical experience in a U.S. county elections office.

4 From Trust Model(s) to E-Voting Requirements

Whether the above conjecture is valid or not, the facts of life in U.S. elections today are that at present no U.S. county or state will be in as advantageous a position as that we conjecture for some European elections bodies. Balkanization, combined with the packaged product model, have created misfit systems, and have not created a profit motive or market incentive for current or new vendors to create revised or new proprietary products that are a better fit. One overarching reason is the number of jurisdictions; it's not feasible for vendors to obtain, let alone satisfy with products, a set of system requirements that meets the needs – including trust – of even a majority of the jurisdictions. Conversely, elections officials in many jurisdictions are oriented to “making due” with available technology under state or Federal deadlines rather than defining requirements and finding systems that fit them.

Given this situation, the misfit of current U.S. e-voting systems is hardly surprising, and certainly not the result of any lack of effort on the part of the vendors. Given no coherent set of goals, let alone requirements, and no model for how the e-voting systems could be trusted, the vendors had little scope for excellence of fit.

Furthermore, the time-to-market motive—particularly for a fixed set of funds allocated to states by the Federal government's HAVA act [Ha02]—resulted in systems where the misfit resulted in visible malfunction, perceived unreliability, or difficulty of administering, and a growing suspicion about security and integrity. The result has been a general decrease in public confidence.

4.1 Comparison of Trust and E-Voting Requirements

As noted above, the more successful efforts in European e-voting have involved systems that were not off-the-shelf devices, but rather systems developed via bespoke systems integration with a significant degree of stated requirements and a trust model that if not explicit, can be derived for the resulting system and the public confidence outcome of using it.

By contrast, the complex and sometimes historically ugly American political tradition has resulted in a large number of jurisdictions that share, to a varying extent, a particular distrust in elections processes and officials, or at least a dominant pessimism about their integrity, combined with a desire for transparency and verifiability. As a result, American e-voting systems are rather a paradox in that the electorate is implicitly expected to trust computers to partially automate elections processes that are themselves not trusted. At the outset, this is a marginally tenable expectation given most voters' less-than-happy experiences with the reliability, integrity, and security of the personal computers they use. Tenability is strained more with the addition of press coverage of voting device insecurity and election technical snafus.

4.2 Approach to Technical Development Towards Public Confidence

At first inspection, the current situation in the U.S., and the comparison with more positive European outcomes of voter experience and public confidence—not only in similar polling-place e-voting scenarios but also in more aggressive remote e-voting—seems unhopeful for marked improvement.

However, the developmental model, and the approach to development within it, suggests that improvement is possible. We do expect initially to develop e-voting systems requirements to match a coherent trust model or set of elections systems goals. Instead, we use a trust framework rather than a single model, and initially develop requirements bottom up from existing elections processes and the non-misfit functionality of existing e-voting systems. The resulting approach is based on three tenets:

1. Despite the lack of a single trust model or a central authority with the means to even vaguely define one, it is possible to create a trust framework that enables both a public process of determining whether specific e-voting systems are trustworthy, as well as a systems development process that can be performed with this trust framework in mind.
2. Existing e-voting systems, in conjunction with a trust framework, can form the basis for deriving election system requirements and functional requirements for specific e-voting devices – especially polling-place devices that are the focus of most of the controversy that strains public confidence.

3. This process and framework require no small efforts to achieve, and the effort is not in the economic interests of vendors or the current operational scope of Federal entities – though some efforts in the latter area may be helpful. However, if the efforts were carried out strictly in pursuit of the public good, and were successful in creating relevant results, then these results could be suitable for adoption and extension by creators of e-voting systems and by Federal and state government organizations with responsibility for elections.

The remainder of this paper describes the trust framework, the method of creating requirements, and the plan for proof-of-concept activities being undertaken by the Open Source Digital Voting Foundation (hereinafter “OSDV”).

5 “Trust Framework” Defined

The OSDV approach defines a trust framework in a way that is fairly conventional for high assurance dedicated systems, such as aerospace systems, military systems, and other high-integrity or high-security systems that are fixed-function, dedicated or embedded systems. We observe that many types of e-voting systems (including, but not limited to polling place devices) are or should be fixed function systems that could be trustworthy.

The foundational definition is that a trustworthy device or system does all and only what it is designed to do. A trust framework enables assurance that a particular system is in fact trustworthy. For any particular system, the goal of a trust framework is to be specific about the functions a system is supposed to perform, and how that system could be independently assessed as performing only and all of those functions. The elements of a trust framework are:

Specifications: specific, prescriptive written documentation that defines a particular system and its functions. An implementation of such a specification could be trustworthy if it could be assessed as being conformant to the specification, performing all and only the functions in the specification. As an example of a high-assurance system specification, some Common Criteria Protection Profiles could be considered a specification in this sense. Some U.S. military system “Concept of Operations” documents are good examples of documents that capture a portion of what constitutes a high-assurance specification.

Reference Implementations: a set of hardware and software that implements the specification or a documented subset of the specification, typically with expediency taking priority over other commercially relevant properties. Rapid prototypes of a reference implementation can help to clarify the specification. Even partially complete reference implementations can provide a working example of a trustworthy system, both for proof-of-concept and illustration for others’ work on a complete system.

Assessment Guidelines: documentation that specifically describes a methodology for evaluating an implementation of a particular specification. The process of independent assessment is used to evaluate whether a given implementation meets the specification and satisfies other aspects of high assurance, such as software quality. Assessment guidelines are required to enable consistency of assessment efforts across multiple assessments of a system type, and across the efforts of multiple assessors.

Open Assessment Work Examples: Documentation of methods used, findings, results, and overall judgment supported thereby, as a result of the efforts of a complete assessment. System assurance assessments can only assist in building trust and public confidence if the process is transparent and the results are publicly available and vetted. Worked examples of assessment efforts and findings, even undertaken on partial reference implementations, can have a beneficial effect on the clarity of guidelines documents, and serve as a proof-of-concept of the level of effort and feasibility of assessment of a particular specification using corresponding guidelines.

The OSDV approach is to apply this traditional trusted systems approach with related high-assurance systems methodologies to the specifications, reference implementations, open assessments, and documentation of methodologies for e-voting systems. Existing products can serve as the basis for the functional descriptions that are components of a specification for existing product types.

Such efforts have begun on a common system platform for a variety of types of e-voting systems. Platform efforts will be validated in a parallel project to develop e-voting systems based on it, starting with a ballot-scanning device. These efforts are initially focused on polling place devices—as these have caused the most publicly visible effects on voter confidence—but are not intended to be limited to them.

6 The Future: Feasible Development and Assessment of Trustworthy Systems

Assuming that the above efforts are fruitful as envisioned, how might the efforts and results have a markedly positive impact on the current American e-voting dysfunction? One major impact would be to enable a transparently refereed and government supervised evaluation process, similar in some ways to both Common Criteria evaluations performed by today's CCTLs, and to the voting system assessments currently performed for vendors by 3rd parties, in a new program operated by the U.S. National Institute for Standards & Technology (NIST) at the behest of the U.S. Elections Assistance Commission (EAC) [Ea07]. The former types of efforts are standards-based, but intentionally broad and can be burdensome and expensive. The latter are specific to e-voting, but lack public visibility, and cannot be shown to produce consistent results because there are no documented, commonly used (or de-facto standard) system specifications or assessment methods. The OSDV approach will produce results that can fill those gaps in some significant measure.

It is conceivable that in the future, states' certification efforts could be based on the results of transparent, independent evaluations that are feasible and consistent as a result of using standard system specifications and assessment guidelines, together with assessment findings reviews. These standards would be based on OSDV work product, which would have been already proven as usable by other OSDV results in reference implementation, worked example assessment, and public demonstrations. Certainly, the appropriate standards bodies could develop similar standards, but the authors hope the OSDV can fairly quickly develop and validate its work with rapid prototyping and parallel development. The authors envision the OSDV results to be usable during a standards process that would be much shorter as based on the OSDV results than starting afresh with standards committees. We also expect the OSDV results to be complementary to (or in some cases re-use or incorporate by reference) the results of existing work, most notably the U.S. EAC VVSG [Tg07] and work in the U.S. ACCURATE Project [Ac07].

Toward this future, the OSDV Foundation plans to have its reference implementations undergo third party assessment, as well as state certification. Leveraging these results, the OSDV technology transfer plan includes a monetary motivation for others (commercial or public entities) to adopt OSDV technology as the basis for future products: the use of existing, already evaluated platform and core application functionality. This type of adoption could enable product assessments that focus only on extensions outside of the evaluated platform, and be performed more rapidly and cheaply than evaluations of entire systems or revisions to entire systems.

7 The Present: A Digital Public Works Project

Given that vision of future impact, we can describe the current work of the OSDV Foundation as being similar to public works projects and having the following characteristics: based on requirements gathered from existing elections processes; starting from a "blank slate" of functional and trust requirements, without the need to be based on any existing e-voting system; developed transparently in the public eye for the public good, without the motives of commercial gain; performing specification, documentation, prototyping, and assessment efforts in parallel with feedback among these efforts; producing results with proof-of-concept and working examples to validate results. Based on the characteristics, the goal is to deliver proof-of-concepts systems that are developed and documented to be clear about (a) supporting, enabling, and not detracting from election systems requirements discussed above; and (b) the extent and limits of trust required and assumed in the operational environment.

Given these characteristics, we expect OSDV results to provide for the development of systems that could demonstrably support multiple combinations of election system requirements, as well as some well-defined models of trust allocated between technology, practices, physical security, audit, etc.

8 Summary

By comparing European and American experiences, we have argued that current e-voting dysfunction in the U.S. is not based primarily on the use of systems that malfunction due to poor quality, but rather from using commodity systems that are the result of a sometimes hasty and sometimes nearly requirements-free process of development and deployment. Such systems are misfit for their usage and environment because they fail to meet some unstated trust and integrity requirements that might have been derived from a coherent set of trust model and elections process goals—if such a set existed. In the U.S., however, there is no single trust model or single set of explicit (regulatory and legal) requirements, or implicit (operational and design) requirements, but rather a plethora of them. As a result, experience with misfit e-voting technology has drained U.S. public confidence in elections, and created an untenable situation with respect to trust of integrity in e-voting systems.

We have described a partly abductive approach in which we derive system and trust requirements and developmental methodology, by reasoning backwards from both fitting and mis-fitting characteristics of current e-voting devices. We have related this approach to existing misfits, malfunctions, and press coverage that have raised an already high bar in the U.S. (compared with Europe) for trust in elections processes and automation of them. We have described a trust framework and high assurance development methodology that is intended to meet that high bar of trust, and provided a potential model for adoption of OSDV work in that framework.

The overarching goal for adoption is enabling increased U.S. public confidence in e-voting technology and elections in jurisdictions that choose to use high-assurance trustworthy e-voting technology. These intended results will not necessarily be an immediate fit for the needs of a large number of U.S. jurisdictions. However, OSDV results can provide a concrete basis for credible claims of trustworthy systems (a milestone in e-voting in itself), and for iteration of functional requirements to meet specific jurisdictional needs. In addition, the basis for iteration, combined with explicit functional and trust requirements, could further enable some convergence of requirements in multiple jurisdictions, mitigating some effects of the large number of U.S. counties and states.

References

- [AB00] Glenn C. Altschuler and Stuart M. Blumin, *Rude Republic: Americans and their Politics in the Nineteenth Century*, (Princeton: Princeton University Press, 2000).
- [Ac07] 2007 Annual Report, ACCURATE: A Center for Correct Usable Reliable Auditable and Transparent Elections, 21 January 2008, <http://accurate-voting.org/wp-content/uploads/2008/01/2007.annual.report.pdf>
- [BB06] Dr. Nadja Braun, Daniel Brändli, *Swiss E-Voting Pilot Projects: Evaluation, Analysis and How to Proceed*, in *Electronic Voting 2006*, Robert Krimmer, ed., *Lecture Notes in Informatics (LNI) – Proceedings*, (Gesellschaft für Informatik, Bonn 2006).

- [Bo06] Carol Boughton, Maintaining Democratic Values in e-Voting with eVACS®, in Electronic Voting 2006, Robert Krimmer, ed., Lecture Notes in Informatics (LNI) – Proceedings, (Gesellschaft für Informatik, Bonn 2006).
- [Ca02] Jimmy Carter, Gerald R. Ford, Lloyd N. Cutler, Robert H. Michel, To Assure Pride and Confidence in the Electoral Process, Report of the National Commission on Federal Election Reform, (Brookings Institution Press, Washington, D.C., 2002).
- [Ca05] Tracy Campbell, Deliver the Vote: a History of Election Fraud, an American Political Tradition – 1724-2004 (New York: Carroll & Graf, 2005).
- [Ce04] Commission on Electronic Voting, “Interim Report of the Commission on Electronic Voting on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System”, March 2006.
- [Cr04] Ann N. Crigler, Marion R. Just, Edward J. McCaffery, Rethinking the Vote: The Politics and Prospects of American Election Reform, (Oxford University Press, 2004).
- [Ea07] United States Election Assistance Commission, EAC Receives Lab Recommendations from NIST, (Press Release 18 January 2007). <http://www.eac.gov/News/press/docs/01-18-07-eac-receives-lab-recommendations-from-nist>
- [GH07] Rop Gonggrijp and Willem-Jan Hengeveld “Studying the Nedap/Groenendaal ES3B voting computer a computer security perspective” 2007 USENIX/ACCURATE Electronic Voting Technology Workshop, Boston, USA.
- [Ha02] Help America Vote Act of 2002, United States Public Law 107-252, 107th Congress, http://www.fec.gov/hava/law_ext.txt
- [MC03] Lorraine C. Minnite, David Callahan, Securing the Vote: An Analysis of Election Fraud, (New York: Demos, A Network for Ideas and Action, 2003).
- [MM05] Ülle Madise, Tarvi Martens, E-Voting in Estonia 2005: The First Practice of Country-Wide Binding Internet Voting in the World, in Electronic Voting 2006, Robert Krimmer, ed., Lecture Notes in Informatics (LNI) – Proceedings, (Gesellschaft für Informatik, Bonn 2006).
- [Ne07] Intrekking Regeling voorwaarden en goedkeuring stemmachines 1997, Uit: Staatscourant 19 oktober 2007, nr. 203 / page 10.
- [So03] Office of the Secretary of State of California, Secretary of State Debra Bowen Moves to Strengthen Voter Confidence in Election Security Following Top-to-Bottom Review of Voting Systems, (Press Release 3 August 2003). http://sos.ca.gov/elections/voting_systems/tbr/db07_042_tbr_system_decisions_release.pdf
- [Tg07] Technical Guidelines Development Committee, Voluntary Voting System Guidelines, Draft, (United States Election Assistance Commission, 09/06/2007).

Session 5: Verification of E-Voting

Simple and Secure Electronic Voting with Prêt à Voter

David Lundin

University of Surrey, Guildford, Surrey, UK
d.lundin@surrey.ac.uk

Abstract: Prêt à Voter is an electronic voting system with very high security properties. We aim to make the system truly usable and applicable in elections with many races and candidates by allowing the vote to be formed using a voting machine and by printing a minimalistic receipt. We also introduce the procedure/technology mix concept to describe the use of procedures, people and technology to secure electronic voting systems.

1 Introduction

Implementing Prêt à Voter as it is described in a series of papers [Rya05, CRS05, RP05, RP06a, RS06a, Rya07b, LTR+06a, LTR+06b, XSH+07, LR08] has an associated set of fairly hard problems not envisaged by the authors, such as reliable optical character recognition (OCR), multi-page ballot forms in elections where there are many candidates contending many different races, chain of custody issues relating to pre-printed ballot forms, key distribution problems relating to on-demand printed ballot forms, and so forth.

Anecdotal evidence suggests that politicians and civil servants, in Europe and perhaps around the world, are concerned with the accessibility and applicability of electronic voting systems to a higher degree and cutting-edge security technology to a lesser degree than seemingly realised by researchers in the electronic voting field. Consider, for example, the impossibility for a civil servant in a country in continental Europe where there may, for example, be 28 candidates in each of seven races contended on the same ballot form to implement Prêt à Voter 2005 or 2006—the ballot form is simply too large to be scanned.

Further, anecdotal evidence suggests that a major contributor to decisions to use electronic voting in Europe is to simplify the process. For example, when the City of Hamburg, Germany, changed its electoral law it almost became a necessity to use some form of electronic counting of the votes as this would take days and weeks to do by hand [VV06]. The decision was taken to implement a completely new system based on Anoto pens and although this system was very accessible and had some procedures to safeguard the accuracy of the election, it seems it lacked sufficient technical guarantees.

This paper proposes a configuration of the Prêt à Voter electronic voting system in its later guises with emphasis on usability, accessibility and simplicity. Due to limitations to the length of this paper it has been necessary to leave out some technical detail but references provide this detail where necessary.

2 Preliminaries

In this section we describe the properties of end-to-end verifiable systems and introduce the procedure/technology concept.

2.1 End-to-End Verifiability

The will to elect leaders and representatives stems from a mass of people, equal, who have organised and created states and institutions to serve the population. From this philosophical point of view, some may say that once leaders were first democratically elected, they created election authorities and thus these are trustworthy and able to run fair elections for the people. Others are more reluctant to place such trust with such authorities. Consider, for example, some of those states in the world today that wish to disguise an undemocratic rule by holding unfair general elections. The most effective weapon against this at the disposal of the world's truly democratic nations is election observation.

However, election observation is a very blunt instrument with tremendous organisational and budgetary requirements. Although essential, election observation can only function as an audit of the procedures in place to safeguard the election and it is impossible to know, or prove, that the audit is sufficiently complete to allow conclusions to be drawn about the secrecy and fairness of the election.

This suggests that it would be more beneficial, if possible, to audit the election as a whole rather than some subset of the procedures involved. The ability to audit the whole election and (perhaps mathematically) prove that the outcome is exactly as indicated by the voters on election day has been given the name end-to-end verifiability and there exist many systems aiming to do this [AR06, ABBD04, ACvdG07, BFP+01, BT94, Cha04, CRS05, CGS97, FCS06, FOO92, JCJ05, LBD+03, NA03, OMA+99, Pun, Riv06]. There may be other ways of achieving this but we consider end-to-end verifiability a combination of two other: *voter verifiability* and *public verifiability*.

Voter verifiability The voter is given a receipt which she can use to check after the close of the election that her vote has been included in the tally. In order for the system to be coercion resistant, the receipt must not reveal the vote.

Public verifiability Any interested person or organisation can, perhaps using software, check that all the encrypted receipts are properly decrypted into plain text votes and that these are tallied correctly.

2.2 The Procedure/Technology Mix

We confess that we would rather employ a technological solution to security issues in electronic voting systems than a procedural one, but here feel obliged to introduce the *procedure/technology mix*. This is simply the mix of technology, procedures and people that constitutes any electronic voting system.

In the previous section, we claimed that the use of end-to-end verifiability would render the auditing of procedures and people obsolete. This is certainly true regarding the correctness of the outcome of the election; it is simply possible to prove whether the reported outcome is correct or not and if not, find the source of the error.

However, the *secrecy* of the election is, of course, a kind of property that once leaked cannot be “proven” back to secrecy. Furthermore, end-to-end verifiability is unfortunately very hard to achieve with technology only. Consider, for example, a theoretical system, the accuracy and secrecy of which depends on each voting device having its own secret private key. The distribution of these keys is, in fact, a procedural solution to both the accuracy and secrecy problems!

It therefore seems logical that the secrecy of the election is safeguarded by some mix of technology and procedures and we advocate a use of procedures to increase the accessibility of the system where a technological solution would reduce it.

3 Simpler Prêt `a Voter

3.1 Motivation

Our work with the first Prêt à Voter implementation and the subsequent demonstrations have resulted in the identification of two main problems impeding the progress toward the running of a general election:

1. *OCR*. The Optical Character Recognition (*OCR*) used in the first version of the system was not very robust and in order to interpret the marks as successfully as possible, it required the voter to use a seven segment display (like those you see in *LED* clocks) and a thick pen. Although all agreed that the success rate of the *OCR* can be increased, there was strong opposition from those with particular experience of implementing voting schemes against the seven segment display. It was felt that these were too cumbersome and hard to understand. We realise that this is not acceptable in a general election as such a voting system is used rarely by voters and this would introduce a large proportion of errors.

2. *Scanning*. The sheet-feed scanning of the ballot form is evidently very hard to use in elections where there are a number of races and/or a large number of candidates — election law may also stipulate that all races and candidates are printed on a single sheet, making this sheet immensely large. Furthermore, the layout of the ballot form would require that all candidates and their “boxes” were printed along the vertical axis of the paper, further limiting the number of races and candidates that can be printed on any piece of paper. Unfortunately, although that version of the Prêt à Voter implementation did support many concurrent different ballot forms, it did not support the spanning of a single race over more than one ballot form.

The motivation for this configuration of Prêt à Voter is thus simplicity, accessibility and the accommodation of a very large number of candidates. This introduces some procedural safeguards where technological safeguards have previously been envisaged [RS06b, Rya07b]. We argue that this is not only necessary but that it is so important to include as many voters and introduce as few errors as possible in the voting process, and that the procedure/technology mix must be adjusted.

3.2 The Voting Ceremony

In the polling station there are a certain number of voting machines placed in voting booths. The secrecy of the election is based on these voting booths providing proper privacy to the voter and the voting machine similarly being unable to leak the intention of the voter. Thus, there are poll station workers and guards keeping the area under surveillance in order to ensure that the machines cannot be tampered with.³²

The voter is able to enter the polling station without first identifying herself to the poll station staff and she can enter a voting booth so as to interact with the voting machine. It is important that she not be required to identify herself before she can interact with the machine because this makes it harder for the poll station staff or machine to connect the will expressed in the interaction with the machine to a particular voter.

The main purpose of the voting machine is to help the voter express her will in the election, the difficulty of which depends on the election system in place and the abilities of the voter. As the voter is interacting with a computer to make her choices, the accessibility of the system is in itself an important area of research. It thus serves little use to go further into the details of how the voter interacts with the system to indicate her choices and it is sufficient to say that she may do so using her sight, touch and/or hearing and a touch screen, mouse, voice or other input device(s). At the end of the interaction the voting machine prints a vote in plain text (see Section 4.4) which the voter takes away and casts.

³² Note that the accuracy is not threatened by this leak of information: but the privacy of the election is.

Interacting with the machine in the voting booth, the voter is able to produce some maximum number of votes. This must be a number greater than one so that the voter is able to create one vote that correctly captures her intention and some number of other votes that she can choose to audit, see below. The voting machine does not, therefore, know whether a vote it helps to construct will be audited or if it will be cast. It should therefore be disinclined to cheat (or malfunction) because there is some likelihood that it will be found out and taken out of commission. In order to stop voters from occupying voting booths too long and thus stopping others from voting, election law may stipulate some maximum number of votes, such as five or ten, which would be quite sufficient for the purpose.

When the receipt is printed by the machine, the voter can read it through and ensure that it is the vote she indicated to the machine. She turns the vote she is going to cast into an encrypted receipt (see below). Any or all of the other votes she may have created she is able to have audited by approaching an auditing desk. The barcodes on these ballot forms are scanned in by poll station workers and the forms are decrypted and the information printed. The voter is now able to check that the printed information does correspond to the vote she has just audited, indicating this vote was correctly formed. If so, she will grow more confident that the vote she will submit is also correctly formed.

Finally, the voter approaches a submission desk with the encrypted receipt she wishes to submit. She identifies herself to poll station workers and the barcode on the encrypted receipt is scanned and the contents of it are electronically submitted to a central repository (and may be noted next to the name of the voter who has cast it). Note that no submitted data need be kept secret to safeguard the secrecy of the election; it is already encrypted. After the close of the election, this, and all other encrypted receipts, will be decrypted as described in Section 4.7. A stamp is placed on the encrypted receipt by officials, indicating it has been submitted.

The voter can now leave the poll station with her encrypted receipt, and after the close of the election she can use a website to check for the inclusion of her vote in the tally. She does this by entering the serial number of her encrypted receipt and comparing the image of the receipt served by the website with the actual receipt. If the marks on these match exactly she can be confident that her vote is included in the tally.

4 Technical Foundation

4.1 Coping with Single Transferable Vote

In order to support Single Transferable Vote (STV) [Wik07, Soc07] and other schemes where the voter expresses a ranking or awards votes to more than one candidate, we employ the multiple-onion approach introduced by [Hea07]. We provide an overview of the scheme here.

A numerical representation of a candidate is encrypted under a probabilistic threshold public key cryptography scheme. There are many different such encryptions for each candidate and as these are encrypted under a probabilistic scheme they do not look alike. We call these encryptions onions. A set of onions are associated with each ballot form and the voter's choices, as expressed on the ballot form, are translated into an ordering of these onions. If the voter wishes to cast a vote for the candidates in the order C, E, A, D, B then this is encoded by ordering the constituent onions thus:

$$O_C;O_E;O_A;O_D;O_B;O_{\text{stop}}$$

Note that these are encryptions and which candidate they represent is therefore hidden. The stop onion O_{stop} is used to ensure that the length of the vote is not dependent on the number of choices expressed by the voter. A vote only for candidate C, for example, is thus constituted by an onion O_C , the stop onion, and thereafter all other onions in a random order:

$$O_C;O_{\text{stop}};O_A;O_E;O_D;O_B$$

After the close of the election, the first constituent onion of each cast vote is decrypted and the vote given to the indicated candidate. This initiates the applicable STV protocol, which removes candidates and redistributes the votes according to the next choice in order in a number of rounds until the required number of candidates has been elected. Each time the vote is redistributed the next choice is decrypted. In our example, the first candidate is decrypted thus:

$$C;O_E;O_A;O_D;O_B;O_{\text{stop}}$$

If candidate C is subsequently eliminated and his or her votes redistributed, the onion representing candidate C is appended, the plaintext representation of C removed and the next onion decrypted, thus:

$$E;O_A;O_D;O_B;O_{\text{stop}};O_C$$

This is now a vote for E. When a decryption reveals the stop onion, the vote is removed from further redistributions. Each redistribution round contains a re-encryption shuffle so as to hide the ordering of the candidates in the vote; please see [Hea07] for details. This configuration thus limits the impact of an attack popularly called the Italian attack [Hea07] where the ordering of the candidates carries some message to a coercer.

4.2 Pre-Creation of Onions

A source of potential threats to the secrecy of the election pointed out in early papers describing end-to-end verifiable systems [Rya05, BR03, RP05, KSW05, RP06a, RS06a, RP06b, Rya06, Rya07a] was that the voting machine must select random values and errors or predictability in the pseudo-random number generator may render the cryptography useless. Furthermore, the voting machine might use “random” values from a list shared with a culprit or values such that a hash thereof would signal to a culprit the contents of the vote and/or the identity of the voter. To remove this problem, we do not require the machine to select the randomness used in creating the candidate list but employ the distributed pre-creation technique detailed in [RS06a].

4.3 Touch Screen Interface

To accommodate for elections with many races and/or races with many candidates, the proposed configuration of Prêt à Voter has two major differences to previous versions: (a) the receipt is created by a voting machine and (b) the receipt is printed in the *minimal* form presented in the next section.

4.3.1 Creating a Vote with the Machine

This is an example of a possible interaction with the voting machine. The steps involved can be different in appearance, order and number and are adapted to the election. Approaching an idle voting machine, the voter is greeted with a message asking her to touch the screen to initiate the voting process.

| |
|---|
| Springfield Local Election Tap screen to start |
|---|

A list of races is shown with indicators to whether or not a vote has been created in each race. The voter selects a race by tapping the screen³³.

| Select race | |
|-------------------------|-----------|
| Mayor | Not voted |
| Sanitation Commissioner | Not voted |

A list of the candidates in the selected race is shown and the voter is able to tap a single candidate or a number of candidates in the preferred order. A “Clear” button is available on the screen, which clears all choices made and allows the voter to start over. A “Proceed” button allows the voter to return to the list of races.

³³ Or using some other input method, depending on the abilities of the voter.

| Vote for Sanitation Commissioner | |
|----------------------------------|--|
| Shmoikel Krusotsky | |
| Apu Nahasapeemapetilon | |
| Ray Patterson | |
| Homer Simpson | |

Selecting her favourite candidate, the voter completes the vote for the race and clicks the “Proceed” button to return to the race selection screen.

| Select Race | |
|-------------------------|-----------|
| Mayor | Not Voted |
| Sanitation Commissioner | Voted |

The voter is able to return to any race and re-create her vote. A “Proceed” button on the race selection screen allows her to go to a summary screen. Here the voter can select either of two buttons: “Go back” or “Print vote”.

| Summary of your vote | |
|-------------------------|---------------|
| Mayor | Not voted |
| Sanitation Commissioner | Homer Simpson |

When the voter is finished and presses the “Print vote” button, the machine displays a final message whilst printing the vote.

| |
|--|
| Thank you Please take your printed vote |
|--|

4.4 The Minimalistic Encrypted Receipt

The purpose of the minimalistic encrypted receipt is to enable the printing of many races on the same receipt and to aid the voter in checking the receipt on the web bulletin board. To achieve this we wish to print as few candidates as possible on the vote. We first introduce the traditional Prêt à Voter ballot form and its associated encrypted receipt before showing the alterations we propose to these.

4.4.1 The Prêt à Voter Ballot Form and Encrypted Receipt

The ballot form in Prêt à Voter consists of two columns: in the left the candidates are printed in a random order (based on randomness unique for the form) and in the right the voter makes her marks in a grid corresponding to the candidates in the left column. For example:

| Ballot form | |
|-------------------------|-----------|
| Sanitation Commissioner | |
| Homer Simpson | |
| STOP | |
| Apu Nahasapeemaptelon | |
| Ray Patterson | |
| Smoikel Krustofsky | |
| | lk3j92784 |

If a voter makes her marks in the right hand side grid and then detaches and destroys the left hand column, the remaining encrypted receipt does not reveal her vote. However, a value called the onion, printed at the bottom of the grid, can be decrypted to reveal the vote. In this example an encrypted receipt may be:

| |
|-----------|
| 2 |
| 3 |
| |
| 1 |
| |
| lk3j92784 |

It has been envisaged that the Prêt à Voter is a single page, which contains all races in the election and all the candidates in each of those races. The voter makes her mark on the paper and detaches and destroys half, producing an encrypted receipt which is subsequently scanned and then handled electronically. It is quite clear that in an election with many races and many candidates, it is not possible to print all on one piece of paper that can also be fed through a scanner after the marks have been made by the voter.

4.4.2 The Minimalistic Encrypted Receipt

The traditional Prêt à Voter ballot form is printed onto paper before the election (or on demand before they are used [RS06a, LR08]) and as the voter uses a pen to fill out her choices, naturally all candidates must be available on the ballot form. In the scheme presented here a computer is used to create the vote after which the ballot form is printed. Therefore, it is possible to print only the candidate(s) that the voter has indicated a vote for. In our example, when the voter makes her marks using the touch screen she may indicate her choices thus (note that the candidates are listed in the alphabetical order on the screen):

| Vote for Sanitation Commisioner | |
|---------------------------------|---|
| Shmoikel Krustofsky | |
| Apu | |
| Nahasapeemapetilon | |
| Ray Patterson | 1 |
| Homer Simpson | 2 |

When the voter presses the “Print receipt” button the voting machine retrieves the necessary onions and decrypts these (see above) to find the ordering of the candidates. Let us assume in our example that the machine retrieves the onions with serial number 27344, decrypts these and finds that the candidate list has the following order:

| |
|---------------------|
| 27344 |
| Homer Simpson |
| STOP |
| Apu |
| Nahasapeemapetilon |
| Ray Patterson |
| Shmoikel Krustofsky |

The machine now prints the following filled-out Prêt à Voter ballot form, note that only the candidates which the voter has indicated are printed and that these are printed in the order dictated by the onions:

| Ballot form | |
|-------------------------|-------|
| Sanitation Commissioner | |
| Homer Simpson | 2 |
| STOP | 3 |
| Ray Patterson | 1 |
| | 1,2,4 |
| | 27344 |

In this example we are only able to avoid printing two candidates, but in a race with many more candidates the same number of choices made by the voter would drastically reduce the number of candidates that must be printed. The index numbers 1; 2; 4 of the candidates printed are displayed at the bottom right together with the serial number 27344. These values can be printed in the form of a barcode (see below) which allows them to be read in quickly. Note that these numbers together with the choices indicated above by the voter is all that is needed to represent the vote. The voter now checks that the printed vote is truly a representation of her intended vote. If it is not she can discard the vote (by shredding it for example) and produce another. If she is happy with the vote and wishes to cast it, she detaches the two columns from each other and destroys the left hand one. What remains is an encrypted receipt:

| |
|----------------|
| 2 |
| 3 |
| 1 |
| 1,2,4 27344 |

The voter approaches a desk manned by poll station staff, identifies herself and allows the barcode on the encrypted receipt to be scanned. When poll station staff are satisfied that the barcode has been scanned and electronically transmitted to the web bulletin board they stamp the encrypted receipt with an official stamp so as to indicate that it is the receipt of a vote that has been cast in the election. A mark is placed in the register to indicate that this voter has cast her vote³⁴. All votes submitted in this way are collected on the web bulletin board.

4.4.3 The Barcode

All previous versions of Prêt à Voter has required an encrypted receipt to be scanned in and interpreted to form a digital representation that could subsequently be decrypted. This OCR process has been shown to be a significant weakness to the scheme: it results in many errors³⁵.

In this scheme we reduce the amount of work in the scanning process to the recognition of a barcode. These are printed in such a way as to be simple to read and recognise and they can contain check numbers etc to aid the correct interpretation of them. In order to record a vote the system must read the following information from the encrypted receipt:

³⁴ In some constituencies, such as the United Kingdom, the law requires that the ballot form serial number is noted against the name of the voter: that is quite possible to do in this scheme.

³⁵ Note that these errors did not mean that a vote was cast for a different candidate than indicated by the voter—but that the vote had to fill out another ballot form as the first could not be correctly understood by the system.

1. The serial number (27344)
2. Which candidates are shown on the ballot form (1; 2; 4)
3. The marks made by the voter (2; 3; 1)

To enter this information into the barcode, we simply concatenate them:

27344|1; 2; 4|2; 3; 1

When this information is scanned by poll station staff it is submitted to the web bulletin board. Here the appropriate constituent onions are retrieved:

| |
|--|
| 27344 |
| <input type="radio"/> _{RSimpson} <input type="radio"/> _{RSTOP} <input type="radio"/> _{RNahasapeemapetilon} <input type="radio"/> _{RPatterson} <input type="radio"/> _{RKrustofsky} |

The appropriate onions are selected (numbers 1, 2 and 4 in our example) and re-ordered in the correct order as indicated by the choices (2, 3 and 1) — thus the onions are placed in the following order:

| |
|--|
| 27344 |
| <input type="radio"/> _{RPatterson} <input type="radio"/> _{RSimpson} <input type="radio"/> _{RSTOP} |

Note that of course the contents of these onions are unknown! Therefore, the system now holds an encrypted vote submitted by this voter.

4.5 Auditing a Vote

We here argue that it is safe to allow a voter to use a voting machine to create the vote, because she may create any number of votes and audit some of these. If the voting machine attempts to cheat, it cannot be sure that the vote will not be audited and its cheating thus found out. A malfunctioning machine will thus be found with a high probability and taken out of commission.

The first audit that a voter makes out of a vote printed by the voting machine is simply to read it. If the machine has committed an error (or something worse) then the marks printed would not match the intention of the voter. If this is the case, she can simply destroy the vote and create another one — until she receives one that correctly indicates the vote she wishes to cast. Note that the voter may have performed some “human” error while interacting with the machine and not spotted this until the vote has been printed: this gives her another chance to spot such a mistake and to rectify it.

The second audit of the ballot form that can be performed on any vote is the checking of the barcode. This is simply done by the voter allowing the barcode to be scanned by a machine available in the polling station, which shows the contents of the barcode in a human readable form. Such machines can also be supplied by independent organisations — or run as a small piece of software on the voter’s camera-enabled mobile phone. The voter then simply checks that the information shown by the reader corresponds to the information printed in the right column of her vote.

Finally, if the voter decides to audit a created vote then the constituent onions shall be retrieved from the web bulletin board (where they are marked as audited, ensuring that no vote can subsequently be cast with these onions) and decrypted by the tellers. The full candidate list is then displayed to the voter who compares it to the printed vote.

The purpose of this audit is first to find any machine that may malfunction or that has been compromised. Secondly, the audit functions to convince voters that the system is working correctly and that the vote will be decrypted correctly.

4.6 Checking the Receipt

The voter is allowed to take home the scanned and stamped encrypted receipt. She can then, at any time, visit the web bulletin board on the web and search for the serial number printed on the receipt. When she calls up her receipt she should see an exact replica of the receipt she holds in her hands. If this is the case then the voter can be certain that her vote has been included in the final tally. If the receipt is not found on the web bulletin board or if the version she finds there does not match the one she has in her hand, she can accuse those in charge of running the election of malfunction or fraud and she has proof in her receipt that she has cast a vote which is now missing or has been changed.

4.7 Decryption and Tallying

At this stage the web bulletin board contains a list of all encrypted votes that have been cast, in the form of a number of ordered onions. We are unable to describe the decryption here because of limitations to the length of this paper but a detailed specification is available in [Hea07].

4.8 Note on Securing the Machine using Procedures

It is important to note that the accuracy of the election, that is to say, the trustworthiness of the outcome of the election, is safeguarded not by procedures but by the cryptographic properties of the system. The result of the election is thus as trustworthy as in previous configurations of Prêt à Voter [CRS05, RS06a], because they all rely on the same verifiability.

5 Discussion

The main advantages of the proposed scheme is that the voting machine is able to guide the voter through a potentially very complex voting procedure involving any number of races and any number of candidates in those races. The voter turns the plain text vote into an encrypted receipt and the scanning of this receipt is very fast because only a barcode has to be scanned. The main disadvantage to this configuration of Prêt à Voter is that the voting machine must learn the voter's intention in order to produce the printed vote. The secrecy of the election is thus safeguarded simply by procedures that ensure that the machine does not leak any information. As discussed in the introductory sections of this paper, there is a necessity to alter the procedure/technology mix so that it is possible to make the system more accessible and remove a large proportion of the errors associated with the filling out of the ballot form.

5.1 Acknowledgements

Thanks to the anonymous EVOTE08 reviewers for their feedback. Thanks also to Peter Ryan, Steve Schneider, James Heather, Roger Peel, Zhe Xia, Kieran Leech, Roberto Araújo and Jacques Traore, who listened to a presentation of initial ideas.

References

- [ABBD04] R. Aditya, Lee B, C. Boyd, and E. Dawson. An efficient mixnet-based voting scheme providing receipt-freeness. Proceedings of TrustBus'04, pages 152–161, 2004. LNCS 3184.
- [ACvdG07] Roberto Araujo, Ricardo Filipe Custodio, and Jeroen van de Graaf. A Verifiable Voting Protocol based on Farnel. Proceedings of Workshop On Trustworthy Elections (WOTE 2007), 2007.
- [AR06] B. Adida and R. Rivest. Scratch & Vote: self-contained paper-based cryptographic voting. Proceedings of the fifth ACM workshop on Privacy in electronic society, pages 29–40, 2006.
- [BFP+01] O. Baudron, P.-A. Fouque, D. Pointcheval, J. Stern, and G. Poupard. Practical multicandidate election system. Proceedings of the twentieth ACM Symposium on Principles of Distributed Computing (PODC'01), pages 274–283, 2001.
- [BR03] J. Bryans and P. Y. A. Ryan. A Dependability Analysis of the Chaum Digital Voting Scheme. Technical Report, University of Newcastle, CS-TR:809, 2003.

- [BT94] J. Benaloh and D. Tuinstra. Receipt-free secret-ballot elections (extended abstract). Proceedings of the twenty-sixth Symposium on Theory of Computing (STOC'94), pages 544–553, 1994.
- [CGS97] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multiauthority election scheme. Advances of Eurocrypt'97, pages 103–118, 1997. LNCS 1233.
- [Cha04] D. Chaum. Secret ballot receipts: true voter-verifiable elections. IEEE: Security and Privacy Magazine, 2(1):38–47, 2004.
- [CRS05] D. Chaum, P. Y. A. Ryan, and S. Schneider. A practical voter-verifiable election scheme. Proceedings of the tenth European Symposium on Research in Computer Science (ESORICS'05), pages 118–139, 2005. LNCS 3679.
- [FCS06] K. Fisher, R. Carback, and T. Sherman. Punchscan: Introduction and System Definition of a High-Integrity Election System. In PRE-PROCEEDINGS, pages 19 – 29. IAVoSS Workshop On Trustworthy Elections, 2006.
- [FOO92] A. Fujioka, T. Okamoto, and K. Ohta. A Practical Secret Voting Scheme for Large Scale Elections. Advances of Auscrypt'92, pages 244–251, 1992. LNCS 718.
- [Hea07] J. Heather. Implementing STV securely in Prêt à Voter. 20th IEEE Computer Security Foundations Symposium (CSF'07), pages 157–169, 2007.
- [JCJ05] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, pages 61–70, 2005.
- [KSW05] C. Karlof, N. Sastry, and D. Wagner. Cryptographic voting protocols: a systems perspective. Proceeding of USENIX Security Symposium, pages 186–200, 2005. LNCS 3444.
- [LBD+03] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo. Providing receipt-freeness in mixnet-based voting protocols. Proceedings of ICISC'03, pages 245–258, 2003. LNCS 2971.
- [LR08] D. Lundin and P. Y. A. Ryan. Human readable paper verification of Prêt à Voter. Technical Report at the University of Surrey, CS-08-03, 2008.
- [LTR+06a] D. Lundin, H. Treharne, P. Y. A. Ryan, S. Schneider, and J. Heather. Distributed creation of the ballot form in Prêt à Voter using an element of visual encryption. Proceedings of Workshop On Trustworthy Elections (WOTE 2006), pages 119–125, 2006.
- [LTR+06b] D. Lundin, H. Treharne, P. Y. A. Ryan, S. Schneider, J. Heather, and Z. Xia. Tear and destroy: chain voting and destruction problems shared by Prêt à Voter and Punch-Scan and a solution using visual encryption. Proceedings of Workshop on Frontiers in Electronic Elections (FEE 2006), 2006.
- [NA03] C. A. Neff and J. Adler. Verifiable e-voting: indisputable electronic elections at polling places. VoteHere Inc, 2003.
- [OMA+99] M. Ohkubo, F. Miura, M. Abe, A. Fujioka, and T. Okamoto. An improvement on a practical secret voting scheme. Information Security'99, pages 225–234, 1999. LNCS 1729.
- [Pun] Punchscan. <http://www.punchscan.org>.
- [Riv06] R. Rivest. The ThreeBallot voting system, 2006. <http://crypto.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf>.
- [RP05] P. Y. A. Ryan and T. Peacock. Prêt à Voter: a system perspective. Technical Report of University of Newcastle, CS-TR:929, 2005.
- [RP06a] P. Y. A. Ryan and T. Peacock. Putting the human back in voting protocols. Technical Report of University of Newcastle, CS-TR:972, 2006.
- [RP06b] P. Y. A. Ryan and T. Peacock. Threat analysis of cryptographic election schemes. Technical Report of University of Newcastle, CS-TR:971, 2006.

- [RS06a] P. Y. A. Ryan and S. Schneider. Prêt à Voter with re-encryption mixes. Proceedings of ESORICS, 2006. LNCS.
- [RS06b] P. Y. A. Ryan and S. Schneider. Prêt à Voter with re-encryption mixes. Technical Report of University of Newcastle, CS-TR:956, 2006.
- [Rya05] P. Y. A. Ryan. A variant of the Chaum voter-verifiable scheme. Proceedings of the 2005 Workshop on Issues in the Theory of Security, pages 81–88, 2005.
- [Rya06] P. Y. A. Ryan. Verified encrypted paper audit trails. Technical Report of University of Newcastle, CS-TR:966, June 2006.
- [Rya07a] P. Y. A. Ryan. The computer ate my vote. Technical Report of University of Newcastle, CS-TR:988, 2007.
- [Rya07b] P. Y. A. Ryan. Prêt à Voter with Paillier Encryption. Technical Report of University of Newcastle, CS-TR:1014, 2007.
- [Soc07] Electoral Reform Society. 2007. <http://www.electoral-reform.org.uk/>.
- [VV06] M. Volkamer and R. Vogt. New Generation of Voting Machines in Germany — The Hamburg Way to Verify Correctness. In PRE-PROCEEDINGS, Hamburg, Germany, 2006. Frontiers of Electronic Elections (FEE 2006).
- [Wik07] Wikipedia. Single transferable vote, 2007. http://en.wikipedia.org/wiki/Single_transferable_vote.
- [XSH+07] Z. Xia, S. Schneider, J. Heather, P. Y. A. Ryan, D. Lundin, R. Peel, , and P. Howard. Prêt à Voter: all in one. Proceedings of Workshop On Trustworthy Elections (WOTE 2007), 2007.

Improving the Farnel Voting Scheme

Roberto Araújo¹, Peter Y. A. Ryan²

¹Department of Computer Science, TU-Darmstadt
Hochschulstrasse 10, D-64289 Darmstadt, Germany
rsa@cdc.informatik.tu-darmstadt.de

²Centre for Software Reliability, Newcastle University
Newcastle upon Tyne NE1 7RU UK
peter.ryan@ncl.ac.uk

Abstract: Farnel is a voting scheme which first introduced the concept of a ballot box to exchange votes. Recently, Araújo et al. improved this concept to accomplish a voter-verifiable scheme in which voters receive copies of receipts of one or more randomly selected previous cast votes. The scheme, however, relies on a strong requisite to achieve security: trustworthy talliers. With the goal of removing this requisite, in this paper we propose a Prêt-à-Voter style receipt for this scheme. In addition, we present a novel way to initialize the Farnel box and a new scheme based on combining Farnel with Prêt-à-Voter style encoding of receipts.

1 Introduction

Voter-verifiability is a novel security feature provided by several recent voting systems, such as Prêt-à-Voter [Rya04, CRS05] and Punch Scan [PH06]. It allows voters to verify that their votes are accurately counted by means of *protected receipts* and so gives more confidence to the election process. The voters, however, cannot use their receipts to compromise their privacy, even if they are prepared to cooperate with the coercer.

High-assurance voting systems typically rely on cryptography to achieve security and to implement voter-verifiability. Such technology makes the security of modern systems comparable or even better than traditional paper-based elections. However, systems that employ cryptography are not easily grasped by the average voter and so voters need to rely on the assurances of experts.

With the goal of making such schemes more understandable, Randell-Ryan [RR06], Rivest [Riv06, RS07], and Araújo et al. [ACvdG07], introduced voter-verifiable schemes that do not rely on cryptography. These schemes are simple and can be more easily understood by the voters. However, they do not achieve the same levels of assurance as the cryptographic systems. In the scheme proposed in [Riv06], the ballot secrecy is not perfect and it may reveal statistical indications of voting results before the voting end. The proposals of Araújo et al. and of Randell-Ryan require trustworthy talliers or additional mechanisms to counter threats during the vote tabulation.

In this paper we introduce improvements for the scheme of Araújo et al. Especially, we propose a Prêt-à-Voter style receipt in order to detect manipulation of votes by adversaries, including malicious talliers. In addition, we present a novel way to initialize the Farnel box and a new scheme based on combining Farnel [ACvdG07, Cus01] with Prêt-à-Voter style encoding of receipts. Our proposals make use of cryptography to overcome the drawbacks of the previous non-cryptographic solutions.

This paper is organized as follows: in the next section we describe the elements of the Farnel mechanism. In Section 3 we introduce a new ballot form for the scheme of Araújo et al. Then, in Section 4, we show a new scheme based on Farnel that employs only one ballot box. Finally, we present our conclusions in Section 5.

2 Preliminaries

We present here the basic elements of the Farnel approach. The Farnel type voting schemes [ACvdG07, Cus01] are based on the observation that to achieve voter-verifiable it is not necessary for the voter to carry away a receipt corresponding to their own vote. The Farnel approach then is to provide voters, when they cast their votes, with copies of receipts of one or more randomly selected previous cast votes.

This idea has a number of attractive features: ballot secrecy is achieved up front and does not have to be provided by anonymising mixes, etc. during tabulation. In fact, plaintext receipts can be used in contrast to the encrypted receipts of many other voter-verifiable schemes, e.g. [Rya04]. Furthermore, any fears that voters might have that their vote is not truly concealed in an encrypted receipt is mitigated. The Farnel mechanism also mitigates randomization style attacks.

2.1 The Farnel Ballot Box

The Farnel is a concept of ballot box that was first introduced by Custódio [Cus01]. This ballot box performs differently from a conventional one. It is able to shuffle its contents and is initialized with elements (e.g. votes). After receiving elements from voters, it returns to them elements that correspond to randomly selected, previously cast votes. Recently, Araújo et al. [ACvdG07] improved the Farnel concept in order to accomplish a voter-verifiable scheme. In the improved concept, besides shuffling its elements, the Farnel box should be able to copy some elements and to remove scratched surfaces.

We describe the enhanced Farnel box as follows: it is a box that has mechanisms to remove scratch surfaces, and to shuffle and to copy elements in a memoryless way. The box has an initial set of elements cast before the voting. At the time of voting, it is able to receive an element, to shuffle its contents, to copy one or more randomly selected elements from its set, to output the copies, and to add the element received to its set. The box elements may be votes or receipts.

Although the requisites of the Farnel box seem difficult to implement, a tombola (i.e. a raffle drum) normally used in lottery games to shuffle tickets could form the basis of an implementation of the box.

The Farnel box was never formally specified. This way, we introduce now a specification of the box in the process algebra CSP.

Let $Init$ denote the initial set of dummy ballots (say votes or receipts) with which the box is initialized. Let l denote the number of receipts to be output to each voter when they cast their votes and $Ballots$ the set of all possible ballots. Then the Farnel box will start in state $Farnel(Init)$ and its subsequent behavior is defined recursively as:

$$Farnel_l(X) := cast? b:Ballots \rightarrow \square receipt! r: \wp_l(X) \rightarrow Farnel_l(X \cup \{b\})$$

We have used the notation $\tilde{A}l(X)$ to denote set of subsets of X of cardinality l .

Thus, the Farnel ballot box is parametrised by the integer l and its initialization $Init$. At any point, the box can accept a ballot b , after which it outputs a set of ballots in size l chosen at random from its current set X . After this, the new ballot is added to X and the box is ready to receive the next ballot.

2.2 The Initialization Process

The initialization process takes place before the election and is performed by the authorities in a public session. The main objective is to cast a predefined number of votes (or receipts) into the Farnel ballot box and to publish the number of elements cast per option on the bulletin board.

The elements cast before the election are necessary mainly for ensuring the anonymity of the early voters. As the Farnel receives an input from each voter and outputs copies of random elements, it must have an initial set of elements to choose from. Otherwise, after receiving inputs, the Farnel would not have enough elements to select at random and to make the copies.

For the schemes that we describe here, it is necessary to ensure that ballots cast during the initialization are well formed in some way. This will typically involve some form of random auditing. Thus, for example, we might require that 2x blank ballots be created beforehand. The authorities perform the following steps to initialize the ballot box:

(1) Select x blank ballots at random and audit them as necessary. Ballots audited are discarded; (2) Mark the other x unaudited blank ballots according to the number of votes per option specified in advance; (3) Cast the x marked ballots (or receipts) into the Farnel box and publish the number of elements cast on the bulletin board.

Notice that in schemes which employ a conventional and a Farnel box (e.g. [ACvdG07]), the conventional box is initialized with votes and the Farnel is initialized with the corresponding receipts. Also, for schemes using plaintext ballots, the auditing for well-formedness is not necessary and would be omitted.

In order to prevent manipulation, the initialization process should be scrutinized by helper organizations. They should check that the ballot box is empty before it is initialized, as well as verify that all procedures above are performed correctly. Further, the ballot box should be sealed and continually supervised by third parties after the initialization. The seal is removed when the voting starts.

2.2.1 Initialization of the Farnel box with Void Ballots

Where we are using encrypted receipts we have an alternative way to initialize the Farnel box: we include a void option on the ballots and initialize the box with ballots representing votes for the void option. This has the advantage that we do not have to keep a log of the actual votes cast for each candidate during initialization. We do need a robust mechanism to ensure that all initializing votes are cast for void, but it seems likely that this is easier to enforce than maintaining a record of an initial tally. We can use this approach for the Prêt-à-Voter and ThreeBallot style ballots, but not where plaintext receipts are used.

2.3 The Parameters of the Farnel Box

The Farnel box is initialized with a number of elements (votes or receipts) before the voting starts and outputs copies of its elements during the voting, as described. The initial elements ensure the voter's anonymity while the copies are handed to the voter as her receipt. The number of initial elements, as well as the number of receipts given to each voter, compose the parameters of the box.

In order to preserve the voters' anonymity, the initial elements and the voters' elements cannot be distinguished through the copies output by the Farnel box. The number of initial elements is fundamental for guaranteeing this. As the Farnel box outputs elements for each voter, the elements of the early voters have more chance to be output. Hence, these elements may be distinguished from other elements. Depending on the number of initial elements, however, the chance of distinction may be negligible as the initial elements may also be output.

To achieve verifiability while maintaining anonymity, the number of initial elements and the number of receipts should be defined such that:

(1) The voter's anonymity is preserved even if the Farnel box is able to output a copy of her element; (2) An individual receipt or a set of them do not provide enough information to distinguish elements; (3) The number of copies of elements in all receipts is sufficient to detect accuracy problems with an acceptable probability (i.e. the probability that the corruption of any given vote is detected is at least 50%).

We require that the voter should not be able to obtain any information other than her choice when casting her element.

Taking into account these requisites, we have a number of possible strategies for initializing the box: ballots marked at random (with the totals carefully recorded), a predetermined number of votes per option, votes for a void option, or a combination of these methods. If we adopt an initialization with votes for void, we must include a minimal number of votes for the other options. Otherwise, the first voter may vote and receive a copy of her own vote as receipt. An initialization purely with void votes only works if we have mixes during the tabulation. This might seem like overkill since anonymity is already provided by the Farnel mechanism. However, it might still be useful in some contexts and does provide an extra layer of protection.

Note that in the specification of the Farnel box presented before, the box is not able to output the element it receives.

3 A New Ballot Design for the Farnel Variant Scheme

The Farnel scheme was proposed by Custódio [Cus01] (see [ACvdG07] for a description). The scheme employs an original Farnel ballot box and relies on physical signatures. However, it is not voter-verifiable. Recently, Araújo et al. [ACvdG07] introduced a variant of the Farnel scheme. In contrast to the original version, the scheme is voter-verifiable and does not employ signatures. It relies, though, on trustworthy talliers to tabulate the votes.

With the goal of removing this requisite, we introduce in this section a new ballot design for Araújo et al.'s proposal.

3.1 An Overview of Araújo et al.'s Farnel Variant Scheme

The scheme employs a ballot form composed of two halves that are linked by a unique ID and that are separated by perforations. More specifically, the ballot has an options half composed of the voting options as well as an ID and an ID half that contains the same ID of the options half (see Figure 1). These IDs are covered by scratch surfaces.

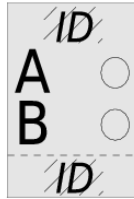


Figure 1: The ballot form of the Farnel variant scheme.

Besides the unusual ballot form, the scheme depends on two ballot boxes. One of them is conventional and the other is a Farnel box. These boxes are initialized before the voting. That is, the conventional box receives dummy votes (i.e. marked option halves) and the Farnel box receives the ID halves (i.e. receipts) corresponding to the votes. The scratch surfaces in the halves are detached during the initialization and at the end the number of votes cast is published on a bulletin board.

At time of voting, the voter receives a blank ballot and detaches its scratch surfaces. She then compares the IDs on the halves and if they match, she marks her option. After that, she separates the two halves of her ballot, casts the option half into the conventional box, and the other half into the Farnel box. Upon receiving the half, the Farnel box shuffles its ID halves and copies a set of them as receipt to the voter. As alternative to avoid comparison of IDs, the scheme may have an auditing process to check ballots before the voter receives her blank ballot and require the voter to cast her vote without removing the scratch surfaces. The Farnel box then removes the scratch of the half that it receives.

After the voting, the authorities publish the content of both ballot boxes on the bulletin board and count all votes from the conventional box. The dummy votes are then subtracted from the total of votes to obtain the results.

In order to verify the votes published on the bulletin board, voters and observers compare the ID halves with the IDs in the options halves. The voters can also match the IDs on their receipts with the options halves on the board.

3.1.1 Drawback

Due the receipt style employed, the proposal requires trustworthy talliers. These authorities should supervise the votes strictly after opening the ballot boxes. On the contrary, an adversary (e.g. a malicious tallier) is able to compromise the voting results as follows.

According to the scheme, the two halves of all ballots are published after the voting. This way, they can be compared to verify the exactness of the voting results. Before publishing the options halves, though, an adversary could replace a vote (i.e. a marked option half) by a new one marked to a different option, but that contains the same ID of the replaced vote. This substitution would not be detected by voters and observers, as they only compare IDs.

3.2 Combining the Farnel Variant Scheme and Prêt-à-Voter

The main problem of the receipt used in Farnel variant is that it does not depend on the option chosen. This way, an adversary is able to replace votes without being detected. In order to detect such a problem, a receipt should contain some information related to the option selected. However, this information should not reveal the option itself before the voting closes and should still be able to detect replacement of votes. Otherwise, the receipt can leak statistical information about the voting results as the Threeballot scheme [Riv06, RS07] (see [ACvdG07] for details). We introduce now a new ballot design for the Farnel variant that satisfies these requirements.

3.2.1 The Ballot Form

Our ballot form is based on the Prêt-à-Voter [Rya04, CRS05] ballot and is inspired by the ideas of Randell-Ryan [RR06] and of Scratch-and-vote [AR06]. Differently from the original Prêt-à-Voter ballot design, however, the ballot here does not include a mixnet onion.

The ballot is composed of two pages that are overlaid initially. The top page has a list of voting options in a random order with a selection bubble beside each option. The top page also includes a commitment to the list of options and its respective decommitment value. The bottom page contains the same bubbles and the same commitment as the top page. The commitment printed on both pages, as well as the value to open it on the top page, are covered by scratch surfaces. A carbon mechanism transfers the selections from the top page to the bottom page (see Figure 2 for an example of this ballot form).

Formally, the new ballot form is described as follows: Let C be a set of options available, π_C a permutation of C , H a secure hash function used here as commitment, and r a random number from a large (key) space. π_C , $H(\pi_C, r)$, r , and bubbles to select an option compose the top page. The bottom page contains *only* $H(\pi_C, r)$ and the bubbles in same position of the top page.



Figure 2: The proposed ballot form for the Farnel variant scheme.

The new ballot form satisfies the requisites above. The votes now are tabulated from the top pages and the receipts are made from the bottom pages (without the scratch surfaces). Because each bottom page contains the same selections of its corresponding top page and also includes the commitment to the options on the top page, an adversary cannot replace a top page by another with a different permutation or with a selection for a different option, without being detected. Moreover, since the bottom page does not include the option selected, an adversary cannot use receipts to obtain indication of the results before the voting closes.

3.2.2 New steps for the Initialization, the Voting, and the Tallying phases

Due the modification of the ballot form, the initialization, the voting and the tallying steps in the original scheme need to be adapted.

Before the Voting

The conventional box and the Farnel box are now initialized with marked top pages and with bottom pages, respectively (see also Section 2.2). Before initializing the boxes, however, the officials publicly audit ballots as follows: they separate the pages of each ballot and scratch off their surfaces; they then hash the options and the random number on top page, and compare the result with the hashes on both pages. Ballots audited are discarded.

Voting

In the voting phase, upon proving her eligibility to the voting authorities, the voter receives a sealed envelope with a blank ballot. If required by the voter, her ballot can be audited (as above) and she receives a new blank ballot. The voter performs the following steps to vote:

1. (Selecting the option) In the voting booth, the voter marks her choice on the top page and it is transferred to the bottom page.
2. (Verifying the ballot) She then inserts her ballot into a special envelope, which has transparent borders and a window to show just the scratch surface. After this, she hands the envelope to the authorities. They verify that the surface on the top page is intact and that the voter did not separate the two pages.
3. (Casting the top page) The voter separates the pages of the ballot and casts the top page into the conventional ballot box.
4. (Obtaining the receipt) She casts the bottom page into the Farnel box. The box shuffles its contents and outputs copies of randomly selected bottom pages as receipts.

Observe that the special envelope prevents the authorities to learn the voter's choice while verifying the surfaces, and the pages were not separated before.

Tallying and Verifying the Votes

As the Farnel variant scheme, the contents of the two ballot boxes are published on a bulletin board in the tallying phase. Now, the scratch surface on the top pages should be removed before publishing the ballots and the commitments should be decommitted to verify the ballots. That is, the random number and the options on the top page are hashed together and the resulting hash is compared with the hash on both pages.

From the pages published on the bulletin board, everyone can perform the same procedures as the talliers to verify the votes. The voters, especially, match their receipts with the corresponding bottom pages on the board.

4 Single Box Farnel Scheme

The design presented above is awkward in several respects: it requires two ballots boxes and the vote casting procedure is rather complicated and vulnerable to certain threats. We present here an improved version of the Farnel variant that requires just one ballot box and uses a simpler vote casting procedure.

4.1 Requisites

The ballot form

As the design presented in Section 3.2.1, the ballot here is composed of two pages that are initially overlaid. The top page, though, contains *only* the options in a random order along with bubbles to select them. The bottom page contains the same bubbles as the top page and an index. Also, it includes one commitment to the options of the top page and the index. The index indicates the options' order and helps the authorities to identify the order in the tallying process. The commitment and the index are printed at the foot of the page, on the left and on the middle, respectively. In addition, the bottom page includes the corresponding decommitment that is printed close to the index. The commitment is covered by a scratch surface apart from the index and from the decommitment.

More formally, let C be a set of options available, I a set of positive integers, π_C a permutation of C , H a secure hash function used as commitment, i an index that is a unique number in I , and r a random number from a large (key) space. The top page is composed of π_C and bubbles to select the options. The bottom page contains $H(\pi_C, r, i)$, r , i , and the same bubbles of the top page (see also Figure 3).

The list of possible permutations (i.e. options' orders) for all ballots and the index corresponding to each permutation are published on the bulletin board before the voting.

The Ballot Box

The scheme employs just a Farnel ballot box that is initialized (see Section 2) with marked bottom pages before the voting starts; the corresponding top pages are destroyed.

4.2 The Scheme

Before the Voting

As required by the Farnel box, we define a number of copies l that each voter receives as receipts and initialize the box with a number of dummy votes (Section 2 details this process).

For the initialization as well as for the voting phase, we require an auditing process. The audit is necessary to detect malformed ballots and is performed as follows: the authorities select a set of ballots at random, separate the two pages of each ballot, and detach their scratch surfaces. In order to verify a ballot, the authorities hash the options on the top page along with the random number and the index printed on the bottom page. They then compare the resulting hash with the value $H(pC,r,i)$ also on the bottom page. Moreover, the authorities verify that the randomization on the top page corresponds to that one indicated by the index i . In the voting phase, helper organizations assist the voter to audit ballots in the same way.

Voting

The voting authorities hand a blank ballot to the voter in a sealed envelope after verifying her eligibility. The voter can either use the blank ballot to vote or ask the authorities to audit it. In the latter case, the authorities publicly detach the scratch surfaces on the ballot and check the commitment (as before) through a computer. This procedure can be performed again by helper organizations that would employ their own computers. Assuming that the ballot is verified as well-formed, it is discarded and the authorities hand a new blank ballot to the voter. In principle, we could allow the voter to opt to audit a number of ballots before accepting one to use to cast her vote. If any ballot fails the audit checks, then recovery mechanisms need to be invoked. Discussion of this is beyond the scope of this paper.

To cast her vote, the voter performs the following steps (see also Figure 3):

1. (Selecting the option) In the voting booth, the voter chooses her option and marks the corresponding bubble on the ballot (a).
2. (Verifying the ballot) She separates the two pages of her ballot (b) and adds the bottom page into an envelope to make visible only the scratch surfaces. After this, she destroys in public the top page by means of a paper shredder (c) and hands the envelope containing the bottom page to the officials. They verify that the surfaces are whole.

3. (Casting the vote) The voter removes the bottom page from the envelope and casts it publicly into the Farnel box (d).
4. (Obtaining the receipt) After receiving the bottom page, the Farnel box removes the scratch surface that covers only the commitment value on the left side, shuffles its set of bottom pages (e), and copies one of them. The copies are held by the voter as her receipt (f).

Note that the scheme may employ a mechanism to prevent voters from destroying top pages other than their own. For example, the ballots could be numbered in a similar way as in the case of preventing chain voting attacks (see Jones [Jon05] for details).

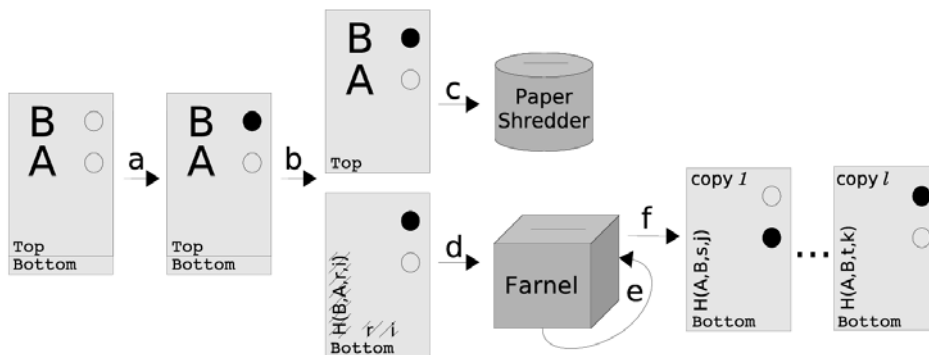


Figure 3: The main voting steps of the single box Farnel scheme.

Recovering and Tallying the Votes

In order to tally the votes, the talliers open the Farnel box, detach the scratch surfaces on all votes, and publish the votes on the bulletin board. Then, the talliers start the process to recover the votes. In this process, they compare the index on the vote with the index on the bulletin board to identify the permutation of the options; remember that the permutations as well as their indexes were previously published. From the permutation identified and the mark on the ballot, the talliers determine the option chosen by the voter. After recovering the votes, the authorities open all commitments using the random numbers and the indexes. In this step, they hash the random number and the index along with the permutation identified before, and compare the resulting hash with the hash on the vote. Now, the talliers count the votes in the same way as Farnel, that is, all votes are counted and the votes cast during the initialization phase are subtracted from this sum.

Verifying the Votes

Voters can, as usual, visit the bulletin board and confirm that their receipts appear accurately, and complain if they are not. Particularly, they verify the commitments and the marks on their receipts correspond to those on the votes published on the board. Helper organizations and observers verify that the talliers performed their work correctly.

4.2.1 Human Readable Paper Audit Trail

In the manner of Ryan [Rya07], the scheme could be adapted to provide a HRPAT by employing a conventional ballot box as alternative to the paper shredder. This way, instead of destroying the top page in a paper shredder, this page may be cast into the conventional ballot box. The box would store the top pages as an audit trail so that the votes can be counted without depending on the votes from the Farnel box.

5 Conclusions

We have presented a new ballot design for the scheme of Araújo et al. and a new voter-verifiable scheme based on Farnel. The solutions rely on the Prêt-à-Voter style ballots and cryptography to achieve security. Despite employing cryptography, the proposals require only a hash function and the voters perform simple steps to verify the votes corresponding to their receipts. That is, they just match numbers (i.e. hashes) and the marks on their receipts with the votes on the board. Helper organizations perform a more thorough verification of the hashes.

Moreover, we have introduced a novel way to initialize the Farnel box that employs void ballots. This initialization, however, only works with the ballot forms that give rise to protected receipts with a void option, e.g., Prêt-à-Vote style ballots. The new process would be easier to monitor and verify than having to maintain and record the total of the various votes cast in the initialization phase. Even so, ensuring only void votes are cast during the initialization phase is still challenging and will require carefully designed monitoring procedures.

Implementing the concept of the Farnel box in a way that requires minimal trust in the mechanism or procedures remains challenging. Rivest employed the original Farnel idea to overcome the reconstruction attack in the version of the Threeballot proposed in [Riv06]. In his scheme, a copy of a vote is made in advance and then it is exchanged by means of Farnel. This may be proved easier to implement with less trust assumptions. However, to prevent any possibility of the voter wandering off with her original receipt, the two steps (i.e. copy and exchange) need to be performed in close proximity.

An interesting feature of the Farnel mechanism is that it may help counter certain psychological style attacks on voter-verifiable schemes in which voters are convinced that the secrecy of their vote is not guaranteed. Using Farnel, the voters do not retain their own receipts, so any fear that the vote can be extracted should be mitigated. The down-side is that voters may be less motivated to check receipts if the receipt they hold is not their own. This may be offset by ensuring that voter helper organizations are on hand to perform the checks on behalf of the voters. If voters are given more than one receipt each this should also help as long as a reasonable proportion of voters are diligent enough to check all or many of their receipts.

Besides helping counter psychological attacks, the Farnel idea also mitigates randomization style attacks. These attacks were introduced by Schoenmakers [Sch00]. To perform a randomization attack, the adversary instructs the voter to generate a receipt that has a certain property. The adversary will not know what vote will be encoded, this is effectively random. The effect then is to force voters to vote for a random candidate, so nullifying their right to vote freely. The attack can be applied to Prêt-à-Voter and to Punch Scan schemes as the voter receipt in these schemes contain the position chosen by the voter. This way, an adversary may ask the voter to place her X in a specific position and to show him afterwards the receipt marked in this position. By means of the Farnel idea, however, the voter exchanges her receipt before leaving the voting place. Thus, the adversary cannot verify that the voter followed his instructions.

References

- [ACvdG07] Roberto Araújo, Ricardo Felipe Custódio, and Jeroen van de Graaf. A Verifiable Voting Protocol based on Farnel. IAVoSS Workshop On Trustworthy Elections (WOTE'07), June 2007.
- [AR06] Ben Adida and Ronald L. Rivest. Scratch & vote: self-contained paper-based cryptographic voting. In WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society, pages 29–40, New York, NY, USA, 2006. ACM.
- [CRS05] David Chaum, Peter Y. A. Ryan, and Steve A. Schneider. A Practical Voter-Verifiable Election Scheme. In Sabrina De Capitani di Vimercati, Paul F. Syverson, and Dieter Gollmann, editors, ESORICS, volume 3679 of Lecture Notes in Computer Science, pages 118–139. Springer, 2005.
- [Cus01] Ricardo Custódio. Farnel: um protocolo de votação papel com verificabilidade parcial. Invited Talk at Simpósio Segurança em Informática (SSI), November 2001.
- [Jon05] Douglas W. Jones. Chain Voting, August 2005. <http://vote.nist.gov/threats/papers/ChainVoting.pdf>.
- [PH06] Stefan Popoveniuc and Ben Hosp. An Introduction to Punchscan. IAVoSS Workshop On Trustworthy Elections (WOTE'06), June 2006.
- [Riv06] Ronald L. Rivest. The ThreeBallot Voting System. <http://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf>, October 2006.
- [RR06] Brian Randell and Peter Y.A. Ryan. Voting Technologies and Trust. IEEE Security and Privacy, 04(5):50–56, 2006.
- [RS07] Ronald Rivest and Warren Smith. Three Voting Protocols: ThreeBallot, VAV, and Twin. Electronic Voting Technology Workshop (EVT'07), August 2007.

- [Rya04] P.Y.A. Ryan. A Variant of the Chaum Voting Scheme. Technical Report CS-TR-864, University of Newcastle upon Tyne, 2004.
- [Rya07] P.Y.A. Ryan. Pret a Voter with a Human-Readable, Paper Audit Trail. Technical Report CS-TR-1038, University of Newcastle upon Tyne, 2007.
- [Sch00] Berry Schoenmakers. Personal communication, 2000.

Session 6: Certification of E-Voting

Development of a Formal IT Security Model for Remote Electronic Voting Systems

Rüdiger Grimm¹, Melanie Volkamer²

¹Forschungsbereich IT-Risk-Management
Universität Koblenz-Landau
grimm@uni-koblenz.de

²Institut für IT-Sicherheit und Sicherheitsrecht
Universität Passau
volkamer@uni-passau.de

Abstract: Remote electronic voting systems are more and more used - not so much for parliamentary elections, but nevertheless for elections on lower levels as in associations and at universities. In order to have a basis for the evaluation and certification, in Germany a Common Criteria Protection Profile [PP08] is developed, which defines basic requirements for remote electronic voting systems. This Protection Profile requires a rather low evaluation depth (EAL2+). For elections on higher levels an appropriate adjustment of the evaluation depth is recommended. In its first part this paper points out that increasing the evaluation depth beyond EAL5 is not possible at present, since EAL6 requires formal methods and in particular a formal IT security model. Such a formal model does not exist yet. In the second part, this paper proposes a first step to an IT security model for remote electronic voting systems, which, however, considers only a subset of the security objectives defined in the Protection Profile [PP08].

1 Introduction

Over the last two years, the Gesellschaft für Informatik (GI – the German society of computer scientists) has developed a Protection Profile (PP) for a basic set of security requirements for remote electronic voting systems [PP08] in cooperation with the Bundesamt für Sicherheit in der Informationstechnik (BSI – German Federal Office for Information Security) and the German Research Center for Artificial Intelligence (DFKI). The Protection Profile is based on the Common Criteria [CC06]. It defines a minimum set of security objectives, which every remote electronic voting system has to ensure and a set of assumptions to the environment, in which the system is used. A remote electronic voting system certified against this Protection Profile [PP08] assures a secret, free, equal and universal election only under the condition that the system is used in an environment where the defined assumptions hold.

The Common Criteria (CC) together with the Common Evaluation Methodology [CEM06] define how the compliance of a particular system with the defined security objectives has to be evaluated. The CC differentiates between different evaluation depths. They distinguish between evaluation assurance level (EAL) 1 to 7+, whereby 7+ means the most intensive evaluation. Generally, the deeper this evaluation goes, the higher is the trustworthiness into the certified system. The scope of the system to be evaluated, the evaluation complexity, and the evaluation methods rise with rising EAL level. The Protection Profile, which defines a basic set of security requirements for remote electronic voting systems, requires the assurance level EAL2+ which is characterised by the following aspects:

- Execution of independent and structured tests by the evaluator
- Analysis of the documentation up to the high-level design and the interface specification
- Analysis of the strength of the functions
- Search for obvious vulnerabilities by the evaluator
- Presence of a configuration system
- Evidence of secure system delivery procedures

EAL2+ is certainly sufficient for elections in associations, schools and universities, but not for elections on higher levels and in particular not for parliamentary elections. Thus, for example, the persons in charge of the Protection Profile, which define requirements for the digital election pen³⁶ [PP06]³⁷, require EAL3+³⁸. Some critics demanded EAL4 and even higher.

³⁶ The digital election pen had been planned for the citizenry election in Hamburg in February 2008.

³⁷ The Protection Profile is based on the Common Criteria version 2.3.

³⁸ The Protection Profile required EAL 3 augmented with the following components: ADV_SPM.1 (Informal TOE security policy model) and AVA_MSU.3 (Analysis and testing for insecure states) - replacing AVA_MSU.1.

In the past, systems have been predominantly evaluated according to evaluation assurance levels equal or below EAL4+, since starting from the EAL5 semi-formal and/or formal methods are required. The application of such methods causes substantial additional effort for manufacturers and evaluators. The decision for such a high evaluation assurance level should be made before starting the development because (semi-)formal methods cannot be implemented in the follow-up (the effort to do so in the follow-up is as large as a complete new development). However, EAL5 provides a substantial increase in the trustworthiness of certified systems compared to EAL4, because a semi-formal description of the system design as well as a more modular and therefore better analysable architecture is demanded. A corresponding increase can be identified from EAL5 to EAL6 because the semi-formal specification languages are replaced by formal specification languages. "Past experiences show that a formal modelling of the security policies given as a formal security model may lead to an increase of confidence in the security of the product that obeys these security policies." [DFKI02]

Starting from EAL6, the Common Criteria component ADV_SPM.1 has to be ensured, which demands the use of a formal IT security model. Moreover, the component requires a consistency proof (in form of a mathematical proof) for the model itself and a compliance conformance between the system specification and the defined model. To do so, it is possible to use already published and established formal IT security models³⁹ as a whole or in parts. If no suitable formal IT security model exists, such a model must be developed.

The latter case holds for remote electronic voting systems. Therefore, such a formal IT security model has to be developed before an evaluation according to EAL6 and/or 7 can be aimed. In the context of this article we point out, by the example of some concrete security objectives defined in the Protection Profile, how such a formal IT security model can be designed.

In the further contribution, the definition of an IT security model is introduced (see chapter 2), then it is discussed whether existing IT security models can be applied (see chapter 3). Subsequently, security objectives from the Protection Profile are identified, which are considered for the definition of a formal IT security model (see chapter 4), and afterwards a formal IT security model is developed and proven to ensure all characteristics of an IT security model (see chapter 5). The paper closes with the proposal of future work activities and a short summery (see chapter 6).

³⁹ Examples for available and established IT security models are: Bell/LaPadula model, the Clark Wilson model, and the Biba model.

2 IT Security Model (General Introduction)

Model Definition. According to [Grimm08], IT security models define system states and state transitions, differentiate between secure and insecure states, and explain under which circumstances secure states are reached. An IT security model can be more or less formal. All IT security models contain the following *five description elements*:

1. The definition of a superior security objective
2. The specification of secure system states⁴⁰ which represent together the superior security objective
3. A trust model, describing a set of assumptions about the environment in which the system is used and under which the set of secure system states is equivalent to the superior security objective.
4. A set of permitted state transitions
5. A security theorem, claiming that applying any permitted state transitions to any secure state necessarily transfers to a secure state again.

Explaining the Coherences. An IT security model has to close the following two gaps:

- between the secure system states and the superior security objective (trust model in 3) and
- between the permitted state transitions and the secure system states (security theorem in 5).

For our purpose the first gap is already closed by the Protection Profile; in particular by

- the security problem definition, including a list of assumptions about the environment,
- the list of security objectives for the system, and
- the discussions in section „security objective rationale“.

Therefore, this aspect is not further discussed in this paper. The second gap is closed by the security theorem with its corresponding proof in sections 4 and 5 of this paper.

⁴⁰ The specification of secure system states corresponds to the Common Criteria security objectives (in case of a non formal IT security model).

Definition of Secure System States and Permitted State Transitions. The secure states (description element 2) and the permitted state transitions (description element 4) have to be described as accurately and precisely as possible. One informal way to formulate secure states is the definition of security objectives according to the Common Criteria [CC07]. In this case, the security theorem (description element 5) is proven by a linguistically convincing and conclusive argumentation. For applications which require a high security assurance, the definitions of a secure state and of permitted state transitions must be consistent and the corresponding security theorem must hold without any doubt. In this case, it is necessary to specify the secure states and the permitted state transitions in a formal way, and the security theorem must be proven with mathematical means. The formal specification of both together (in description elements 2 and 4) together with the formal proof (in description element 5) represents a *formal IT security model*⁴¹.

In the case of a formal IT security model, a third gap has to be closed - the gap between the linguistically formulated security objectives from the Protection Profile and the formal specification of the secure states. This cannot be formalised, but this is the subject of an argumentative discourse of security and application experts.

Advantages of the Application of Formal Methods. The application of formal IT security models has three main advantages:

- No natural language can guarantee an unambiguous interpretation and, therefore, it provides no feasibility to prove consistence in the formulation of secure states and permitted state transitions. Vulnerabilities in the implementation of these are a consequence. In contrast, the application of mathematical established technical equipment, which makes the application of computer-aided proofs possible, enables the definition of unambiguous and inter-subjective secure states and permitted state transitions.
- The development of a formal IT security model is used to identify and remove inconclusive, inconsistent, contradictory, or not enforceable secure states and/or permitted state transitions which cannot be detected with natural language.
- Using natural language for the specification of secure states and permitted state transitions causes similar problems for the evaluator - it is hard and in general not unambiguous to decide whether the implemented security functions are sufficient to ensure the specified secure states and permitted state transitions. Based on a formal specification of the system, it can be formally proven that the specification and later the implementation conform to the formal specification of the secure states and permitted state transitions.

⁴¹ The Common Criteria defines formal security models in the following way: "A formal security model is a precise formal presentation of the important aspects of security and their relationship to the behaviour of the TOE; it identifies the set of rules and practises that regulate how the TSF manages, protects, and otherwise controls the system resources. [...] the formal security policy model is merely a formal representation of the set of SFRs being claimed." [CC06]

3 Application of Available IT Security Models for elections

To our knowledge, no formal IT security model is available which completely covers the superior security objective of a secure remote electronic election. Caused by the numerous different tasks of a remote electronic voting system, the existence of such a model also seems to be unrealistic. However, the integrity model of Clark Wilson [CW87] and the confidentiality model of Bell-LaPadula [BLP73] can possibly describe partial security objectives.

The Clark Wilson model introduced the separation of duty principle to security modelling. For different partial security objectives in the context of a remote electronic voting system, it might be possible to use the separation of responsibilities in the sense of Clark Wilson. The Protection Profile defining basic security requirements for remote electronic voting systems [PP08] demands, for example:

***O.AuthPollworkers:** The TOE implements an authentication function which supports the separation of duty principle for at least two members [...]. Thus, at least two poll workers control each other.*

This PP security objective corresponds to the certification rule C3 and the penetration rules E2 and E3, which describe the "internal consistency" of a system in the Clark Wilson model:

- E2: The system has a list mapping users to transaction procedures (user X, TPi, (CDIa, CDIb, CDIc, ...)) and ensures that users can only execute transaction procedures according to this list.
- C3: The allocation list from rule E2 complies with the separation of duty principle.
- E3: The system authenticates the user's identity before executing any transaction procedure.

The Bell-LaPadula model prevents confidential information flow to public domains. This is achieved by mandatory access control. This approach could conceivably structure voters, poll workers, ballots and the ballot box in a hierarchical information flow model à la Bell-LaPadula and, thus, to model the secrecy of the vote. These approaches are still open research tasks.

The following chapters will discuss other security objectives defined in the Protection Profile, which cannot be modelled with Bell LaPadula, Clark Wilson or none of the other well-known formal IT security models. Therefore, a new formal IT security model is developed for these PP security objectives. The developed transaction procedures for the penetration of these security objectives could be embedded into a superior separation of duty model according to Clark Wilson. This integration needs to be further analysed in the context of future work.

4 Selection of PP Security Objectives

The development of a formal IT security model for remote electronic voting systems is a complex task and happens gradually by adding security objectives, defined in the Protection Profile, step by step. The security model, which will be presented in chapter 5, is a first step accomplished for two selected security objectives from the Protection Profile defining basic security requirements for remote electronic voting [PP08]. This first step illustrates how the further security objectives can be specified formally. The two selected security objectives are:

O.UnauthVoter: *Only eligible voters who have been unambiguously identified and authenticated are allowed to cast a vote that is stored in the e-ballot box.*

O.OneVoterOneVote: *It is ensured that (A) each voter can cast only one vote and that (B) no voter loses his voting right without having cast a vote. [...].*

5 Formal IT Security Model for Remote Electronic Voting

Different possibilities to model a particular system exist. According to [Grimm08] an IT security model for the above identified security objectives can be described in the following way:

Definition of the Superior Security Objective (1). Execution of a secure, equal, universal, direct, secret, and free remote electronic election.

Definition of a System State. A system state is represented by a triple of the following three entries:

1. W – Set of eligible voters (those who are listed in the electoral register and have not yet cast a vote).
2. S – Set of (encrypted) votes stored in the e-ballot box.
3. $voter: S \rightarrow M$ – Mapping (encrypted) votes on their electors.
 M is a superset of W_{total} , that is, $M \supseteq W_{total}$. M contains any user who tries to access the remote electronic voting system, whether or not this particular user has the right to cast a vote. The function $voter$ assigns each (encrypted) vote to its producer (voter).

Remark 1: in the case of postal voting, the function $voter$ is realised by the outer envelope which is labelled with the sender's name and address. During the tallying phase, the sender information is checked and is verified whether $voter(s) \in W_{total}$ or $voter(s) \in M \setminus W_{total}$. In the first case, the outer envelope is removed and the inner one containing the vote is put into the ballot box, while in the second case the envelope is destroyed.

Remark 2: the values of *voter* are visible only for the last vote (or votes) cast into the e-ballot box, i.e., only for the $s \in S_{i+1} \setminus S_i$. After anonymising S , the values of *voter* cannot be reconstructed. Therefore, in praxis, the *voter* mapping should only be used during state transitions on the $s \in S_{i+1} \setminus S_i$. Secure state transitions are controllable on this “visible subset” $S_{i+1} \setminus S_i$ of S_{i+1} only (see rules for permitted state transitions (4) below). For the “invisible part” S_i of the *voter* mapping on S_{i+1} we define $voter_{i+1}|S_i = voter_i$.

Initial State. $\langle W_{total}, S_0 = \{\}, voter_0 = \{\} \rangle$ is the initial state.

W_{total} stands for the set of all voters in the electoral register (those who have already cast a vote and those who still have the right to cast a vote). The two empty sets S_0 and $voter_0$ stand for the empty e-ballot-box in the beginning and the corresponding empty mapping of the empty box on the users of the voting system.

Specification of Secure States (2). It has to be defined which properties represent a secure state. According to chapter 4, the PP security objectives O.UnauthVoter and O.OneVoterOneVote are selected to be specified in terms of formal state properties denoting a secure state:

- **O.UnauthVoter:** $\forall s \in S: voter(s) \in W_{total}$; that is, the e-ballot box contains only those e-votes ($s \in S$) from which the corresponding elector ($voter(s) \in W_{total}$) is listed in the electoral register. In order to ensure this, the voter needs to be unambiguously identified and authenticated.
- **O.OneVoterOneVote:** (A) $\forall s, s' \in S: voter(s) = voter(s') \Rightarrow s = s'$; that is, whenever the set S of cast votes contains two votes from the same voter, then these two votes are identical. Thus, only one of the stored e-votes is tallied. This means that each voter can cast only one vote.
(B) $\forall x \in W_{total} \setminus W: \exists s \in S: voter(s) = x$; that is, a voter can only become an elector if his e-vote is stored in the e-ballot box ($s \in S$). Thus, he cannot lose his right to vote without having cast a vote which has been successfully stored in the e-ballot box.

Remark It is easy to prove that these three conditions for a secure state are equivalent to the following two conditions: “ $W_{total} = W + voter(S)$ ” (where “+” denotes the disjoint union of sets) and “The *voter* mapping is injective.” An alternative way to prove the security theorem (5) would be to prove that these two conditions are implied by the permitted state transitions (4). However, we prefer to derive our three conditions of a secure state (2) directly from the following permitted state transitions.

Trust model (3). The set of assumptions about the environment and the corresponding reasoning are part of [PP08].

Permitted State Transitions (4). A state transition from state $Z_i = \langle W_i, S_i, voter_i \rangle$ to $Z_{i+1} = \langle W_{i+1}, S_{i+1}, voter_{i+1} \rangle$ is permitted if one of the following rules holds:

- State transitions in which no vote is cast:
[rule 1] $W_i = W_{i+1} \wedge S_i = S_{i+1} \wedge voter_i = voter_{i+1}$
- State transitions in which a vote is cast and successfully stored in the e-ballot box, that is, the sets S and W are modified:
[rule 2] $\exists s \in S_{i+1} : (voter_{i+1}(s) \in W_i \wedge W_{i+1} = W_i \setminus \{voter_{i+1}(s)\}) \wedge S_i = S_{i+1} \setminus \{s\}$

Remark 1: All $m \in M$ can initiate a state transition by casting a vote. However, for not permitted state transitions holds: $m \in M \setminus W_{total} \Rightarrow W_{i+1} = W_i$ and $S_{i+1} = S_i$.

Remark 2: The state transition rules use the *voter* mapping only on its visible part, that is, on $S_{i+1} \setminus S_i$. This makes the transition rules usable in praxis.

Theorem (5). For all permitted state transitions starting with the initial state, $Z_0 = \langle W_{total}, \{\}, \{\} \rangle$ holds that any reachable state is a secure state.

Proof. The theorem can be proven by mathematical induction. To simplify our notation, we write *voter* instead of $voter_{i+1}$ or $voter_i$, we understand that $voter_{i+1} \setminus S_i = voter_i$. To simplify the main proof, it is helpful to first prove that for all permitted state transitions Z_0 to Z_i the following three lemmas L1, L2 and L3 hold. These are now named and proven:

L1: $S_i \neq S_{i+1} \vee W_i \neq W_{i+1} \Rightarrow \exists s \in S_{i+1} : (S_{i+1} \setminus S_i = \{s\} \wedge W_i \setminus W_{i+1} = \{voter(s)\})$

Interpretation: During each permitted state transition according to [rule 2] exactly one new vote is generated and exactly the one associated voter loses his right to vote.

Proof for L1: In the case $S_i \neq S_{i+1} \vee W_i \neq W_{i+1}$, [rule 2] had to be applied. Therefore, there exists an $s \in S_{i+1}$ for which holds: $S_i = S_{i+1} \setminus \{s\}$: Thus s is the only element in $S_{i+1} \setminus S_i$. Therefore, the first part of the lemma is proven. Moreover, according to [rule 2] the following statement holds for this s : $voter(s) \in W_i$ with $W_{i+1} = W_i \setminus \{voter(s)\}$. Thus, $voter(s)$ is the only element in $W_i \setminus W_{i+1}$. Therefore, the second part of the lemma is proven.

q.e.d. (L1)

L2: $W_{total} = W_0 \supseteq W_1 \supseteq W_2 \supseteq \dots \supseteq W_i$

Interpretation: The set of eligible voters can only decrease.

Proof for L2: This lemma is a trivial consequence of [rule 2].

q.e.d. (L2)

L3: $\forall s \in S_i : \exists j < i : \text{voter}(s) \in W_j \setminus W_i$

Interpretation: For each vote stored in the e-ballot box, there exists a voting right discarded earlier.

Proof of L3: Application of proof by induction over i , starting with $i=1$:

Induction Base: For $i=1$: Choose $j=0$, then this case is equal to the special case of L1 with S_1 and S_0 .

Induction Hypothesis: L3 holds for some $i \geq 0$

Induction Step: For $i+1$ holds:

$\forall s \in S_{i+1}$ does either hold $s \in S_{i+1} \cap S_i$ or $s \in S_{i+1} \setminus S_i$. In the first case the statement is true according to the induction hypothesis. In the second case, L1 proves the statement.

q.e.d. (L3)

Back to the main Proof:

- *Induction Base:* All three secure state properties do hold for the initial state Z_0 because S_0 and $W_{\text{total}} \setminus W_0$ are equal to the empty set.
 - *Induction Hypothesis:* The secure state property holds for some state Z_i ; $i \geq 0$.
 - *Induction Step:* It needs to be shown that for all possible states Z_{i+1} reachable by permitted state transitions from Z_i holds that a secure state is reached:
 - [rule 1] $W_i = W_{i+1} \wedge S_i = S_{i+1}$; thus $Z_i = Z_{i+1}$. Therefore, applying the induction hypothesis it holds that also Z_{i+1} is a secure state.
 - [rule 2] $\exists s \in S_{i+1} : (\text{voter}(s) \in W_i \wedge W_{i+1} = W_i \setminus \{\text{voter}(s)\}) \wedge S_i = S_{i+1} \setminus \{s\}$
- We prove each of the three properties of a secure state separately:

O.UnauthVoter:

Induction Hypothesis: For some $i \geq 0$ holds: $\forall s \in S_i : \text{voter}(s) \in W_{\text{total}}$

Induction Step: Then for $i+1$ holds:

$\forall s \in S_{i+1} : s \in S_{i+1} \cap S_i \wedge s \in S_{i+1} \setminus S_i$.

- Case $[s \in S_{i+1} \cap S_i]$: this holds because of the induction hypothesis.
- Case $[s \in S_{i+1} \setminus S_i]$: according to L1 holds: $W_i \setminus W_{i+1} = \{\text{voter}(s)\} \Rightarrow \text{voter}(s) \in W_i$ and according to L2 holds: $W_i \subseteq W_{\text{total}}$, hence $\text{voter}(s) \in W_{\text{total}}$.

q.e.d. (O.UnauthVoter)

O.OneVoterOneVote(A):

Induction Hypothesis: For some $i \geq 0$ holds: $\forall s, s' \in S_i: voter(s) = voter(s') \Rightarrow s = s'$

Induction Step: Then for $i+1$ holds:

For all s and s' only the following three possibilities exist:

- Case $[s, s' \in S_{i+1} \cap S_i]$: this holds because of the induction hypothesis.
- Case $[s, s' \in S_{i+1} \setminus S_i]$: according to L1 holds: $S_{i+1} \setminus S_i = \{s\} \Rightarrow s = s'$
- Case $[s \in S_{i+1} \setminus S_i \wedge s' \in S_i]$: according to L1 holds: $W_i \setminus W_{i+1} = \{voter(s)\} \Rightarrow voter(s) \in W_i \setminus W_{i+1}$ and according to L3 holds $\exists j < i: voter(s') \in W_j \setminus W_i$. Thus, $voter(s) \in W_i$ and $voter(s') \notin W_i$. Thus, both values can never be equal. Thus, the statement holds also in this third case.

q.e.d. (OneVoterOneVote(A))

O.OneVoterOneVote(B):

Induction Hypothesis: For some $i \geq 0$ holds: $\forall x \in W_{total} \setminus W_i: \exists s \in S_i: voter(s) = x$

Induction Step: Then for $i+1$ holds: For $x \in W_{total} \setminus W_{i+1}$, x must be in one of the following sets:

- Case $[x \in (W_{total} \setminus W_{i+1}) \cap (W_{total} \setminus W_i)]$: this holds because of the induction hypothesis.
- Case $[x \in (W_{total} \setminus W_{i+1}) \setminus (W_{total} \setminus W_i)]$: according to L2 holds: $W_{total} \supseteq W_i \supseteq W_{i+1}$. Thus, $(W_{total} \setminus W_{i+1}) \setminus (W_{total} \setminus W_i) = W_i \setminus W_{i+1}$; thus, $x \in W_i \setminus W_{i+1}$; in addition, it holds: $W_i \neq W_{i+1}$. According to L1 holds $W_i \setminus W_{i+1} = \{voter(s)\}$ for $s \in S_{i+1} \setminus S_i$. Then, deduced from $x \in W_i \setminus W_{i+1}$ it holds: $voter(s) = x$; this completes the proof for $i+1$.

q.e.d. (OneVoterOneVote(B))

All together: q.e.d. (Theorem)

6 Future Work and Summary

Currently, a Protection Profile (PP) defining basic security requirements for remote electronic voting [PP08] is accomplished in Germany. This PP demands the evaluation assurance level EAL2+. The current discussions about the evaluation of electronic voting systems in general illustrate that the critics demand a high EAL level. We agree because political elections are the highest property of a democracy. Therefore, we believe that formal methods are well motivated for voting applications. However, concerning an evaluation according to EAL6 or EAL7 there are still a couple of open questions and research tasks to solve (not only concerning remote electronic voting). It is necessary to further discuss the specification of IT security models for remote electronic voting systems.

This contribution demonstrates with two examples how security objectives, defined by the basic profile PP can be integrated into a formal IT security model. Up to a complete formalisation of all security objectives and their integration in a closed IT security model for remote electronic voting systems, substantial research has to be carried out.

Acknowledgements

We thank Dieter Hutter for his helpful comments on our formalisation method.

References

- [CC06] Common Criteria for Information Technology Security Evaluation, Version 3.1, 2006.
- [CEM06] Common Methodology for Information Technology Security Evaluation, Version 3.1, 2006.
- [DFKI02] H. Mantel, W. Stephan, M. Ullmann, and R. Vogt. Leitfaden für die Erstellung und Prüfung formaler Sicherheitmodell im Rahmen von ITSEC und Common Criteria. Version 1.0c http://david.von-oheimb.de/cs/teach/BSI-Leitfaden_1.0c.pdf, 2002
- [Grimm08] R. Grimm, IT-Sicherheitsmodelle. Arbeitsberichte aus dem FB Informatik der Universität Koblenz-Landau, Feb 2008, erscheint in WISU
- [PP06] M. Volkamer and R. Vogt. Digitales Wahlstift-System. Common Criteria Protection Profile BSI-PP-0031, <http://www.bsi.de/zertifiz/zert/reporte/PP0031b.pdf>, 2006.
- [PP08] M. Volkamer and R. Vogt. Core Requirements for Online Voting Systems. Protection profile, German Research Center for Artificial Intelligence, 2008.
- [CW87] D. Clark and D. Wilson. A Comparison of Commercial and Military Security Policies. Proceedings of the 1987 IEEE Symposium on Security and Privacy, Oakland, CA. Computer Society Press of the IEEE, Washington DC, 184-194, 1987.
- [BLP73] D. E. Bell and L. J. LaPadula. Secure Computer Systems: Mathematical Foundations, and A mathematical model. ESD-TR-73-278, MTR-2547, Vols 1&2. The MITRE Corporation, Bedford, MA, Nov 1973.

The Certification of E-Voting Mechanisms. Fighting against Opacity

Jordi Barrat i Esteve

Dpt. Estudis Jurídics de l'Estat / R+D (SEJ2007-64886)

University of Alacant

Cta. Sant Vicent del Raspeig s/n

E-03690 Sant Vicent del Raspeig

jordi.barrat@ua.es

Abstract: Many countries are using certification procedures to guarantee the full compliance of e-voting mechanisms with democratic standards, but the data generated by these analysis is normally handled almost secretly. Given that transparency is a key principle to guarantee citizen's confidence in the electoral process, this opacity would only be acceptable after a correct balance of the concurrent interests. The paper provides specific data on the certification mechanisms of some countries and assesses the feasibility of a disclosure of the certification reports.

1 Introduction

Electronic voting raises several concerns, like, for instance, whether it can provide the same degree of electoral transparency and citizen control that already exists in our current elections. It is not clear how it can guarantee a meaningful recount similar to the traditional one based on paper ballots given that one of the main problems of any electronic voting solution is that an average citizen cannot easily understand how it is working. The current electoral structure allows everybody, even a person without specific skills, to check the accuracy of the process, but unfortunately the electronic voting platforms, at least if they have no paper trail, will never achieve the same degree of external supervision. Its implementation, therefore, should be to strengthen by supplementary control measures, so that, although different from the traditional ones, it would emulate the current framework so that the citizenry could have enough confidence in these new electoral devices.

Although there are different solutions to this problem (e.g. open source e-voting platforms), one of these new mechanisms could be a certification process. They already exists with the traditional paper voting systems, but they become much more important if applied to electronic voting platforms. The electoral authorities would only agree to voting machines that, according to several technical analyses, comply with detailed conditions previously set up. This process would be quite similar to the certification of industrial products, but here there are some specific features because we are not trying to check only whether a device is technically correct. We are also trying to compensate for the lack of citizen control that exists where voting procedures accept computer components. Moreover, ordinary industrial products generate external evidences of their performance, but electronic voting solutions cannot provide these external data because they must also guarantee the secrecy of the vote.

There are several items to be analysed in a certification procedure. The first one could be to decide who will actually carry out the technical analysis that any certification process entails (i). We should opt between public or private bodies and we could also analyse which criteria have been used for each appointment and the detailed conditions and terms to conduct this task. We could also wonder which components of the voting machines will be checked (ii). Once again, the landscape is very different depending on the country. We could find very detailed lists of requirements to be checked by the certification institutions, but also very ambiguous and generic documents. A third focus point could be the legal rules about the disclosure of the reports issued by the certification bodies and the availability of the overall file, that is, the technical documentation of the voting machine (e.g. source code) (iii). Following the patterns of the ordinary industrial certification processes, these policies use to be very opaque.

Due to length restrictions, this paper will only provide an overview of the third point. The analysis includes a preliminary theoretical approach in conjunction with detailed references of some real cases of binding electronic voting systems, namely in Belgium, Estonia, Netherlands (Internet voting not included) and France (Internet voting not included). However, a full understanding of the problem would also require taking into account the approaches developed in other countries like, for instance, the United States, Venezuela or Brazil.

2 The Certification Reports: How to Handle Sensitive Data

The credibility of a system such as electronic voting is supported by a combination of measures designed to increase its openness. The certification is one of these measures, but its actual effects will largely depend on the disclosure of its final findings and it is worth noting that, except for some slight nuances, in all the cases which have been observed, the decision taken was to restrict to the maximum the access to the documentation produced by the technical analysis.

Thus, we should not place too many expectations on the efficacy of the certification measures, at least strictly from the citizen's point of view. There is no doubt that such measures are thought to carry out a correct supervision, but, if such an obscurity is kept, they will by no means be able to emulate the openness and popular control guaranteed by the traditional voting systems. We shall analyse below the situation observed in several countries, paying special attention to the arguments put forward in order to deny access to the aforementioned documentation and also to certain situations where the possibility to achieve a wider spread seems to be making its way.

The French case is particularly interesting, since the public authorities had to take a position regarding a request by which a citizen expressly demanded the disclosure of the certification reports related to the three authorized voting companies. On February, 3rd 2006 the French Ministry of the Interior refused to grant such a claim following the criteria provided by the CADA –*Commission d'Accès aux Documents Administratifs*—. The CADA is an advisory body whose mission consists precisely on deciding, in the light of the regulations on the access to public information, which documents can be actually disclosed and, on the basis of different criteria, which must be handled in a different way. This Commission recommended not to disclose the requested documentation, arguing that it could be detrimental to "le secret industriel et commercial ... [et] compromettre le bon déroulement des élections" (the commercial and industrial secrecy ... [and] endanger the correct electoral management).⁴²

Two reasons are given. The first one (i) emphasizes the rights of the private companies which take part in the process, pointing out that the disclosure of the documentation could be detrimental to their interests, specifically to their commercial and industrial secret. Please note that we are referring to the two companies involved and not only to the one that undertakes the development of the computer applications. This fact implies that both would be at risk, on the one hand, the control over the voting technological solution, and, on the other hand, the internal certification methodology used by the company responsible for drafting the report.

From my point of view, an ideal solution must take into account these legitimate interests, but it must also avoid considering them to be the only important interests in this field. As it has been pointed out before, electronic voting does not have the same features as other areas where the certification reports are normally secret. The reports related to many industrial products are subject to these opaque rules, but the electronic voting has a peculiarity that consists in the fact that it is impossible to verify whether the system really works properly. For instance, it will be relatively easy to prove that an authorized train does not meet the analysed parameters, since external evidences will appear. If an authorized train fails to reach the speed that it should theoretically achieve according to a previous technical document, it is obvious that someone has failed—either the railway company or the certification authorities.

⁴² Document available at: www.ordinateurs-de-vote.org/IMG/jpg/cada.jpg [September 7th 2007].

Unfortunately, this method cannot be used in the electronic voting field. In view of the fact that the vote is secret, and unless we decide to implement a paper receipt, there is no external evidence beyond the computer audit that allows us to assert that the results obtained by means of the electronic system faithfully reflect the voter's will. As a matter of fact, the scandals arising from some electronic voting applications, such as the those caused in Sarasota (Florida) or in Schaerbeek (Belgium), are based on absolutely illogical results, as, for instance, the recording of an unusually high rate of abstentionism in a given election⁴³ or a vote distribution that is incompatible with the electoral formula.⁴⁴ These extreme cases may in fact be inspected, and such has been the case, but nothing can be done in other less dramatic cases that would happen, for instance, if the electoral fraud consisted only in shifting the direction of a vote in each constituency.

Thus, the legal framework, which supports the certification of the electronic voting, must rest on this basis and not, as usually happens, on the false premise that the general guidelines for the certification of other products are also applicable in this field.

The ideal solution would obviously consist in enforcing the public and general disclosure of these reports, but before reaching such a stage, it is advisable to examine the possibility of finding an intermediate solution which may not only satisfy the companies involved, but which could also be especially beneficial for the openness required by any electoral system.

⁴³ In 2006, Christine Jennings lost her seat as a representative by a very few votes, but in Sarasota County something strange happened and more than 10% of the voters, even though they had attended the polling station and had voted in many of the simultaneous calls for elections that usually take place in the United States, surprisingly decided to abstain from the election for the House of Representatives, which is one of the most important calls. Moreover, if we compare this percentage with that obtained in the neighbouring region, we will easily prove that the citizens who behaved in a similar way in such a region were many fewer on a relative footing. Further information at: Division of Elections / Florida Department of State - <http://election.dos.state.fl.us/CongressDistrict13.shtml> [September 15th 2007].

⁴⁴ To be specific, a candidate obtained a number of preferential votes that exceeded the votes received by the list of candidates in which he was included. There was a difference of 4096 votes. The Collège des Experts, together with the company involved and the Ministry of the Interior itself, pointed out that the most probable reason "pouvait être attribuée à une inversion spontanée d'une position binaire dans la mémoire vive du PC ... Un écart de 4096 peut être occasioné par une inversion de la 13ème position binaire du compteur" (could have been a spontaneous inversion of a binary position within the live PC memory ... A difference of 4096 [votes] could be generated by an inversion of the 13rd binary position of a counting device) [Co03, p.19]. The existence of a physical endorsement for each vote in the form of magnetic cards made it possible to repeat the counting and, in view of the fact that this technical incident did not happen again, they opted to accept the second results as valid. However, this does not make what happened less serious and it raises the question of what the solution would have been in the event that there had been no magnetic cards.

We may consider first whether the very premise on which we rely is certain, that is, whether the belief that disclosing these reports will unavoidably entail an irreparable harm for the industrial and commercial property rights of the companies involved. As a matter of fact, stating that this belief is certain, at least in such a convincing and general way, is far from reflecting the reality. There are several factors that must be taken into account and that may make this statement more flexible in certain respects. One of these factors consists in requiring certain previous certification parameters, which must be detailed and comprehensive and must even include the method to be used for the verification. This is what happens in France, where the electronic voting systems must accredit that a total of 114 conditions of different kinds are met. One of the sections included in the certification reports will obviously consist in a detailed review of these requirements and the integration of the corresponding comments regarding the fact of whether or not the voting prototype has passed the tests.

If the circumstances are as described, the risk of revealing important trade and business secrets seems to be quite remote, and thus, allowing at least a partial disclosure of the certification reports would be reasonable. We should bear in mind that sometimes the comments will not just consist in an affirmative or a negative remark, but they will provide some additional information and these are the details which will precisely help strengthen the electoral openness and the trust of the citizens. The incident that occurred in France regarding the internal clock of NEPAD's machines is a perfect example of what has been stated.⁴⁵

⁴⁵ As a result of a lawsuit brought in Vaucresson, the Ministry of the Interior disclosed part of the report that Bureau Veritas had drafted for NEDAP [available at: www.ordinateurs-de-vote.org/IMG/pdf/nedap_20070412_veritas.pdf (September 7th 2007)]. The issues at stake were, on the one hand, the hypothetical contradictions between the devices manufactured by NEDAP, which had been purchased at that time in Vaucresson, and on the other hand, some of the conditions which were required by the technical regulations on which a report had to be delivered by the certification authorities, to be specific by Bureau Veritas.

Thus, for instance, the 6th requirement establishes that the members of the polling station must be able to "régler l'horloge interne de la machine à voter" (adjust the internal clock of the e-voting machine) and to the same effect the 46th requirement states that such adjustment must rely on "les données heure-minute-seconde" (the data hour-minute-second). The aim of both conditions is to get devices able to "dater les divers événements et comptes-rendus mémorisés au cours d'un scrutin" (fix the temporal data of the different actions and memos saved during the election) (46th requirement) and, subsequently, the final printings produced by the voting machine must include "les heures d'ouverture et de clôture du scrutin" (opening and closing hours of the election) (19th requirement). Another important issue was the locking mechanism of the voting system, since the 7th requirement envisages "un double dispositif d'authentification électronique" (a double electronic authentication device).

To begin with, from my point of view, it is difficult to assert that the pages that were sent to court compromise the trade secrets of NEPAD or *Bureau Veritas*. In both cases the pages only contained some three-column tables where, together with a tag regarding each requirement demanded by the legal regulations, *Bureau Veritas* had included a comment to the effect of whether or not the prototype complied with each legal condition. Should there be any doubt about the interpretation of the legal regulations or about the total or partial compliance with them, as in the clock's case, the certification authority shall reflect the results obtained and describe as minor or major discrepancies the differences that have been found. All-in-all, we are dealing with documents which neither uncover a computer's architecture nor explain in detail the internal methodology of *Bureau Veritas*, but still they can be extremely helpful for the citizens to get an exact idea of how an electronic voting system works.

For instance, in the internal clock's case, the most important fact is not so much whether or not the machine has an absolute or a relative timer, an argument which was, by the way, rejected by the *Conseil d'État*⁴⁶ as well as by the *Conseil Constitutionnel*.⁴⁷ The important fact is that now reading the report lets us know that the machine did not really comply with all the legal requirements and that the certification company as well as the Ministry itself had to resort to the cunning argument that the discrepancies were minor in order to be able to validate them.⁴⁸

⁴⁶ As a result of an appeal lodged in Versailles, the Conseil d'Etat solved this question as follows: "Considérant ... que le règlement technique fixant les conditions d'agrément des machines à voter impose seulement que les machines soit dotées d'une horloge interne que le bureau de vote puisse régler lors de son initialisation et qui permette le chronométrage des événements du scrutin, mais n'exige pas que ce réglage et ce chronométrage soient opérés directement en fonction de l'heure légale; que par suite il est manifeste que le système d'horodatage 'relatif' retenu par les concepteurs de ces machines ne méconnaît pas les conditions d'agrément des machines à voter" (Taking into account ... that the technical document is only requiring an internal clock for each voting machine that could be adjusted by the polling staff during the opening and that allows the chronological counting of the actions generated during the election, but it does not require a counting linked to the official hour; it is thus obvious that the relative counting foreseen by the computer scientists fully complies with the conditions for the acceptance of the voting machines) (Ordonnance no. 305184 from May 2nd 2007).

⁴⁷ The Conseil Constitutionnel literally accepted the judgement given by the Conseil d'Etat and, on the basis of the same objection, dismissed an appeal lodged in Aulnay-sous-Bois as a result of the parliamentary elections held in June [Decision 2007-3449 from July 26th 2007]. May I draw your attention to the fact that the argument related to the existence of a mechanical key does not seem to have been used either in the litigation before the Conseil d'Etat or in the one before the Conseil Constitutionnel.

⁴⁸ Diverse mechanisms are used in order to deal with the literal sense of the technical requirements, although they all have a common origin, which is some discrepancy between the voting system subject to analysis and the legal requirements. Sometimes the strategy consists in acknowledging some minor discrepancies which, therefore, would not compromise a general positive assessment. This is what happens with the mechanical key problem (7th requirement) and, setting aside the classification of the incident as serious or slight, with the implementation of a relative clock (6th requirement).

However, sometimes the certification authority agrees that the corresponding requirement has been met, even though the previous comments logically lead to a different conclusion. Such is the case, for instance, of the 19th requirement which states that the documents generated by the computer contain all the data "exceptées les heures d'ouverture et fermeture, qu'il convient d'ajouter à la main" (unless the opening and closing hours, that should be manually added) (the italics are mine). The surprising fact is that, as it was pointed out before, according to the technical document, these data related to time are precisely the data which must be printed.

This detail could only become known as a result of the publication of the extract sent to court, since it was not included in any of the previous public statements. In this sense, a wider spread of these tables which, as has been said before, do not compromise the commercial interests of the companies, could provide the citizens with a more complete and detailed sight of the certification process, of the possible implications of the discrepancies, and of the criterion used by the certification authorities in order to classify them as minor or major discrepancies. Although most of the citizens actually lack technical knowledge, such data would allow them to have a better-grounded opinion on whether or not the certification process has been properly designed to perform its purpose, that is to say, to verify whether or not the electronic voting system observes the basic principles of any democratic election.

Other parameters to be taken into account consist in identifying which players will actually receive the sensitive data of the e-voting company and under which conditions. If we implement a certification process, the vendor is accepting to provide sensitive data to a third party, that is, the certifying body, and it seems therefore feasible that other stakeholders might have access to the same information or, at least, to the final report generated by these certification activities. Obviously the vendor could require some conditions, like a confidentiality agreement similar to the one already accepted by the certification body, but there should be no obstacle to broaden the recipients of this information to research groups, to professional corporations or to given civil society organizations closely related to these topics. It would not be a full openness, that could barely guarantee a minimum of confidentiality, but we are managing to involve some supplementary stakeholders. We maintain the same confidentiality conditions already implemented, but we enhance the principle of transparency.

If we analyse the praxis in some countries, we will easily discover that the apparently strict confidentiality requirement is actually breached in some cases. *ES&S*, for instance, accepted during the last French presidential elections, a partial disclosure of its *Bureau Veritas* certification report to some customers belonging to local administrations because, in France, these bodies are actually deciding which e-voting supplier, among the three previously authorized, is the best one. These representatives were invited to *ES&S* headquarters where they could read –not copy— the report. If the vendor itself is implementing such protocols, it would hardly be acceptable not to provide the same information with the same conditions to other stakeholders that seem to be at least as important as local authorities. I am referring, for instance, to political parties.

Belgium is an interesting example, although we will also find some paradoxes. While the source code is largely spread, the certification reports, apparently less dangerous information, are handled with great opacity. The source code is delivered to the political parties even before the elections, although they have to respect a confidentiality agreement. Their IT experts could therefore analyse the system and communicate to the Ministry of Interior whatever mistakes they have found. Second, the electoral authorities upload the full source code to the website immediately after the elections.⁴⁹

⁴⁹ See a technical analysis carried out by aFRONT based on the source code used in 2003 and 2004: www.afront.be/lib/vote.html (September 15th 2007).

This transparent behaviour hardly matches with the treatment provided to the results of the certification activities. It would be difficult to reject the publication of the certification report on the grounds of risks for the industrial property, because the source code will already be known by the citizenry. Following the aforementioned Fresh arguments, we could also argue that what is actually in danger is the methodology of the certifying institution, but we already know that this parameter could have minor relevance if the criteria are previously set up in a very detailed way. Unfortunately, Belgium does not meet this condition because the criteria are not detailed and therefore the certifying bodies have large powers to assess whether the software complies with them.

This opaque approach may have unwanted consequences since the citizenry could become more and more reluctant to easily accept the fair behaviour of the electoral authorities. It is worth recalling, for instance, the following statement of the *Collège des Experts*: "Il est à noter que l'attitude du SPF Interieur vis à vis les rapports des organismes d'avis est fort peu critique. En effet, peu importe la qualité des tests, un rapport positif est visiblement accueilli avec un gran soulagement" (It is worth noting that the Ministry of Interior's behaviour is not very rigorous regarding the reports issued by the certifying companies. Despite the actual quality of the checks, a positive report is publicly received with a great relief) [Co07, p. 16]. The only way to avoid this perception is to accept a full disclosure of the certification report and the *Collège* actually makes this recommendation later [Co07, p. 28].

The Netherlands also has a nuanced framework that does not match with the simple and quick French solution. The *Brightsight's* report was kept secret during the 2006 elections, but the implementation of the Act regarding a free access to the public information allows the disclosure of significant data about the relationships between the electoral authorities and their computer supplier *Groenendaal* [Wv07]. The certification report is not publicly available yet, however.

Finally, assuming that Estonia does not have a formal certification procedure [DM02, p. 238], its electoral authorities accepted in 2007 several verifications carried out by specialists, but unfortunately "the results of these reviews were not made public" [Os07, p 15]. The private audit, carried out during the electoral period aiming to check whether the operational protocols were correctly followed, is not publicly available either [Os07.p. 15].

There are therefore some interesting paradoxes. While the system seems to be very open, accepting reviews carried out by any interested group, the subsequent decisions are very opaque because the findings of these procedures remain secret. Is it actually useful, from a democratic point of view, to foster such confidentiality agreements? Obviously these reviews are important achievements, mainly if we take into account what is happening in other countries, but their usefulness is not clear since we will not be able to alert the society to the vulnerabilities that we could have found.

It is difficult to find balanced solutions in these cases, but we could try to soften confidentiality agreements so that any person could at least publicly provide a general overview of his/her analysis confirming the system's reliability or pointing out some weaknesses. The first statement will definitively strengthen the citizen's confidence and the second one, even in these generic terms, will likely rouse citizen's concerns and will foster further check ups by the electoral authorities themselves.

Finally, there was a second argument (ii) within the CADA's recommendation. A full disclosure of the certification reports "pourrait compromettre le bon déroulement des élections." Certainly, one common argument against open source is the risk to provide sensitive information to external hackers. Although this is a technical debate and this paper only has a legal approach, it is worth underlining that many computer scientists, even perhaps a large majority, are actually supporting open source solutions as the best ones. Jason Kitkat, for instance, thinks that a disclosure is not neutral and actually increases the system's security: "Cryptographers and security professionals use peer review to provide assurance for the quality of their systems. A security scheme whose source code and design is known yet continues to offer a useful level of protection is a good one" [Ki04, p. 65; same opinion Ru06, p. 125]. There will be other challenges, like the verification that all the devices are actually containing the correct code, but the security and robustness of the product would be enhanced with an open strategy.

3 Concluding Remarks

The certification of industrial components used to be an ordinary procedure thought to guarantee their quality and security within a standardized protocol of supervision mechanisms. However, electronic voting platforms have some specific features, like the need to maintain the transparency of any electoral step and the lack of a paper trail that, if required, could allow us to perform a second tally. Since the certification process should take into account these specific needs, we should profile a special protocol for this single product. Although there are several items to analyse: who is doing the technical analysis (i), which criteria should be used (ii) and who should receive the final reports (iii), this paper is only focused on the third one.

The protection of the industrial property has been so far a common argument to reject a full disclosure of the certification reports. It is a legitimate position, but it should be balanced with other approaches given that we are talking about electoral processes and therefore the citizens' confidence in the system should be a major outcome. A fair business concurrence might also be a sound argument against opacity. Should e-voting systems increase their implementation worldwide? Should new or more balance between transparency and property be sought? Despite the current framework, the paper shows how some minor data coming from given countries actually suggests that the opacity is not well grounded and that it would be easily feasible to include a certain degree of transparency without breaching the industrial property.

These humble measures could be a good beginning in order to achieve afterwards a new balance between electoral transparency and other opposite interests. Moreover, the Belgian experience should be seriously taken into account, because its structural weakness, the Collège des Experts, provides external control over the e-voting process.

References

- [AH04] Álvarez, M.; Hall, T.: Point, Click and Vote: The Future of Internet Voting. The Brookings Institution, Washington, 2004.
- [Co03] Collèges des Experts: Rapport concernant les élections du 18 mai 2003. Collège des Experts chargés du contrôle des systèmes de vote automatisés, [Brussels], 2003. www.poueva.be/IMG/pdf/RapportExperts2003.pdf [September 15th 2007]
- [Co07] Collèges des Experts: Rapport concernant les élections du 10 juin 2007. Collège des Experts chargés du contrôle des systèmes de vote automatisés, [Brussels], 2007. www.poueva.be/IMG/pdf/RAPPORT_CONCERNANT_LES_ELECTIONS_DU_10_JUIN_2007.ocr.pdf [September 8th 2007]
- [DM02] Drechsler, W.; Madisse, Ü.: E-Voting in Estonia. In: Trames. Journal of the Humanities and Social Sciences. n. 3, 2002; P. 234-244.
- [Fe07] Fernández Rodríguez, J. J.: Voto electrónico. Estudio comparado en una aproximación jurídico-política (Desafíos y posibilidades). Fundap, Querétaro, 2007.
- [Gr03] Gritzalis, D. A. (ed.): Secure Electronic Voting. Advances in Information Security. Kluwer, Boston, 2003.
- [KB04] Kersting, N.; Balderstein, H. (eds.): Electronic Voting and Democracy: a Comparative Analysis. Palgrave Macmillan, Basingtoke, 2004.
- [Ki04] Kitcat, J.: Source Availability and E-Voting: An Advocate Recants. In: Communications of the ACM. n. 47(10), 2004; P. 65-67. <http://doi.acm.org/10.1145/1022594.1022625> [September 4th 2007]
- [Kr06] Krimmer, R. (ed.): Electronic Voting 2006. (Col. "Lecture Notes in Informatics – LNI" / P-86), Gesellschaft für Informatik, Bonn, 2006..
- [OS07] Osce: Republic of Estonia. Parliamentary Elections 4 March 2007. OSCE/ODIHR Election Assessment Mission Report. OSCE (The Organization for Security and Co-operation in Europe), Warsaw, 2007. www.osce.org/item/25385.html [September 15th 2007]
- [PK04] Proser, A.; Krimmer, R.: Electronic Voting in Europe. Technology, Law, Politics and Society. Gesellschaft für Informatik, Bonn, 2004.
- [Ru06] Rubin, A. D.: Brave New Ballot. The Battle to Safeguard Democracy in the Age of Electronic Voting. Morgan Road Books, New York, 2006.
- [TM05] Trechsel, A. H.; Méndez, F. (eds.): The European Union and E-Voting. Addressing the European Parliament's Internet Voting Challenge. Routledge, London, 2005.
- [Tu05] Tula, M. I. (coord.): Voto electrónico. Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales. Ariel, Buenos Aires, 2005.
- [Wv07] Wvsn: Voting systems company threatens Dutch state. Ed. Wij vertrouwen stemcomputers niet — WVSN, Amsterdam, 2007. www.wijvertrouwenstemcomputersniet.nl/English/Groenendaal [September 2nd 2007]

Session 7: Technological Issues of E-Voting

Code Voting With Linkable Group Signatures

Jörg Helbach¹, Jörg Schwenk², Sven Schäge³

Chair for Network and Data Security
Ruhr-University Bochum
Universitätsstr. 150
D-44780 Bochum

¹joerg@helbach.info
^{2,3}{joerg.schwenk|sven.schäge}@rub.de

Abstract: Code Voting is an appropriate technology to deal with the “Secure Platform Problem” [Riv02]. However, code voting as proposed by Chaum [Cha01] is vulnerable to vote selling and other flaccidities. In this paper we describe the vulnerabilities of code voting and propose to extend code voting to prevent vote selling. For this purpose we combine code voting with linkable group signatures and vote updating. We analyze the security properties of this new approach.

1 Introduction

Regarding remote online voting systems one of the major issues is the security of the voting client, i.e. the personal computer of the voter, as it cannot be considered to be trustworthy. Due to this fact in 2002 Ronald Rivest coined the term “Secure Platform Problem” [Riv02]. Even though different cryptographic voting protocols exist, the problem is that the voting client could be infected with malicious software, which is nowadays a widespread problem. Some estimates say that between 15% and 25% of all computers on the Internet are infected with malware bots [Web07], i.e. they have been under the complete control of an adversary. Hence, the voter cannot be sure that his electronic ballot is submitted faultless and unmodified to the voting server. Some methods for resolving this problem have been analyzed in [Opp02]. A good approach to overcome this problem is to use code voting as introduced by David Chaum in 2001 [Cha01]. Instead of a candidate's name, the voter only submits a voting transaction number (voting TAN) to the voting server. There is no correlation between the chosen candidate and the voting TAN on the voting client. So even if malware is installed on the client, it cannot identify the decision of the voter.

In this paper we will describe the code voting approach in detail and show that it is vulnerable against vote selling and denial of service attacks regarding the voting client. We then propose to improve code voting to deal with those vulnerabilities. Furthermore we combine code voting with vote updating and linkable group signatures. At last we describe the security properties of the new introduced approach.

2 Election Requirements

2.1 Security Requirements

In general voting systems used for (political) elections have to be free, universal, secret and equal. Much research has been done to adopt those requirements to remote online voting systems. Regarding Germany respectively Europe two important studies are the catalogue of requirements of the Physikalisch-Technische Bundesanstalt (PTB) [PTB04] and the recommendation of the Committee of Ministers of the Council of Europe [CoE04]. In 2006 Grimm et.al. analyzed those requirements and developed a protection profile for non-political elections according to the Common Criteria [GKM+06].

Summarized one can specify the following list of security requirements, which is not intended to be complete or comprehensive:

- Completeness and soundness of the Internet voting protocol(s),
- Correctness of the results
- Authenticity of both the voter (or the voting client acting on behalf of the voter, respectively) and the voting server,
- Secrecy of the ballots (including, for example, anonymity of the voter),
- Integrity of the ballots (including, for example, protection against malicious software)
- Non-duplication of the ballots,
- Availability and reliability of the voting process (including, for example, protection against denial of service attacks)

Even though single of those requirements are easy to fulfil, it is quite difficult to achieve all requirements concurrently, for some of them are contradictory. Furthermore appropriate cryptographic methods exist to deal with single requirements. E.g. to guarantee the secrecy of the ballot, one can use asymmetric encryption technologies. But as the encryption has to be computed on the voter's local client computer (in case of a remote online voting system), it is possible that malicious software forges the encryption process. As the local voting client is an important part of a remote online voting system and malware is an increasing problem on personal computers, it is difficult to ensure the client's security and integrity. As mentioned, therefore, in 2002 Ronald Rivest introduced the term "Secure Platform Problem" [Riv02]. We think that code voting, which we will describe in the next section is one (if not the only one) approach that works on a large scale.

2.2 Other requirements

Additionally to the security requirements there are further requirements, which a (electronic) voting system has to or should fulfil.

As mentioned above a political election has to be free, i.e. the voter must be able to vote for his favoured candidate without the fear of oppression or other disadvantages. The secrecy of the voter's ballot protects the freeness of his or her vote. Due to these facts a vote has to be anonymous, i.e. an attacker must not be able to correlate a (intercepted) ballot to a voter. Furthermore the voter must not be able, voluntary or nonvoluntary, to prove his vote to a third person to prevent vote selling or coercion of the voter. In the literature this property is named receipt-freeness.

Another relevant property of voting systems is the verifiability of the election process. In our democracy it is very important that the voter trusts this process and its result. This trust is often addicted to the possibility to check the election process in general and the calculation of the tally in particular. We distinguish between two kinds of verifiability, individual and universal verifiability. A voting system is individual verifiable, if the voter can check that his or her ballot has been computed in the tally correctly. Certainly the voter must be the only one, who can check his own vote. A voting system is universal verifiable, if it is individual verifiable and additionally all voters can check that the tally was calculated correctly. The particular challenge regarding individual and universal verifiability is not to compromise the receipt-freeness of the voting system.

3 The Secure Platform Problem

There is a simple attack against most of the remote voting systems proposed in the literature: If the attacker is able to control the communication channel between PC and voter, he can present the voting options in a different order, intercept the choice of the voter and redirect it to a voting option of his choice. This approach is similar to recent attacks on online banking systems [Gri03] [SW07] [LS07]. All cryptographic primitives employed can protect the voter's choice only from the point where it has been entered into the PC. There are two major options to solve this problem:

- Securing the PC against malware, e.g. by using Trusted Computing techniques.
- Using a separate channel from the voting authority to the voter, e.g. by snail mail, or by using a stand-alone security token.

We propose to use code voting [Cha01], where the separate channel is instantiated by snail mail. However, this scheme is vulnerable to vote selling attacks, so to be able to use this scheme in political elections, we have to add additional functionality. This additional functionality will be a linkable group signature scheme that is executed inside the untrusted PC. This may at first seem contradictory, but the adversary does not gain an advantage by manipulating the GS scheme, as long as the private key of the group member remains secret.

4 Code Voting

The term code voting was introduced in 2001 by David Chaum [Cha01]. Each eligible voter is issued a code sheet as shown in table 1.

| Candidate | Voting TAN |
|-----------|------------|
| Alice | 738747987 |
| Bob | 983293774 |
| Clark | 192851911 |
| ... | ... |

Table 1: Printed Code Sheet.

As with many remote online voting systems, the voter connects to the remote voting server, but instead of submitting the name of his or her favoured candidate the voter only enters the appropriate voting TAN, i.e. if a voter wants to vote for Bob he just enters 983293774 into the voting application. Using code voting we assume

- a trustworthy voting authority, which issues a valid code sheet to every eligible voter, and
- the according voting servers and databases to be reliable and secure.

With the two additional requirements

- all voting codes are random and unique for every code sheet and every candidate, and
- the code sheets must not be distributed by electronically means

we can consider code voting secure against active and passive attacks [HS07]. In a passive attack the adversary can read the submitted voting TAN. As this voting TAN is random and there is no correlation between the voting TAN and the chosen candidate, the best the attacker can do is guessing the vote. In an active attack the adversary not only can read, but also could modify or discard the submitted voting TAN. For the attacker neither knows the corresponding candidate nor can calculate a new voting TAN, the best he can do is guessing again. However, code voting is vulnerable to unnoticeable denial of service attacks, as the attacker could prevent the voting client from submitting the chosen voting TAN to the server either by simply discard the voting TAN or modifying the voting TAN, so that it is invalid. The voter has no possibility to discover that his vote wasn't delivered to the voting server. For this purpose a possible extension of the basic code sheet is to introduce a confirmation TAN, which is displayed after the voting TAN was delivered correctly to the voting server as shown in table 2.

| Voting TAN | Candidate | Confirmation TAN |
|-------------------|------------------|-------------------------|
| 738747987 | Alice | 332676873 |
| 983293774 | Bob | 676476488 |
| 192851911 | Clark | 301287123 |
| ... | ... | ... |

Table 2: Printed code sheet with confirmation TAN.

After the voter entered the voting TAN and it was successfully delivered to the voting server, the server responds with the confirmation TAN. This confirmation TAN is also random and unique for every code sheet and every candidate, so the voter has evidence, that his chosen voting TAN was delivered correctly to the voting server. However, one has to think about the voter's claiming possibilities in case of a faulty or missing confirmation TAN. With this solution one possible (averaging) attack is to prevent the voter from voting by means of a denial of service attack, i.e. the voter enters the chosen voting TAN, but malware on the client computer prevents from submitting the voting TAN to the voting server. Then the malware either answers with a random, faulty confirmation TAN or doesn't answer at all. We then can assume, that the voter would enter another voting TAN (in particular when vote updating is allowed) to check, if his code sheet is correct. Presumably, the voter would then enter a voting TAN corresponding to an outsider candidate, which the malware allows to pass. However, this problem that neither the sender nor the receiver of a TAN could know, if his message was delivered successfully, is comparable to the two army problem [AEH75][Gra78], which illustrates the problems and challenges of attempting to coordinate an action of two parties over an unreliable communication channel. However, though one can show that the two army problem has no solution, often as a solution approach a three-way handshake is used, as e.g. used in TCP. According to this approach we propose a 3-step scheme by adding a third TAN, the finalization TAN (see table 3). The voting server only counts the vote, if the finalization TAN has been entered by the voter. With the attack described above, one can assume that the voter wouldn't enter the finalization TAN, if he or she doesn't receive the correct confirmation TAN.

| Voting TAN | Candidate | Confirmation TAN | Finalization TAN |
|-------------------|------------------|-------------------------|-------------------------|
| 738747987 | Alice | 332676873 | 442367810 |
| 983293774 | Bob | 676476488 | 123456789 |
| 192851911 | Clark | 301287123 | 520172861 |
| ... | ... | ... | ... |

Table 3: Printed code sheet with confirmation and finalization TAN.

5 Vote Selling

However, even with a finalization TAN, code voting is vulnerable to vote selling, as the voter could simply sell the code sheet or a scanned copy thereof to an attacker. Even if vote updating is allowed and the vote seller tries to update his or her vote, he or she is racing with the vote buyer, and the vote buyer can arrange to be almost certain to win the race, since the vote buyer can re-perform the update as many times as needed. We have to assume that the vote buyer probably has more resources and patience than the vote seller, and, for instance, can automate the process of repeatedly sending updates.

In the following sections we will improve code voting with group signatures and vote updating to deal with vote selling.

6 Code Voting With Linkable Group Signatures

6.1 Group Signatures

In 1991 Chaum and van Heyst presented the concept of a group signature scheme [CH91]. A group signature is used to allow every member of a group sign messages on the group's behalf. In most cases those signatures are anonymous, i.e. it is not possible to identify which member of the group has signed a particular message. In addition, one cannot check if two signed messages were signed by the same group member. However, only a designated group manager exists who manages the membership list of the group and who can reveal the identity of the signer of a message.

6.2 Procedures in Group Signature Schemes

The group signature setting comprises three parties, namely the group manager M , the group members u_i and one or more verifiers w_j . In a group signature scheme, these parties participate in several polynomial-time algorithms (Fig. 1)⁵⁰:

- **GMKEY**: a probabilistic algorithm that generates the private keys isk (issuing key) and opk (opening key) for M together with a group public key gpk .
- **GUKEY**: a probabilistic key generation algorithm that provides each user u_i with a public key pair (upk_i, usk_i) . The key upk_i is also referred to as membership key or pseudonym and should only be known to u_i and M .
- **JOIN**: an interactive algorithm in which M computes a membership certificate v_i on upk for user u_i using isk . Using v_i , u_i can prove to any verifier w_j that he is a member of the group administered by M .

⁵⁰ We here omit the JUDGE procedure, assuming that each identity determined by the OPEN algorithm is accompanied with a proof of that fact.

- SIGN: a probabilistic algorithm in which u_i generates a signature s on an arbitrary message m using a membership certificate v_i and a secret key usk_i . Essentially, for a group signature scheme, no party can learn from s which v_i was used to generate it nor determine if any two signatures s and s' have been generated by the same group user.
- VERIFY: given gpk , m , and s a verifier w_j can use this deterministic algorithm to determine if a received signature s has actually been signed by a group member.
- OPEN: given opk and a message m with a corresponding group signature s , this deterministic algorithm can identify the originator of s .

A secure group signature scheme must guarantee the following (informal) security properties⁵¹ [ACJT00]:

- Correctness: A group signature s , which has been correctly generated by a group user, is always accepted by a verifier.
- Unforgeability: only group users can generate valid group signatures.
- Anonymity: no one (except M) can learn the identity of the originator of a valid group signature.
- Unlinkability: no one (except M) can decide whether two signatures have been issued by the same user.
- Traceability: the group manager M can associate all valid group signatures with their originator.
- Coalition-resistance: a set C of malicious group users cannot work together to successfully create valid group signatures, which are associated to a user u_i who is not a member of C .

In [BSZ05] the security requirements of group signature schemes are reduced to just four basic properties (including correctness). Each property is then formalized in an attack experiment. Accordingly, a group signature scheme is called secure with respect to a certain security property if no polynomial-time attacker can win the corresponding experiment with a non-negligible probability.

⁵¹ We remark that some authors even consider further security properties.

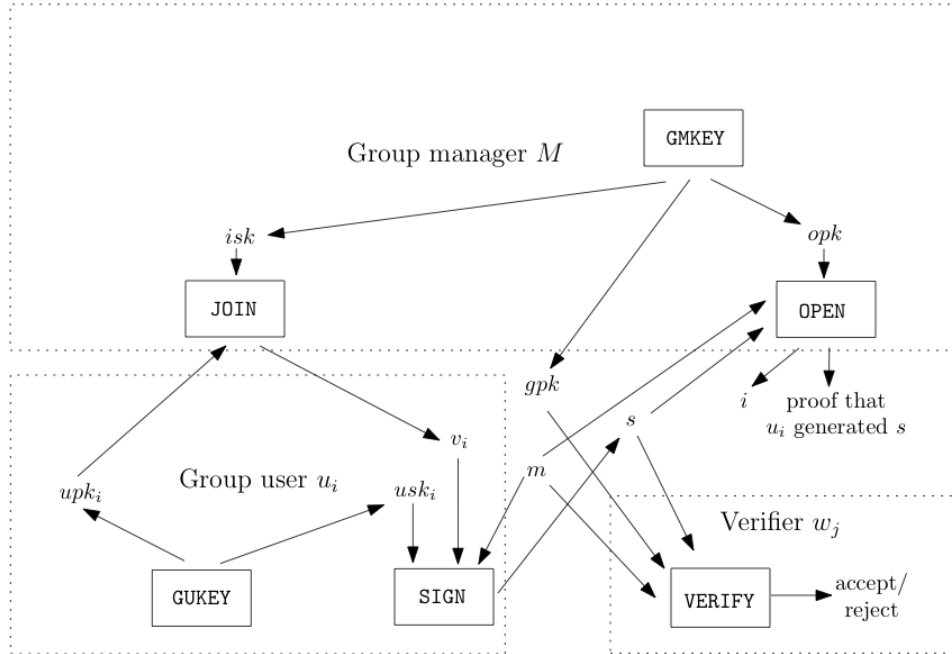


Figure 1: Group signature scheme. *gpk*: group public key; *isk*: (private) issuing key; *opk*: (private) opening key; *usk_i*: (private) user key; *upk_i*: membership key; *m*: message to be signed; *v_i*: membership certificate; *s*: group signature on *m*; *i*: user identity

6.3 Signatures of Knowledge

Signatures of knowledge are among the most important building blocks for group signature schemes. They are based on zero-knowledge protocols in which a prover can convince a verifier that he possesses a certain secret without revealing any information on that secret. Basically, usual 3-move zero-knowledge proofs of knowledge are made non-interactive using the Fiat-Shamir heuristic by replacing the verifier in the first two protocol steps with a hash function. Accordingly, the output of the hash function is interpreted as one or more challenges for the prover. The input to the hash function consists of the random commitments of the prover along with additional public information. In a signature of knowledge, these values are concatenated with the message to be signed. Signatures of knowledge can be proven secure in the random-oracle model. As a result, a signature of knowledge convinces a verifier that its issuer knows a certain secret while at the same time not revealing any information on that secret. Similar to [CS97] we denote signatures of knowledge rather descriptive than technical. According to this, a signature of knowledge of the fact that the issuer knows, for example, the discrete logarithms of y to the base g is denoted as:

$$SK\{(\alpha) : y = g^\alpha\}(m).$$

Such signatures of knowledge can easily be constructed using Schnorr signatures [Sch91]:

Let $H: \{0,1\}^* \rightarrow \{0,1\}^k$ be a collision-resistant hash function with a k -bit output and $G = \langle g \rangle = \langle h \rangle$ be a cyclic group of prime order p . Then, a signature of knowledge of the above fact is a pair

$$(c, d) \text{ in } \{0,1\}^k \times Z_p^*$$

satisfying

$$c = H(m || v || g || g^d y^c).$$

Signatures of knowledge can also be used to prove more complex statements about secrets, like

$$SK\{(\alpha, \beta): y = g^\alpha \text{ and } z = h^\beta\}(m)$$

$$SK\{(\alpha, \beta): y = g^\alpha \text{ or } z = h^\beta\}(m)$$

$$SK\{\alpha): y = g^\alpha \text{ and } \alpha \text{ is in } [A, B]\}(m).$$

The security properties of signatures of knowledge make them suitable for the design of SIGN algorithms. To show that he is a group user of M 's group, u_i has to prove that he (i) possesses a group membership certificate y_i issued by M and (ii) that he knows the private key usk_i corresponding to the public key upk_i certified in v_i . By showing his membership certificate or his membership key directly to a verifier, the user would make his signatures linkable. Using signatures of knowledge u_i can show possession of both values without actually revealing them. Essentially, u_i exploits that signatures of knowledge can be randomized (just like interactive zero-knowledge proofs of knowledge) by the prover. The group user only has to choose a new random commitment (corresponding to the first protocol move in an interactive zero-knowledge proof) every time he issues a group signature. In this way u_i can guarantee that no two signatures are equal, thus making the group signature scheme unlinkable.

6.4 Linkable Group Signatures

In 1997 Camenish and Stadler introduced the first efficient group signature scheme. Using this group signature scheme the length of the public key is independent from the size of the group. Even if a new member joins the group it is not necessary to calculate a new public key. Furthermore, in this scheme it is possible to assign the two different roles of the group manager (issuer of membership certificates and opener of group signatures) to different parties, which is a very desirable property regarding electronic voting systems. Since then, a large number of group signature schemes have been proposed [GW07]. We will show how to change such schemes to linkable GS schemes using the high-level description from [CS97]. Our starting point is to force each group user not to randomize his signatures of knowledge:

- The group manager M computes a key pair $(\text{sig}_M, \text{ver}_M)$ of a digital signature scheme, and a public key encryption key pair $(\text{enc}_M, \text{dec}_M)$, and publishes the two public keys.
- Alice joins the group by choosing a random value x , sending her membership key $z=f(x)$ (f a one-way function) in an authenticated way to M , and receiving in return her membership certificate $v=\text{sig}_M(z)$.
- Alice signs a message m by encrypting (m,z) using the group managers encryption key, i.e. $d=\text{enc}_M(m,z)$. (Note: We omit the random number here to make the GS linkable.) She computes a signature of knowledge that she knows the values x' and v' satisfying the following equations: $d=\text{enc}_M(m,f(x'))$ and $\text{ver}_M(v',f(x'))=\text{true}$.

To protect the private key (x,z,v) against the attacker controlling the PC, this key can e.g. be bound to a TPM chip (which is much easier than to secure the whole platform using TPM technology), or it can be stored on a smart card (e.g. an electronic passport).

6.5 Vote Updating

To prevent vote selling in some voting systems, vote updating is used. That is, the voter could cast his or her ballot as often as he or she wants to, but only the last cast ballot is computed in the tally. The basic idea is that even if a voter sells his ballot to an attacker, he could easily update his or her vote. Hence the vote buyer never can be sure that the vote seller will not update his vote, after he has proven his choice to the vote buyer. E.g. the Estonian voting system, which was employed for the first political election over the Internet, uses vote updating [Est05]. Besides the advantages some disadvantages also exist. These advantages and disadvantages that are also different types of vote updating, are not further addressed in this paper, but are analyzed and discussed in [VG06]. However, we think that vote updating is a good method to prevent vote selling, but cannot be the only measure and therefore has to be facilitated by other measures [OSH08]. In this paper we will use vote updating as a part of a measure against vote selling, independent from the type of implementation of vote updating.

6.6 Improved Voting Scheme

To deal with vote selling and the secure platform problem, we propose to improve code voting. We assume a trustworthy voting authority, which consists of representatives of all parties that are supervising each other⁵². We further assume a group signature scheme as described in section 6.4. The voting authority is divided into different groups, which are responsible for the following tasks:

- Printing and issuing the code sheets to the eligible voters.

⁵² In the literature, this property is called Separation of Duties.

- Operating the voting servers and the according databases, which we assume to be reliable and secure.
- Managing the group signature scheme by issuing the private keys to the eligible voters.
- Managing the group signature scheme by opening the signed voting TANs, i.e. verifying that every eligible voter only casts one ballot.

Each member of the voting authority should only belong to one of those groups.

The improved voting scheme works as follows: Prior to the election, each eligible voter is issued a private key according to the group signature scheme. Additionally, in a second step, the voting authority prints code sheets as seen in table 3. We assume that for every voter and every candidate the voting TANs, the confirmation TANs and the finalization TANs are randomly chosen using a good PRNG algorithm. Since the printing procedure links the voting TANs to the candidates, this process has to be monitored not only by the members of the code sheet issuing group, but by all voting authority members. For that purpose the different parties and their representatives in the voting authority then can check a control sample if the correlation between voting TAN and candidate is correct for the valid code sheets.

In a third step the valid code sheets are shuffled, put into anonymous envelopes and then they are distributed to the eligible voters. After the election has been started the voter connects to the voting server and enters the voting TAN for the desired candidate into the voting software and signs it with his private key according to the linkable group signature scheme. This signature could include information about e.g. the electoral district. The signed voting TAN is sent to the voting server over a MIX net. After the voting server has answered with the correct confirmation TAN, the voter approves his vote with the (signed) finalization TAN. In the improved code voting scheme we allow vote updating, i.e. every voter could submit several valid voting TANs to the voting server, but only the last submitted voting TAN approved with the corresponding finalization TAN counts in the tally. With the aid of the group signature, the responsible group of the voting authority ensures that a single voter can cast only one valid voting TAN regardless of how many code sheets he may have bought.

Therefore, this voting authority group opens the group signature to check if the voter already cast a ballot⁵³. The finalized voting TAN is stored in the database, where older required voting TANs will be removed. If the voter gets either no or a faulty confirmation TAN, the client may be infected with malicious software, and he may vote again using another voting client, if the group signature scheme is transferable⁵⁴.

⁵³ For further research it would be interesting to analyze if threshold schemes could be applied in conjunction with the linkable group signature scheme, so that m out of n group managers are needed to open a signature.

⁵⁴ This is e.g. the case if the private key is stored on a smart card.

It is an open question whether at the end of the election the voting authority should publish the submitted voting TANs: since they are checkable also by a coercer, even if vote selling is impossible, the adversary may control the voting decision of certain voters.

7 Security Properties

A passive adversary is only able to attack the secrecy of an election. He can observe the TANs entered into the web browser. Since those TANs were chosen at random, the best an attacker can do is guess the vote. Additionally, in our voting scheme the voter sends his signed voting TAN to the server. As his or her vote is sent over a MIX net, an allocation between IP address and the submitted voting TAN is not possible. Even though malware on the voting client could just read the voting TAN, it cannot identify the chosen candidate. So our voting scheme is secret.

Further, our voting scheme is equal because the group signature is linkable by the group managers, i.e. for every eligible voter only one signed voting TAN is counted in the tally. If the voting scheme doesn't publish the submitted voting TANs, the proposed voting scheme is receipt free, but it is not verifiable. Because our voting scheme uses linkable group signatures, a vote buyer can only cast as many ballots as he has different group signature keys. For that purpose, the group managers have to issue a private key, which a voter presumably would not give to an attacker, e.g. a private key according to an ePass.

8 Summary

In this paper we proposed to use code voting as a reasonable measure against the “Secure Platform Problem” that is a major threat to most of the proposed electronic voting schemes. As the code voting model is vulnerable against vote selling, we extended code voting using vote updating and linkable group signatures to prevent vote selling attacks regarding the voting client and described some security properties of the new approach.

References

- [ACJT00] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. In *Advances in Cryptology – CRYPTO 2000*, vol. 1880 of *Lecture Notes in Computer Science*, pages 255–270. Springer 2000.
- [AEH75] E. A. Akkoyunlu, K. Ekanadham, and R. V. Huber. Some Constraints and Tradeoffs in the Design of Network Communications. In *ACM SIGOPS Operating Systems Review*, volume 9, pages 67–74, 1975.
- [BSZ05] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of Group Signatures: The Case of Dynamic Groups. In *Topics in Cryptology - CT-RSA 2005*, volume 3376 of *Lecture Notes in Computer Science*, pages 136–153. Springer-Verlag, 2005.
- [Cha01] D. Chaum. Sure Vote: Technical Overview. In *Proceedings of the workshop on trustworthy elections (WOTE '01)*, <http://www.vote.caltech.edu/wote01/pdfs/surevote.pdf>, 2001.

- [CS97] J. Camenisch and M. Stadler. Efficient Group Signature Schemes for Large Groups. In *Advances in Cryptology - CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 410–424. Springer-Verlag, 1997.
- [CvH91] D. Chaum and E. van Heyst. Group signatures. In *Advances in Cryptology – EUROCRYPT'91*, volume 547 of *Lecture Notes in Computer Science*, pages 257–265. Springer-Verlag, 1991.
- [Cyb05] Cybernetica. General description of the estonian e-voting system, online available under <http://www.cyber.ee/english/services/eGovernment/evoting.html>, 2005.
- [GKM+06] R. Grimm, R. Krimmer, N. Meißner, K. Reinhard, M. Volkamer, M. Weinand, and J. Helbach. Security Requirements for Non-political Internet Voting. In *Proceedings of the 2nd International Workshop on Electronic Voting 2006*, volume 86 of *Lecture Notes in Informatics*, pages 203–212, 2006.
- [Gra78] Jim Gray. Notes on Data Base Operating Systems. In *Lecture Notes in Computer Science*, volume 60, pages 393–418, 1978.
- [Gri03] Roger A. Grimes. An SSL trojan unmasked. <http://www.infoworld.com/article/06/03/03/75970\100Psecadvise\1.html>, 2003.
- [HMR04] Volker Hartmann, Nils Meißner, and Dieter Richter. Online Voting Systems for Nonparliamentary Elections – Catalogue of Requirements. Technical Report PTB-8.5-2004-1, online available under http://www.berlin.ptb.de/8/85/LB8_5_2004_1AnfKat.pdf, Physikalisch-Technische Bundesanstalt, April 2004.
- [HS07] Jörg Helbach and Jörg Schwenk. Secure Internet Voting with Code Sheets. In *EVoting and Identity, First International Conference, VOTE-ID E-Voting and Identity, First International Conference, VOTE-ID*, pages 166–177, 2007.
- [LS07] H. Langweg and J. Schwenk. Schutz von FinTS/HBCI-Clients gegen über Malware. In *Proceedings of D-A-CH Security*, pages 227–238, 2007.
- [oE04] Council of Europe. Legal, operational and technical standards for e-voting. http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/02_e-voting/01_Recommendation/Rec%282004%2911_Eng_Evoting_and_Expl_Memo.pdf, 2004.
- [Opp02] R. Oppliger. How to Address the Secure Platform Problem for Remote Internet Voting. In *Proceedings of the 5th Conference Security in Information Systems (SIS 2002)*, pages 153–173, http://www.ifi.unizh.ch/~oppliger/Docs/sis_2002.pdf, 2002. vdf Hochschulverlag.
- [OSH08] R. Oppliger, J. Schwenk, and J. Helbach. Protecting Code Voting Against Vote Selling. In *SICHERHEIT 2008 - Sicherheit, Schutz und Zuverlässigkeit*, volume 128 of *Lecture Notes in Informatics*, pages 193–204, 2008.
- [Riv02] R. Rivest. Electronic voting. In *Financial Cryptography '02*, volume 2339 of *Lecture Notes in Computer Science*, pages 243–268. Springer-Verlag, 2002.
- [Sch91] C. P. Schnorr. Efficient Signature Generation by Smart Cards. In *Journal of Cryptology*, volume 4, pages 161–174. Springer-Verlag, 1991.
- [SW007] Secure Works: Win32.Grams E-Gold Account Siphoner Analysis. <http://www.secureworks.com/research/threats/grams/>, 2007.
- [VG06] M. Volkamer and R. Grimm. Multiple Casts in Online Voting: Analyzing Chances. In *Proceedings of the 2nd International Workshop on Electronic Voting 2006*, volume 86 of *Lecture Notes in Informatics*, pages 97–106, 2006.
- [Wan07] Guilin Wang. Bibliography on Group Signatures, <http://icsd.i2r.a-star.edu.sg/staff/guilin/bible/group-sign.htm>, 2007.
- [Web07] T. Weber. Criminals may overwhelm the web, <http://news.bbc.co.uk/1/hi/business/6298641.stm>, 2007.

CAPTCHA-based Code Voting

Rolf Oppliger¹, Jörg Schwenk², Christoph Löhr²

¹eSECURITY Technologies
CH-3073 Gümligen
rolf.oppliger@esecurity.ch

²Ruhr-University Bochum
D-44780 Bochum
{joerg.schwenk|christoph.loehr}@rub.de

Abstract: Code voting provides an appropriate technology to address the secure platform problem of remote Internet voting, but it is not particularly user-friendly. In this paper, we propose the use of CAPTCHA- an acronym standing for Completely Automated Public Turing tests to tell Computers and Humans Apart - to improve the user-friendliness of code voting, discuss the security of CAPTCHA-based code voting, and elaborate on a possible implementation.

1 Introduction

Elections and votes are fundamental processes for the proper operation of democratic states and their (democratically legitimated) governments. In the literature, the term *electronic voting* (or *e-voting* in short) is used to refer to elections and votes that are supported by electronic means. With the proliferation of the Internet, its use for e-voting has been proposed by many people (mainly politicians) as a way to make voting more convenient and as it is hoped to increase participation in elections and votes. The term *Internet voting* is therefore used to refer to election or voting processes that enable voters to cast their ballots over the Internet. This basically means that the ballots must be represented electronically, and that the electronic ballots must be transmitted to election officials using the Internet as a transport medium.

There are many possibilities to implement Internet voting, and poll-site Internet voting, Kiosk voting, and remote Internet voting are usually distinguished in the literature (e.g., [Cal00]). In this paper, we only focus on remote Internet voting, i.e., Internet voting where the voter (or a third party acting on behalf of the voter) uses his personal computer (PC) to cast a ballot over the Internet. From a security viewpoint, remote Internet voting is the most challenging possibility to implement Internet voting. In states that support absentee balloting, such as all-postal voting, any other form of Internet voting (i.e., poll-site Internet voting and Kiosk voting) is likely to fail. This is because the other possibilities require the voter to visit a voting place, and this is probably too inconvenient compared to the simplicity of casting ballots from home. In Europe, for example, a few states have started to employ remote Internet voting in geographically restricted pilot projects, such as in three cantons of Switzerland [Ber08], or for official use, such as in Estland.

Against this background, it is possible and likely that the use of remote Internet voting tends upwards, and that the security of remote Internet voting will become a major issue. Security, in turn, has many aspects, and there are several partly complementary security technologies, mechanisms, and services that can be used to address them. As argued in [Opp02], code voting, i.e., voting by providing randomly-looking codes instead of YES or NO in the case of a vote and candidates' names in the case of an election, is an appropriate technology to address the secure platform problem of remote Internet voting. Unfortunately, code voting is not particularly user-friendly, and in this paper we explore possibilities to use *Completely Automated Public Turing tests to tell Computers and Humans Apart* (CAPTCHAs) also known as *Reverse Turing Tests* (RTTs) or *Human Interactive Proofs* (HIPs) to improve the user-friendliness of code voting. We think that CAPTCHA-based code voting provides an interesting possibility to implement code voting in a real-world setting.

The rest of the paper is organized as follows: The security requirements of (remote) Internet voting are summarized in Section 2. Code voting and CAPTCHA-based code voting are introduced and discussed in Sections 3 and 4. A preliminary security analysis is given in Section 5. Finally, conclusions are drawn and an outlook is given in Section 6.

2 Security Requirements

There are many investigations and studies that elaborate on the security of Internet voting in general, and remote Internet voting in particular (e.g., [Cal00, Rub01]). The results all give evidence that security (including privacy and reliability) is among the most important preconditions for the successful deployment of Internet voting. The current paper ballot systems set a standard that is adopted as a security baseline for Internet voting. They represent certain tradeoffs between voter convenience and protection against fraud and abuse. It is generally required that elections and votes conducted over the Internet are at least as secure as the current paper ballot systems. In states that support absentee balloting in the form of all-postal voting, however, it is this voting technology that sets the security standard for Internet voting.

There are many lists of security requirements for (remote) Internet voting that can be found in the literature⁵⁵. There is even an e-voting protection profile for the Common Criteria drafted in Germany⁵⁶. The following list of security requirements is not intended to be complete or comprehensive:

- Completeness and soundness of the Internet voting protocol(s);
- Correctness of the results;
- Authenticity of both the voter (or the voting client acting on behalf of the voter, respectively) and the voting server;
- Secrecy of the ballots (including, for example, anonymity of the voter);
- Integrity of the ballots (including, for example, protection against malicious software);
- Non-duplication of the ballots;
- Availability and reliability of the voting process (including, for example, protection against denial-of-service attacks).

Some security requirements are complementary and don't interact with each other (e.g., integrity and non-duplication of the ballots). Other security requirements, however, are (or at least seem to be) contradictory in some sense. For example, one way to attest the correctness of a voting process is auditability, meaning that the entire voting process can be audited in some reasonable way. Auditability, however, sometimes contradicts to the secrecy of the ballots. In fact, there is a lot of research going on in the cryptographic community to address this apparent contradiction and to guarantee ballot secrecy and the correctness of the results simultaneously. Most of this research elaborates on schemes and protocols for verifiable secret sharing and secure multi-party computation as pioneered by Yao [Yao82].

⁵⁵ In 2004, for example, the Committee of Ministers of the Council of Europe adopted Recommendation Rec(2004)11 that specifies "legal, operational and technical standards for e-voting." These standards, among other things, also comprise security requirements.

⁵⁶ <http://www2.dfki.de/fuse>

Many security requirements of (remote) Internet voting can be addressed with existing technologies, mechanisms, and services. For example, there are many technologies that can be used to secure the server side. Examples include firewall technologies and intrusion detection systems (IDS) or intrusion prevention systems (IPS). The authenticity of the voter and the voting server can be addressed with public key certificates. Similarly, the secrecy and integrity of the ballots can be guaranteed with a cryptographic protocol, such as the Secure Sockets Layer (SSL) [FKK96] or Transport Layer Security (TLS) [DR06] protocol. It is, however, important to note that the use of the SSL/TLS protocol protects the secrecy and integrity of the ballots only during the transmission over the Internet. The ballots are not automatically protected on the client or server side. In fact, additional security technologies, mechanisms, and services are required to protect the secrecy and integrity of the ballots before and after they are transmitted over the Internet. There are additional risks for the secrecy of the ballots (i.e., privacy risks) related to the use of spyware (in the home setting) or remote system administration tools (in the institutional setting).

Due to the fact that a remote Internet voter uses his PC to cast a ballot and that this PC may be subject to malware, the insecurity of the client-side platform represents the major vulnerability (and Achilles heel) of remote Internet voting. Rivest coined the term *secure platform problem* to refer to the problem of protecting an inherently insecure client-side platform against malicious software and corresponding attacks [Riv01].

Due to the fact that the *secure platform problem* is hard and difficult to solve, there are several e-voting research and development projects that don't even address it. For example, in the FAQ document of the European CyberVote project⁵⁷, the question “Can a virus or Trojan horse attack CyberVote?” is answered in the following way:

“Yes, like any other client software in an insecure PC environment.

Anti-virus software should be used and strict security guidelines followed to limit the risk of a virus or Trojan horse attack.

Secure user interface techniques can be applied to the CyberVote client to prevent Trojan horses.”

Unfortunately, the FAQ document does not further explain the term “secure user interface techniques.” It turns out that there are not many security technologies, mechanisms, and services that can be used to effectively address the secure platform problem of remote Internet voting. In fact, we think that code voting as introduced next is one (if not the only) technology that may work in a real-world setting.

⁵⁷ http://www.eucybervote.org/faq_security.html#q35

3 Code Voting

The term *code voting* is used to refer to an e-voting technology in which the voter casts his ballot by providing a voting code instead of YES or NO (in the case of a vote) or a candidate's name (in the case of an election). The voting code, in turn, looks like a random string. If the alphabet consists of all decimal digits 0...9, then the voting code basically represents a number. In general, however, any alphabet can be used and the voting codes can be arbitrarily long.

To the best of our knowledge, the first code voting system was proposed by Chaum [Cha01]. In such a system, each voter is equipped with a code sheet (i.e., a sheet that itemizes all voting codes) and he must enter the appropriate voting codes to cast his ballot. An exemplary code sheet for an election is illustrated in Table 1. If the voter wants to vote for Bob, then he must enter 990234 (instead of “Bob”).

| Candidate | Voting code |
|-----------|-------------|
| Alice | 236412 |
| Bob | 990234 |
| Carol | 141290 |
| Dave | 782755 |
| Eve | 774892 |
| ... | ... |

Table 1: A code sheet with voting codes

Due to the fact that voting codes look like random strings, code voting effectively protects against passive and active attacks:

- In a passive attack, the adversary sees a voting code sent over a network (using, for example, a network management or system administration tool), and must then be able to tell whether this code represents YES or NO (in the case of a vote) or to which candidate the code actually refers to (in the case of an election). If the voting codes are chosen with a good random bit generator or a cryptographically secure pseudorandom bit generator (PRBG), then the best the adversary can do is guessing. In this case, seeing the voting codes sent over the network does not help the adversary.
- In an active attack, the adversary does not only see a voting code sent over a network, but he can also manipulate it. For example, the adversary may employ malware or a client-side remote system administration tool to turn a voting code representing YES into a voting code representing NO (in the case of a vote) or a voting code of one candidate into a voting code of another candidate (in the case of an election). Again, if the voting codes are chosen with a good random bit generator or a cryptographically secure PRBG, then the adversary does not know the other voting codes, and hence the best he can do is again guessing.

In either case, the success probability of an adversary is not better than guessing, meaning that the best an adversary can do is guessing. This is independent from the adversary's computational resources and available time. Consequently, the security that is achieved is unconditional or information-theoretic. There are, however, two conditions that must be fulfilled to achieve this level of security:

- As mentioned before, the voting codes must be random, i.e., they must be chosen with a good random bit generator or a cryptographically secure PRBG;
- The code sheets must be personal and distributed out-of-band⁵⁸, using, for example, a trustworthy postal mail delivery service.

Also, it is important to note that code voting requires a modified voting behavior, and that there may be some legal constraints to consider (not addressed in this paper).

In spite of the fact that code voting as discussed so far is able to provide unconditional or information-theoretic security, it may still be the case that an (active) adversary simply deletes a voting code in transit. To protect against this attack, it may be worthwhile to have the server send back a verification code and have the voter verify this code.

Table 2 illustrates an exemplary code sheet with voting and verification codes. Again, if the voter wants to vote for Bob, then he must enter 990234 and wait for the server to send back the verification code 672345. If another verification code is sent back, then something illegitimate is going on and the voter is well advised to stop voting (needless to say that some dispute-resolving mechanisms must also be put in place here).

| Candidate | Voting code | Verification code |
|-----------|-------------|-------------------|
| Alice | 236412 | 124355 |
| Bob | 990234 | 672345 |
| Carol | 141290 | 045686 |
| Dave | 782755 | 687432 |
| Eve | 774892 | 234115 |
| ... | ... | ... |

Table 2: A code sheet with voting and verification codes

If the voter verifies the verification code, then it makes a lot of sense to communicate the result of the verification step to the server (otherwise, the server does not know whether the result is correct). This is where the confirmation code comes into place. Table 3 illustrates an exemplary code sheet with voting, verification, and confirmation codes. In our toy example, the voter would confirm the successful verification of the verification code 672345 by sending the confirmation code 574546 to the server. At this point, there is no need to continue the recursion (and send more codes back and forth).

⁵⁸ It is important that the code sheets must be provided outside the voter's PC (i.e., the PC that is used by the voter to cast his vote). If the code sheets were inside the PC, then malicious software could get and use them to change the ballots. Also, the voting codes must be randomly or pseudo-randomly chosen from a sufficiently large set of possible values to make the probability that malicious software can correctly guess them sufficiently small (i.e., negligible).

| Candidate | Voting code | Verification code | Confirmation code |
|-----------|-------------|-------------------|-------------------|
| Alice | 236412 | 124355 | 252435 |
| Bob | 990234 | 672345 | 574546 |
| Carol | 141290 | 045686 | 124145 |
| Dave | 782755 | 687432 | 243521 |
| Eve | 774892 | 234115 | 967468 |
| ... | ... | ... | ... |

Table 3: A code sheet with voting, verification, and confirmation codes

The bottom line is that there are many possibilities to implement code voting. In addition to casting a vote by simply entering a voting code, the voter may verify a verification code sent back from the server (to verify that he has casted the vote to an authentic server, and that the vote has been properly registered by the server). Also, the voter may acknowledge proper verification of the verification code by sending out a confirmation code.

In Table 4, we summarize the $2^3-1=7$ possibilities to implement code voting. Among these possibilities, we think that the following four possibilities are meaningful in practice:

- Voting code-only implementation;
- Verification code-only implementation;
- Voting and verification code implementation;
- Full implementation (i.e., voting, verification, and confirmation codes).

| Possibilities | Voting code | Verification code | Confirmation code |
|---|-------------|-------------------|-------------------|
| Voting code-only implementation | X | | |
| Verification code-only implementation | | X | |
| Voting and verification code implementation | X | X | |
| | X | | X |
| | | X | X |
| Full implementation | X | X | X |

Table 4: Possibilities to implement code voting

In a voting code-only implementation, the voter casts his ballot by simply sending a voting code to the server. In a verification code-only implementation, the voter casts his ballot as usual, but waits for a verification code sent back from the server. It is then up to the voter to verify this code. A verification code-only implementation is particularly interesting, because the voter has to minimally change his behaviour (i.e., he can still enter YES or NO and only validate the verification number sent back from the server). This advantage, however, may also be disadvantageous, because it is possible and likely that some voters don't care about the validity of verification codes sent back. As its name suggests, a voting and verification code implementation employs voting and verification codes. Last but not least, a full implementation employs voting, verification, and confirmation codes. It goes without saying that this is the preferred choice from a security viewpoint, and that all other choices represent tradeoffs.

A practically relevant question refers to the length of the various codes. Obviously, the length must make the probability to correctly guess a code sufficiently small. For example, if the number includes 10 binary digits (bits), then the probability of correctly guessing a code is $1/2^{10} = 1/1,024 = 0.000975562$. Due to the fact that the numbers cannot be verified off-line (without access to the code sheets), this seems to be sufficient. 10 bits can be represented with $\log_2 2^{10} = \log_{10} 1,024$ decimal digits which is slightly more than 3 digits. Consequently, 4 decimal digits can be used to encode a code and some redundancy to detect errors (error detection is particularly important for voting and confirmation codes that are entered by the user).

In theory, 10-bit code numbers can be randomly generated, using a random bit generator. In practice, however, the code numbers are more likely generated with an appropriately seeded pseudorandom bit generator (PRBG) or a construction that employs a keyed hash function, such as the HMAC construction [KBC97]. In either case, the generation of the code numbers is not further addressed in this paper.

Last but not least, we note that a guessing attack may have an equalizing effect on the outcome of an election or vote. If, for example, a candidate only gets a few votes under "normal" circumstances, then he may get an average number of votes under a guessing attack. This is because it is equally likely to guess a voting code for an unpopular candidate as it is to guess a voting code for a popular candidate. Hence, the outcome of an election or vote that is subject to a guessing attack may be equalized to some extent. Because we do not further address guessing attacks, this point is not further discussed in this paper.

4 CAPTCHA-based Code Voting

The potential difficulty of differentiating humans from computers pretending to be humans was addressed already in 1950, when Turing described his now-famous test. In short, the *Turing test* is a proposed test for a machine to demonstrate intelligence [Tur50]. It proceeds as follows: a human judge engages in a natural language conversation with one human and one machine, each of which are trying to appear human. If the judge cannot reliably tell which is which, then the machine is said to pass the Turing test. In order to keep the test setting simple and universal (to explicitly test the linguistic capability of the machine instead of its ability to render words into audio), the conversation is usually limited to a text-only channel such as a teletype machine as Turing suggested, or, more recently, Internet-based messaging.

In the mid-1990s, people came up with the idea of using a reverse Turing test to have a machine test whether a user is human. For example, in 1995, Lam of The Chinese University of Hong Kong implemented a reverse Turing test in a voting application written for Radio Television Hong Kong. The public was able to vote for their favourite singers and songs online for the first time in the annual “Top Ten Chinese Songs Award.” To prevent automatic and machined submissions, users were required to correctly input a 6-digit number that was represented as an image. In 1996, the first reference of automated tests, which distinguish humans from computers for the purpose of controlling access to Web services, appeared in a manuscript of Naor [Nao96]. Other primitive reverse Turing tests seem to have been developed in 1997 at AltaVista to prevent bots from adding URLs to their search engine.

In 2000, von Ahn and Blum developed and publicized the notion of a *Completely Automated Public Turing test to tell Computers and Humans Apart* (CAPTCHA), which included any program that can distinguish humans from computers. They invented multiple examples of CAPTCHAs, including the first CAPTCHAs to be widely used on the Internet (at Yahoo!) [vABL04]. The acronym CAPTCHA is trademarked by Carnegie Mellon University. Alternatively, a CAPTCHA is sometimes called *Reverse Turing Test* (RTT) or *Human Interactive Proof* (HIP).

In general, there are many possibilities to implement CAPTCHAs, RTTs, or HIPs. A common type of (visual) CAPTCHAs requires that the user type in the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. Such CAPTCHAs are also used in this paper (as an example). But there are many other visual CAPTCHAs and CAPTCHAs based on audio or video. More recently, for example, Microsoft Research has come up with a HIP called ASIRRA (Animal Species Image Recognition for Restricting Access) that works by asking users to distinguish between photographs of cats and dogs [E+07]. Audio CAPTCHAs, in turn, have been developed and are being deployed for handicapped persons. In essence, any task that can be efficiently solved by a human but is not known to be efficiently solvable by a machine can be turned into a CAPTCHA, RTT, or HIP. There are many opportunities for research and development here.

In CAPTCHA-based code voting, the voter does not cast his ballot directly by providing an appropriate voting code, but indirectly by clicking on an appropriate CAPTCHA. Clicking on a CAPTCHA, in turn, causes a random-looking voting code (representing a cryptographic hash value) to be sent from the browser to the server. Let us consider an exemplary (and simplified) election in Germany, in which the voter can select between five political parties. If, for example, a voter visits <http://wahlen.nds.rub.de>, then the voting server sends back a dynamically generated Web page in which the parties' acronyms are rendered as CAPTCHAs and visually presented to the voter in random order.

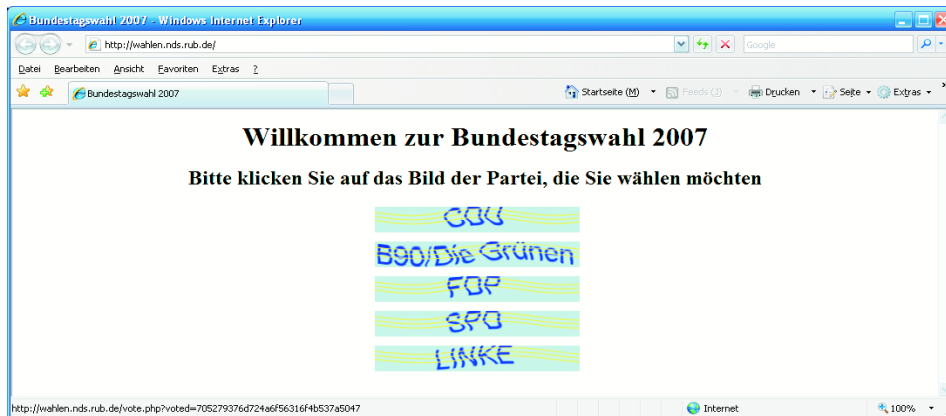


Figure 1: First screen for CAPTCHA-based code voting

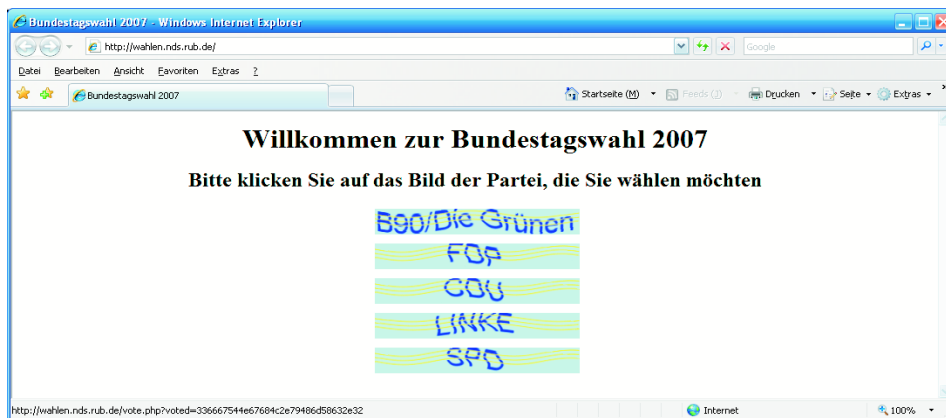


Figure 2: Second screen for CAPTCHA-based code voting

Figures 1 and 2 illustrate two possible screens. If, in this example, the voter selected CDU on the first screen (choice 1), then the voting code sent to the server would be:

705279376d724a6f56316f4b537a5047.

Similarly, if the voter selected CDU on the second screen (choice 3), then the voting code would be:

336667544e67684c2e79486d58632e32.

In either case, the voting code represents a cryptographic hash value and is visible in the browser's status line. Note that the two codes are different and unlinkable despite the fact that the selected party is the same. Also note that in CAPTCHA-based code voting, there is no urgent need to minimize the length of the voting code. The voting codes are sent by the browser to the server in a way that is transparent to the user, i.e., the user does not have to type it in. This simplifies things considerably, and the discussion held at the end of Section 3 is obsolete in this setting. So from a usability perspective, CAPTCHA-based code voting is perfectly fine. The user experience does not significantly deviate from what he knows and is accustomed to. In the following section, we address the question whether CAPTCHA-based code voting is also fine from a security perspective.

5 Preliminary Security Analysis

If one considers the use of code voting to overcome the secure platform problem, then one is mainly concerned with the possibility of automated client-side attacks mounted by malware. More specifically, one wants to make it impossible for an adversary to write malware that can modify a vote in some meaningful way. This must be true even if the malware has access to all information that is available in the client's operating system or browser. Note, for example, that such malware has access to the browser's state and content of Web pages, and hence that it is able to read out the voting codes. But it does not know what code belongs to what choice, and hence it can only make random guesses. In the example given above, the malware is likely to be able to read out the voting code 705279376d724a6f56316f4b537a5047 for the first choice on the first screen, but it is not able to associate this code to the CDU party (because this association is done outside the client system in the brain of the voter). Consequently, it cannot decide whether this selection is the appropriate one, and hence whether it should modify the vote. Also, in the case of an election with more than two options, if the malware knew that it should modify the vote, it would still not know which other option to select.

The bottom line is that CAPTCHA-based code voting remains secure (in the sense sketched above) as long as the CAPTCHAs in use remain secure, i.e., cannot be solved by a machine. If somebody can write a piece of software that can break the security of the CAPTCHAs, then this software can also be used to trivially break the security of CAPTCHA-based code voting. So we have to make the critical assumption that the CAPTCHAs in use are secure. This assumption is critical, because the security of CAPTCHAs has come under fire and many researchers are trying to compromise them.

Based on the assumption that the CAPTCHAs in use are secure, one can argue that CAPTCHA-based code voting remains secure as well. But there are still a few subtle attacks that must be considered with care. Let us briefly elaborate on two examples.

1. If an adversary has introduced himself in the communication channel between the client and the server, then he is representing a man-in-the-middle (MITM) and can display any CAPTCHA or CAPTCHA-like image. It is then simple for him to circumvent or bypass CAPTCHA-based code voting (because he can create the CAPTCHAs and therefore knows what they represent). Consequently, the use of technologies and mechanisms that protect against MITM attacks seems to be mandatory. There are a few such technologies and mechanisms available; examples include ciphersuites for the TLS protocol that support authentication based on pre-shared keys [BH06], SSL/TLS session-aware (TLS-SA) user authentication [OHB08], the use of client-side public key certificates, and a few more. Unfortunately, these technologies and mechanisms are not yet widely deployed, and hence, any currently available infrastructure for remote Internet voting and CAPTCHA-based code voting is vulnerable to MITM attacks. It is best to make this vulnerability explicit.

2. Since an increasingly large number of e-commerce application providers employ CAPTCHAs to make sure that their users are human, an adversary could collaborate with these providers to exploit the human resources (and capabilities) of their users. For example, an adversary could set up a free Web-based CAPTCHA service for e-commerce application providers. If invoked, this service could use CAPTCHAs found on compromised client systems and provide them to the users of the service. The responses could then be used by the malware to modify the vote in some meaningful way. In the example given above, the malware would input the five CAPTCHAs found on the first screen to the service. The service would dispatch the CAPTCHAs to individual users, and return the strings representing the names of the parties to the malware. The malware would then be able to decide if and how to meaningfully modify the vote. There is hardly anything that can be done technically to protect against such a distributed attack. Consequently, one must carefully monitor the CAPTCHAs that are used by service providers, especially during the time frames of the elections and votes that are supported by CAPTCHA-based code voting. Too many occurrences of strings that represent political parties or names of politicians should be taken as an alert.

We think that both attacks are relevant and must be considered with care. In particular, we think that the use of technologies and mechanisms to protect against MITM attacks and a careful monitoring of CAPTCHAs in widespread use are mandatory in a real-world deployment of CAPTCHA-based code voting.

6 Conclusions and Outlook

The secure platform problem is severe for remote Internet voting. The malware-based client-side attacks that are currently mounted against Internet banking (e.g., [ORH08]) can easily be turned into attacks against remote Internet voting. The attack vectors are essentially the same, i.e., it does not matter whether malware manipulates an Internet banking transaction or a remote Internet voting transaction. In either case, the manipulation occurs after user authentication and can be made transparent to the user. This should be kept in mind when people argue about the (in)security of remote Internet voting.

Against this background, we think that code voting provides an appropriate technology to address the secure platform problem of remote Internet voting, but that it is not particularly user-friendly. There are different possibilities to implement code voting, and these possibilities have specific advantages and disadvantages.

In this paper, we proposed the use of CAPTCHAs to improve the user-friendliness of code voting, briefly discussed the security of CAPTCHA-based code voting, and elaborated on a possible implementation. CAPTCHA-based code voting can only be as secure as the CAPTCHAs that are used. Alternatively speaking, if an adversary is able to break the CAPTCHAs in use, then he is also able to break the security of CAPTCHA-based code voting. Consequently, the current state-of-the-art in breaking CAPTCHAs should be closely monitored and observed. For example, there is a recently published low-cost attack on CAPTCHAs employed by Microsoft⁵⁹. In spite of the progress that has been made in order to break the security of CAPTCHAs, we still think that CAPTCHA-based code voting provides an interesting possibility to implement code voting in a real-world setting, and that it has potential for the future. It is certainly worthwhile to implement it, and to explore its use (and usability) in a field study.

⁵⁹ <http://homepages.cs.ncl.ac.uk/jeff.yan/msn.htm>

References

- [Ber08] Beroggi, G.: Secure and Easy Internet Voting. IEEE Computer, Vol. 41, Number 2, February 2008, pp. 52-56.
- [BH06] Badra, M.; Hajjeh, I.: Key-Exchange Authentication Using Shared Secrets. IEEE Computer, Vol. 39, Number 3, March 2006, pp. 58-66.
- [Cal00] California Secretary of State, California Internet Voting Task Force, Final Report, January 2000, <http://www.ss.ca.gov/executive/ivote/>.
- [Cha01] Chaum, D.: SureVote: Technical Overview. Proceedings of the Workshop on Trustworthy Elections (WOTE '01), August 2001, <http://www.vote.caltech.edu/wote01/pdfs/surevote.pdf>.
- [DR06] Dierks, T.; Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346, April 2006.
- [E+07] Elson, J. et al.: Asirra: A CAPTCHA that Exploits Interest-Aligned Manual Image Categorization. Proceedings of the 14th ACM Conference on Computer and Communications Security (ACM CCS 2007), 2007, <http://research.microsoft.com/asirra/papers/CCS2007.pdf>.
- [FKK96] Freier, A.O.; Karlton, P.; Kocher, P.C.: The SSL Protocol Version 3. Internet-Draft, 1996.
- [Nao96] Naor, M.: Verification of a human in the loop or Identification via the Turing Test. 1996, citeseer.ist.psu.edu/naor96verification.html.
- [OHB08] Oppliger, R.; Hauser, R.; Basin, D.: SSL/TLS Session-Aware User Authentication. IEEE Computer, Vol. 41, Number 3, March 2008, pp. 59-65.
- [Opp02] Oppliger, R.: How to Address the Secure Platform Problem for Remote Internet Voting. Proceedings of the 5th Conference on "Sicherheit in Informationssystemen" (SIS 2002)}, Vienna (Austria), October 3-4, 2002, vdf Hochschulverlag, pp. 153-173.
- [ORH08] Oppliger, R.; Rytz, R.; Holderegger, T.: Internet Banking Client-Side Attacks and Countermeasures. Submitted for publication.
- [Riv01] Rivest, R.L.: Electronic Voting. Proceedings of Financial Cryptography '01, February 2001, <http://theory.lcs.mit.edu/~rivest/Rivest-ElectronicVoting.pdf>.
- [Rub01] Rubin, A.D.: Security Considerations for Remote Electronic Voting over the Internet. Proceedings of the 29th Research Conference on Communication, Information and Internet Policy (TPRC 2001), October 2001, <http://avirubin.com/e-voting.security.html>.
- [Tur50] Turing, A.: Computing machinery and intelligence. Mind, Vol. LIX, No. 236, October 1950, pp. 433-460.
- [vA+04] von Ahn, L. et al.: Telling Humans and Computers Apart Automatically-How Lazy Cryptographers Do AI. Communications of the ACM, Vol. 47, No. 2, February 2004, pp. 57-60.
- [Yao82] Yao, A.C.: Potocols for Secure Computations. Proceedings of 23rd IEEE Symposium on Foundations of Computer Science, Chicago, Illinois, November 1982, pp. 160-164.

Session 8: Political Issues of E-Voting

E-Voting in Brazil – Reinforcing Institutions While Diminishing Citizenship

José Rodrigues Filho

Universidade Federal da Paraíba, Cidade Universitária
58.059-900 João Pessoa, Brazil
jrodrigues-filho@uol.com.br

Abstract: Brazil became the first country in the world to conduct a large-scale national election using e-voting technology. What does it mean for democracy to hold an electronic election for millions of poor people, most of them living under the poverty line? Is the high investment in e-voting technologies designed to the benefit of millions of illiterate people? The discussions about the lack of security of e-voting in Brazil and in many other countries are based on a rather reductionist view that neglects both its social and political aspects. In this work, an attempt is made to expand the critique of the problems of e-voting beyond its lack of security and technological failures. It is argued that information technology in many parts of the world is reinforcing institutions and has done little to change our democracy. In its current form, e-voting technology in Brazil seems to be reinforcing some institutions while diminishing citizenship and democracy.

1 Introduction

There are numerous and conflicting interpretations in the concept of citizenship, but it is commonly understood in terms of a framework of rights and obligations [Ja98]. In many countries there are some core political rights and obligations normally associated with citizenship – voting, deliberation or participation in the political process, and the access or right to the provision of information. So, how to improve citizenship and political practices envisaged in these core political rights and obligations?

It is argued that while Information and Communication Technologies (ICTs) hold the potential to improve the democratic process, expand citizenship and empower the people, they have the ability to perpetuate or exacerbate existing inequalities and other divides. Commenting on the gap in access to ICTs, some authors have stated that “the information revolution could paradoxically become a cause of even greater inequality and worsening poverty” among developing countries [McO04]. In addition, there are comments about the dangers of digital opportunities pointing out that the “unequal diffusion of technology is likely to reinforce economic and social inequalities leading to a further weakening of social bonds and cultural cohesion” [UN05].

Little research has been conducted to answer questions related to the effects of ICTs on citizenship, the political process, and its opportunities and dangers. In addition, the literature has shown that answers to these questions have been rather extreme. They have either a sceptical view over-emphasizing the negative aspects of ICT, on the one hand, or, on the other hand, an optimistic or Utopian view, enthusiastically spelling out hope that new technologies would strengthen and enhance the democratic process [GI01].

It is stated that the influential political science research in modern democracy has narrowed citizenship and reduced it down to the right to vote in elections, turning democracy to be experienced at elections time and not between elections. In Brazil, voting is mandatory and the duty to vote is very much questioned by voters. E-Voting, as a political tool, was introduced as part of an electoral reform that seems to be reinforcing this very narrow concept of citizenship, especially taking into consideration that election turnout decreased in the last election and vote buying increased considerably. It seems that with the erosion of democracy, voter turnouts have declined in many countries, independent of the nature of voting as a right or as a duty.

There is a need of more empirical research surrounding citizenship and new technologies and not just theoretical discussions. Because Brazil was the first country in the world to conduct the biggest election in the planet using e-voting technologies, when more than 100 million voters cast their ballots on more than 406.000 touch-screen machines scattered all over the biggest country in South America, an attempt is made in this study to approach the topic of e-voting in the Brazilian citizenship subject, looking at the impact of the electoral reform (e-voting) on the realization of citizenship that should seek to empower people through the use of ICT. An electoral reform or a new technology may have a positive impact on democracy and citizenship, if developed and implemented from below and not from the top-down model of politics.

2 ICT and Citizenship

There are diverse understandings of the term citizenship, which require a broad range of philosophical, sociological and political theory for its discussions and debate. In a less narrow view, citizenships consist of a compact of legal rights, protections and duties between government and individual members of society. In a broad sense, citizenship represents a framework of universal political, civil, social and participation rights. According to Janowski, citizenship comprises active and passive rights and obligations. "Citizenship is passive and active membership of individuals in a nation-state with certain universalistic rights and obligations at a specified level of equality" [Ja98]. In short, there is no universal definition of citizenship, and it is a contested concept with multiple definitions. Citizenship is "a peculiar and slippery concept with a long history [Ri92]."

According to Elliot (2000), two different theoretical perspectives to access the roles of individuals and their interrelationships in the current debate of citizenship have been identified: traditional social liberal, and neo-liberal. The traditional social liberal approach, in which the Marshallian theory of citizenship have been extensively discussed for half a century, emphasizes the importance of civil, political and social rights as elements of citizenship [El00].

The neo-liberal approach, on the other hand, rejects the welfare state, as the social rights element of citizenship, and supports the free market. In short, it emphasizes individual obligation and denies the collective rights and responsibilities. Due to new relations between nation states and citizenship and democratic control, there has been reformulation of those traditional concepts of citizenship. Therefore, new notions of citizenship have come onto the recent academic agenda as follow:

- ecological citizenship concerned with the rights and responsibilities of the earth citizen [St94];
- cultural citizenship involving the right to cultural participation [Tu93];
- minority citizenship involving the rights to enter a society and to remain within it [El00];
- cosmopolitan citizenship concerned with how people may develop an orientation to many other citizens, societies and cultures across the globe [He95].
- technological citizenship is concerned with the ways in which citizenship norms, rights, obligations and practices are encoded in the design and structure of our increasingly digital surroundings [Lo05].

The expansion of Information and Communication Technologies (ICTs) in several countries has given rise to many e-government and e-democracy systems and initiatives very much based on an administrative-technological perspective. The information technological network infrastructure created from a nation-state perspective or from above is oriented more towards the provision of services into a network than towards the implementation and development of democracy or citizenship. It is recognized how crucial these services are, but in many instances they do not actually empower the citizen. The establishment of e-government and e-democracy, and the implications behind the initiatives of the cyber-state, promise to revolutionize many countries in terms of governance and democracy. However, it is mentioned that “while there is the political possibility of shaping the emerging cyber-state as a vehicle of empowerment,” especially for the marginalized others, “there is also the prospect that Internet-facilitated government will exacerbate inequalities” and diminish citizenship status [Mc04].

Under this nation-state perspective or top-down model, citizenship is constructed based on principles of the liberal tradition and “citizenship rights are being reconceptualized to reflect the neo-liberal agenda, in which citizens are expected to take care of themselves and those who fail to become self-sufficient are considered problematic and deviant” [Mc04]. In this case, an alternative society is a self-help society, based on morals of helping that can produce community services by voluntary work. In consequence, a so-called ‘new lower class’ is emerging, even in the richest OECD-countries. “These people are the long-term unemployed, permanently poor, badly-off ethnic groups and those who have fallen through all social safety nets.” In short, they are second class citizens that cannot realize the principles of good citizenship – autonomy, self-esteem, participation and influencing in their own reference community and society, challenging the traditional concept of citizenship.

With the expansion of ICTs there is a need to understand not only the opportunities created by new technologies but also the risks regarding the realization of citizenship and civil rights. Therefore, ICT and citizenship should not be separated, because ICT in itself does not guarantee the realization of the rights of the citizen. Despite the determinist view and the expanding literature favouring the use of ICTs in the information society, e-government and e-democracy, it is recognized that the citizenship is at risk. The problem is that the conditions of technology are emphasized, but it is not fully clear what exactly is meant by the concept of the citizens’ information society. It is recognized that many initiatives are necessary to turn computers and the Internet into a tool for civic participation. If, in the developed world, it is found that “mere presence of favourable conditions for making ICT a civic tool are not enough” [Ol06], in developing countries the situation is too complex.

Unfortunately, in the developed world, most of the academic work produced does not seem to worry about the relationship between ICT and citizenship, making it difficult for people to believe that they make a difference in a local/national governing, because the agenda seems to be already set. On the other hand, in developing countries, in some instances, one may even fear making a critique on how badly resources are allocated in the field of information technology.

In a framework of citizenship rights and obligations comprising civil, political, social, and participation rights and obligations, underpinned by elements of ‘good society,’ such as freedom, equality and justice, the political rights and obligations of voting, participation in the democratic process and access to information were selected for further discussion. In short, what is the impact of the electoral reform that introduced e-voting technology in Brazil on the political rights and obligations normally associated with citizenship - voting, participation in the democratic process, and access to information?

3 E-Voting in Brazil

It is stated that both democracy and voting are processes much more complex than their electronic version and a secure voting system in itself is a basic element of a true democracy. The e-voting technology in Brazil consists of the so-called Direct Recording Electronic (DRE) devices, which allow voters to cast their ballots directly through touch-screen voting machines. In this case, voters have to go to the polling stations to cast their ballots after a conventional identification. In remote electronic voting systems voters cast their ballots remotely, using the full potential of ICT [RRB05]. In other words, the DRE is a kind of offline voting system and the Internet is the online voting system.

The modality of electronic voting in Brazil through machines of the type Direct Recording Electronic (DRE) Voting System or electronic ballot boxes (Urnas Eletrônicas - UR) does not seem to have modified the traditional ritual of elections. The great difference is that in the traditional voting system the voters could see the ballot papers fall into an urn bag, placed in it by themselves, surrounded by inspectors. With the electronic ballot box, the voters do not have the certainty that their votes were registered and no inspector or witness certifies this: the vote is registered electronically.

Therefore, in the current system of electronic voting (DRE), the voter does not see the ballot box, but a representation of it. In turn, the machine does not supply an independent and true registration of each individual vote that could be used for a count or verification of errors in the machine or some type of tampering. In this case, if the machine registers a result in its memory that is different from that chosen by the voter, neither the voter nor the inspectors will know about it. Because of this, some specialists in computer security believe that such machines are more vulnerable to tampering than any other form of voting system, especially through the use of malicious computer codes.

Some specialists argue that software can be modified in such a way that the results of an election can be modified, being very difficult to be detected [Fi03]. Consequently, the security of electronic voting is susceptible to failures and frauds and some Brazilian experts question our e-voting system and its security through Internet journals, forums, articles and books [BC06, Ma02, Si02]. Similarly, comments and reports of international scientists corroborate with what our academics and scientists say, such as reports that argue on the security and risks of this kind of system in the United States [BC06, CMIT01, Ko03, Ko03]. It is known that electronic voting has existed for a long time in developed countries such as the United States, Germany and Japan, among others [Ma00], but more recently there have been many concerns about e-voting insecurity, especially in the more traditional democracies.

Some authors have been in favour of a more reliable e-voting system that can have the so-called voter-verifiable trails and an open source code, and it is likely that this kind of system may appear with the advance of technology and its lower price, although it is alleged that e-voting will never be error-free. On the other hand, some authors have emphasized the importance of political and socio-technical approaches for the development of an e-voting system that can ensure public trust in the results of an election [RR05]. Thus, apart from the technical aspects, it has been mentioned already that e-voting in Brazil has exacerbated alienation and the digital divide [RG08].

Paradoxically, the Superior Electoral Court (Tribunal Superior Electoral – TSE), known as the Electoral Justice, is responsible for election administration in Brazil; it has unexpectedly and rapidly adopted one technological system that has not yet been sufficiently tested even in the developed world. According to the critics of electronic voting, the Electoral Justice has opened the doors for new and sophisticated frauds much more serious than the traditional ones [Ma05], once the ballot's verification became private and the Electoral Justice the owner of the ballot boxes [Fr02].

During the last ten years, the Electoral Justice in Brazil has developed an intensive campaign emphasizing the security of e-voting, and on how the citizens should be proud of this technology that is said to be made in Brazil. Consequently, through the use of an intense propaganda, the Electoral Justice was able to institutionalize e-voting, and most of the population is proud of e-voting machines, believing that they are more secure than the traditional system.

However, over the last few years, the complaints about e-voting machine failures, corruption, and all sort of other critiques have intensified both in Brazil and in other countries that held elections more recently, such as the United States, Holland and France. Early in 2007, for the first time, the Brazilian Congress created a Sub-Commission for Electronic Voting that opened some hearings to improve the security of e-voting in the country. In one of its first hearings, a famous Brazilian politician and one of the richest men in the country, confirmed that for several times, at election time, he was asked whether he would really want to be elected. In another hearing an expert in e-voting technology security stated that he trusted the banking system more than e-voting machines in Brazil. In other words, he stated that e-voting machines are not secure at all.

A few months latter the Sub-Commission for Electronic Voting recognized the e-voting system insecurity in Brazil and proposed e-voting machines with paper trail capabilities to enable voter verification during elections. Although the so called voter-verified paper trail is demanded as the essential requirement to mitigate the risks associated with software and hardware flaws, there have been questions as to whether voter-verified paper trails will provide a significant benefit, given the costs added to e-voting tools. It has been recognized that many of the problems associated with e-voting machines are caused by a lack of training for workers who sometimes do not even know how to change the paper in the machines with paper trail or administrative mistakes. Anyway, in the case of Brazil, a few hours after the Sub-Commission published its final report, the Electoral Justice in Brazil rebutted it.

4 Corruption, Vote Buying and Turnouts

One of the purposes to use e-voting technology in the developed world is to increase turnouts, due to the discredit of voters with politicians and political parties. So, the kind of electoral reforms proposed in many countries to make it easier for registered voters to cast their ballots tends to benefit politicians and their parties with perverse consequences towards political engagement [Be05].

In Brazil, many electoral reforms have been approved over the last few years, but none of them aiming at improving political engagement. Although we do not know about the true relationship between e-voting technology and turnout, during the last election turnouts have decreased in the Parliament election in Brazil. A decrease in turnout may be a reduction in citizenship, but its relationship with e-voting technology is not clear. In the last election there was an intensive campaign on the Internet from the young people proposing to make the vote null. How far this campaign has influenced the population is also not yet known.

It is necessary to make it clear that an increase in turnouts does not necessarily mean more political participation and civic engagement. In many countries there is some political participation at election time, but people need democracy between elections and not only at election time. People want to participate in the decision making process between elections, and this is not always the case. It is here that the use of ICTs may help voters to have a better engagement in the political process. In the case of Brazil, voters need government “of, by, and for the people.”

What is e-voting for, when money is choking our democracy to death? With the increase in the cost of getting elected, exploding beyond the reach of ordinary people, during the last election it was possible to register that our representatives in the Brazilian Parliament are richer than their predecessors. In this case, is the Brazilian Congress, the so called “People’s House,” really the place for the highest bidder, considering that some of our representatives are elected based on an empire of corruption, turning elections on auctions?

It is known that corruption in elections in Brazil and in many other countries is not an abstract thing. It is a crude and disgraceful reality. Electoral corruption is a kind of arrangement usually involving candidates, donors and voters who are bribed to sell their votes in a transaction in which the object can be cash, food, cloth, construction material, medicine, and the provision of other services. Since the year 2000, the NGO named “Transparência Brasil” has carried out surveys about vote buying in Brazil. According to the Transparência Brasil, the Electoral Justice in the country is responsible for neglecting the problem of vote buying [TB06]. It is very strange that the Electoral Justice is very much in favour of the e-voting technology system used in Brazil and is enable to enforce the law to combat vote buying. Is there a need of e-voting technology for the elections of corrupted politicians? Vote buying by itself is a sign of reduced citizenship.

So, e-voting in Brazil has not stopped vote buying which is increasing, and in 2006, during the last election, was twice as high than in the previous elections. What is surprising is that vote buying is higher among persons with secondary or higher education than voters with only primary education or below. It is expected that the poorer the voters, the more vulnerable they are to offers. The surveys from *Transparência Brasil* have shown that this is not true. More offers were made to the poorer, but vote buying is registered among the wealthier classes [TB06]. In order to give an idea of the magnitude of the problem of vote buying in Brazil, in 2006 it was found that about 8% of voters were asked to sell their votes for money [TB06]. Considering the number of voters in 2006, this corresponded to about 8.3 million voters, and represents more than the population in some European countries and in some Brazilian states.

5 Conclusion

Because voting is mandatory in Brazil, there is a need of a democratic tool for civic and effective participation in the democratic process, which is contingent upon political participation. Democracy means widespread involvement of ordinary people in matters of governance. In its current trend, e-voting technology does not seem especially hopeful. For those who endorse technologies enthusiastically as they emerge, such as e-voting, any criticisms or requests for wider debate about policy options in technology are often regarded as negative and unhelpful. Critical voices have often been labelled backward and obstructive, especially when they try to explore social and political consequences of technological choices.

Some electoral reforms may have perverse consequences on citizenship and democracy. By making it easier for all citizens to vote does not mean improvement in democracy and citizenship, especially when a top-down political tool is designed in ways that bring more power to the political elite. Can we combine an approach very much based on market-driven forces (e-voting) that suits existing political and bureaucratic elites with a real process of democratization (e-democracy)? In other words, can the state provide services to please the citizens without democratic engagement?

There is no doubt that e-voting facilitates the work of the Electoral Justice in Brazil when, a few hours after an election, the names of those elected are informed. This brings prestige to the Electoral Justice whose power is reinforced by e-voting technology. Over the last ten years there has been an official massive propaganda in Brazil about e-voting and its security, in addition to training and demos on how to vote electronically. As a consequence, the majority of the Brazilian society trusts our e-voting system and its security. In this situation, it is quite hard to comment against e-voting in the country.

In spite of this, it seems that democracy in Brazil is at risk: women's representation in the Brazilian parliament has decreased; our representatives in the Parliament are getting richer than their predecessors, and richer politicians get richer after their elections; turnouts decreased in the last election, and vote buying increased substantially. Corruption in the Brazilian Parliament has reached such a level that a recent edition of the Economist has made reference to it as a "Parliament or Pigsty?" thus, commenting on the sophisticated criminal organization to buy votes [Ec07].

The political elite has no interest in discussing e-voting in Brazil, let alone the poor that are excluded completely from the political life. However, if political participation and civic engagement do not improve, there are substantial arguments to discuss e-voting in Brazil. Due to the trust in the system and the official voice supporting it, there is no chance to question the technology just in terms of its security. However, when social and political issues are questioned, there are many things that people have not thought of, and it is time to start arguing about it. If people care about citizenship, the time is appropriate for the debate about the relationship between e-voting technology and citizenship.

How helpful would it be if the academic research work in the developed world could look not only at the technicalities of e-voting, but to its social and political issues and on how it should be designed in ways to reflect our best understanding of freedom, social justice and addressing the source of inequality and injustice. The technical problems of e-voting, especially in terms of security, can be solved in the near future, and people can easily understand it. However, when matters related to social and political problems are considered, it will take years for the poor voters, for example, to understand what is going to happen to them. This situation forces us to care about them and the future of democracy. We cannot survive without the help of technology, but we cannot let the market work and express our politics just by watching the TV screen.

The e-voting project in Brazil is an initiative that merely reproduces traditional and dominant forms by which power is exercised. This is a tool that exacerbates inequality, alienation, and exclusion, but it seems that it is not awakening the "consciousness of how men are deceived in a permanent way."

References

- [Ba05] Berinsky, A. The Perverse Consequences of Electoral Reform in the United States. *American Politics Research*, 33(4):471-491, 2005.
- [BC06] Brunazo Filho, A.; Cortiz, Maria Aparecida. *Fraudes e Defesas no Voto Eletrônico*. São Paulo, All-Print Editora, 2006.
- [BC06] The Brennan Center of the NYU School of Law. Brennan Center, New York, 2006.
- [CMIT01] The Caltech/MIT Voting Technology Project. Residual Votes Attributable to Technology – An Assessment of the Reliability of Existing Voting Equipment (2001). Available: <http://www.vote.caltech.edu/Reports/index.html>.
- [Ec07] The Economist. Parliament or pigsty? (2007). Available: http://www.economist.com/world/la/displaystory.cfm?story_id=8670490
- [EI00] Elliot, J. The Challenge of lifelong learning as a means of extending citizenship for women. *Studies in the Education of Adults* 32(1), 6-21, 2000.

- [Fi03] Fischer, E.A. Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues, Congressional Research Service (CRS) Report for Congress, November, 4, 2003.
- [Fr02] Freitas, Silvana de. Voto eletrônico amplia chance de fraude. Entrevista. Folha de São Paulo (2002). Available: <http://www.brunazo.eng.br/voto-e/noticias/folha11.htm>
- [Gi01] Gimmler, A. Deliberative democracy, the public sphere and the internet. *Philosophy and Social Criticism* 7(4):21-39, 2001.
- [He95] Held, D. . Democracy and the Global Order. Cambridge: Polity Press, 1995.
- [Ja98] Janoski, T. Citizenship and Civil Society. Cambridge. Cambridge University Press, 1998.
- [Ko03] Kohno, T et al. Analysis of the Electronic Voting System. John Hopkins Information Security Institute. Technical Report TR-2003-19, July 23.
- [Ko03] Konrad, Rachel. E-Voting critics point to security hole. California primary results appeared online before polls closed. Associated Press MSNBC News (2003). Available: <http://stacks.msnbc.com/news/964736.asp?0dm=n15ot>.
- [Lo05] Longford, G.: Pedagogies of Digital Citizenship and the Politics of Code. *Techné* 9:1 Fall 2005.
- [Ma02] Maneschy, Osvaldo et al. *Burla Eletrônica*. Rio de Janeiro: Fundação Alberto Pasqualini, (2002).
- [Ma00] Maneschy, Osvaldo. *Fraude eletrônica nas eleições* (2000). Available: <http://www1.jus.com.br/doutrina/>.
- [Mc04] McNutt, Kathleen. "Will e-Governance and e-Democracy Lead to e-Empowerment? Gendering the Cyber State." *Federal Governance: A Graduate Journal of Theory and Politics*. 4.1, 2004.
- [McO00] McNamara, K., O'Brien, R. Access to Information and Communicatio8n for Sustainable Development Opportunities and Challenges for International Community-Recommendations of the Access Working Group. In GKP II Conference, Global Knowledge Partenership Secretariat. Luala Lumpur, Malaysia, 2000.
- [OI06] Olsson, T.: Appropriating civic information and communication technology: a critical study of Swedish ICT policy visions. *New Media & Society*, 18(4): 611-627, 2006.
- [RG08] Rodrigues Filho, J., Natanael Pereira Gomes. E-Voting in Brazil – Exacerbating Alienation and the Digital Divide. In Mishra, Santap Sanhari. *E-Democracy – Concepts and Practice*. Índia, IFCAI Books, 2008.
- [Ri92] Riley, D. Citizenship and the Welfare State. In: Allan, J., Braham, P. Lewis, P (eds). *Political and Economic Forms of Modernity*. Cambridge: Polity Press, 1992.
- [RR05] Randell, Brian, Peter Y. A. Ryan. *Voting Technologies and Trust* (2005). Available: <http://www.cs.ncl.ac.uk/research/pubs/trs/papers/911.pdf>.
- [RRB03] Riera, Andreu Jorba, Jose Antonio Ortega Ruiz, Paul Brown. *Advanced Security to Enable Trustworthy Electronic Voting*. ECEG Proceedings. 3rd European Conference on e-Government. Trinity College, Dublin, 2003.
- [Si02] Silva, Mônica Correia da. *Voto Eletrônico - É mais Seguro Votar Assim* - Florianópolis. Editora Insular Ltda, 2002.
- [St94] Steenberg, B. Van ed. *The Condition of Citizenship*. Sage Publications: London, 1994.
- [TB06] *Transparência Brasil. Compra de Votos nas Eleições de 2006, Corrupção e Desempenho Administrativo*. 2006.
- [Tu93] Turner, B.S. ed. *Citizenship and Social Theory*. Sage Pub.: London, 1993.
- [UN05] UNPAN. *UN Global E-Government Readiness Report – From E-Government to E-Inclusion*. Division for Public Administration and Development Management. Department of Economic and Social Affairs. United Nation, New York, p.3 2005.
- [YD97] Yuval-Davis, N. *National Spaces and Collective Identities: Border, Boundaries, Citizenship and Gender Relations*. Inaugural Lecture, University of Greenwich, 1997.

The Voting Processes in Digital Participative Budget: A Case Study

Gleison Pereira de Souza¹, Cristiano Maciel²

¹Prefeitura Municipal de Belo Horizonte
Secretaria Municipal Adjunta de Tecnologia da Informação
Rua Goiás nº 58 Centro, Belo Horizonte, Minas Gerais, Brazil
gleison@pbh.gov.br

²Centro Universitário Augusto Motta
Av. Paris nº 72, Bonsucesso, Rio de Janeiro, Brazil
crismac@gmail.com

Abstract: The Participative Budget consists of a process in which citizens can directly participate in decision-making and regulation of public budget spending. The experience of the City of Belo Horizonte (Brazil) with the Participative Budget is a consolidated e-democratic process in the government and, most importantly, for the population. By exploring techniques provided by Information and Communication Technology, the Digital Participative Budget was introduced. Hence, a new question is posed: which methodology should be used for the computerization of this process and what would be the best suited interaction and communication resources for the e-democratic process? Such decisions will be discussed in this paper. This paper presents the experience of Belo Horizonte with the implementation of the Digital Participative Budget, from the very conception and implementation of the project up to the voting period as well as its current phase. Accordingly, this paper broaches the discussion of the conditions that led to the development of this project, the model adopted for the computerization of the process, the functionalities of the web system, and the data from the case studies developed in Belo Horizonte.

1 Introduction

The Participative Budget, or PB, consists of a process in which citizens can directly participate in decision-making and regulation of public budget spending. Participation becomes effective by means of public Participative Budget assemblies, generally implying presence, which assures all citizens an equal weight in the decision-making process, regardless of their affiliation to any type of organization and lacking any privileges.

This public policy of political participation is one of the dialogical instruments created to bring together citizen and public administration in the generation of public interest, creating new pathways for Representative Democracy. Voting does not suffice; one must also participate. It is also not enough to base general (public) decisions in technical theses. These are certainly important, but consensus reached by those directly concerned (whether individual citizens or the community) must always be a desideration of this new Public Administration tendency.

The experience of the City of Belo Horizonte (Minas Gerais, Brazil) with the Participative Budget began in 1993 and was a result of an institutional change seeking the creation of government spheres that would be closer to the citizens and better able to perceive/address the demands of the populace. Today, the Participative Budget is already a consolidated process in the government and, most importantly, for the population of Belo Horizonte. Since it was first established, almost one thousand public constructions have been initiated and delivered to the population, a fruit of the population's choice via Participative Budget.

In the year 2006, the municipal government reached a milestone regarding this policy, guided by the pursuit of increased political participation. By exploring techniques provided by Information and Communication Technology, the Digital Participative Budget was introduced. Hence a new question is posed: which methodology should be used for the computerization of this process and what would be the best suited interaction and communication resources for the e-democratic process? Such decisions will be discussed in this paper.

Consequently, this paper presents the experience of Belo Horizonte with the implementation of the Digital Participative Budget, from the very conception and implementation of the project up to the voting period as well as its current phase. Accordingly, this paper broaches the discussion of the conditions that led to the development of this project, the model adopted for the computerization of the process, the functionalities of the web system, and the data from the case studies developed in Belo Horizonte.

2 Democracy and the Internet

In democracy power can be exercised by many, it is the people's expectations that prevail in all political decisions. According to [Ca64], democratic political forms are grounded on the assumption that no man or limited group of men is wise enough or good enough to govern others without their consent. Inquiring into their preferences is an essential part of the democratic process. However, freedom of expression in democracy does not merely involve being able to express an opinion about predefined options. In order for it to be effective, it must allow people to articulate a discourse, outline proposals, discuss them and confront them with other proposals through public communication means.

There are several classifications for democracy. This paper considers three democracy models as proposed by [As01]: quick, strong and thin. These models are based on the roots of traditional democracy and are used as a bridge between profound democratic theory and its electronic manifestations. A synthesis and later discussion of the characteristics, legitimacy, citizen's role, politician's administrative style and use of ICT's by these models is presented in Table 1.

| Democracy | Quick | Strong | Thin |
|-----------------------------|-----------------|---------------|---------------------------|
| Characteristic | empowers people | consensus | choice efficiency |
| Legitimacy | majority | public debate | government responsibility |
| Citizen's role | decision-maker | opinion-maker | Consumer |
| Administrative style | limited | interactive | Open |
| Focus on use of ICT | decision | discussion | Information |

Table 1: Democracy Models [As01]

Similarly to quick democracy, strong democracy demands active citizens, but rather than speeding up the decision-making process, strong democracy favours a slow and far-reaching involvement of people in the discussion and deliberation processes, —a situation that can be achieved in several electronic forums. While quick democracy starts from the assumption that most citizens have a critical sense of a wide variety of complex issues involving society and that decisions can be defined by the majority, strong democracy favours the development of individuals through information, discussion and debate. The strong model means not only empowering people but also providing education for the understanding of society. When people discuss social issues, a platform of respect, trust, tolerance and openness is created, and these are the essential ingredients of strong democracy. Strong democracy is indicated to conceive an e-Democracy model.

Typically, the only institutionalized channels people have to dialogue with the Government are political and administrative paths - insufficient for a participative democracy - and direct people-citizen dialogue, which is facilitated by communication means capable of turning the transmission of messages into a bilateral process.

We can identify three problems regarding democracy and citizen participation on the Internet [Wo00], namely: 1) difficulty to integrate Internet and political debate and consequently turn away from the ongoing unanimity that prevents any critical reflection; 2) difficulty to actually enter the field of politics; and 3) improving Internet applications, considering that the technical revolution did not have the expected effect on society, which means that the techniques are not efficient enough. Nowadays, traditional development of online e-Democracy follows a relatively predictable model [UK02]: organizations offer information to start with, then they add services and then attempt to add 'interactive' tools.

In order to use ICT's to effect, an infrastructure is needed to allow interaction with and access to the citizens and supporting: organization and classification (information and service); safety and reliability (electronic voting); moderation, control, quality and response guarantee (electronic participation). Implementing ICT's in e-Voting [OV04] [UK02] involves offering an electronic service package such as online voting and registration, devoting careful attention to safety, reliability and scalability. Electronic participation represents the use of ICTs in supporting the information, consultation and participation of citizens [LC07]. Using ICT's to open new communication channels is far more complex, since it requires new relationships to be developed between government, citizens and representatives.

Those relationships in the Brazilian Government, in order to encourage citizen participation in decision-making, have been done through the Participative Budget (PB). The following section discusses this topic.

2.1 Participative Budget

In the Brazilian government model, during the electoral process, politicians present a government project. In case the project foresees a democratic and popular management, it must compromise, among others, the popular participation in the quarrel and application of the public resources, in the clear of practical administrative, in the recovery of the excluded segments citizenship of the society, in the environment sustainable development, in the preservation and valuation of the cultural patrimony and in the construction of dignity and respect to the human rights of a city.

During the execution of such projects, a significant population participation becomes necessary in the elaboration and control of the municipal public budget to consolidate the Participative Budget (PB). PB has been implemented in Brazil since 1989 in cities compromised with democratic management. Today, it is a reality in more than 140 cities.

Cities execute different methodologies looking for real citizen participation. In a general manner, PB is composed by:

- Marketing: papers and posters in the cities inform the calendar and methodology of PB in the current year;
- Council Members: represents the participants of the PB in a region or thematic, elected in an established number by the cities;
- Municipal Assembly or Forum of the PB: is the great meeting of the population to elect and/or to install the new council members of the PB and to deliver to the government, the hierarchy of the workmanships and services demanded for the cities. It's also argued themes/demands and its priority criteria and has realized a rendering of accounts.

- Participative Budget Council (PBC): space of representation and negotiation, making it possible for the council members to intervene in the debate of the municipal budget.
- Council Forum: they are regional or thematic meetings for debate, subjects of general interest. The regiment of the City Council of the Participative Budget is also argued and approved.

Garcia, Pinto and Ferraz [GPF05] analyze three prototypical attempts to increase the participation of the people and propose to create a system, the e-PPB (Electronic Participatory Public Budgeting) that simulates what an executive assistant would do, if humanly feasible, that can be summarized into five tasks:

1. Identification

- read each suggestion
- emphasize the keywords in the message

2. Interpretation

- rephrase the suggestion using the vocabulary of a predefined ontology
- classify each suggestion in one of the known themes or create new themes to incorporated creative ideas

3. Clustering

- group similar suggestions and add statistical information to the classified themes
- create an executive summary to show to the “boss”

4. Analysis

- check if there has been any executive action that has already addressed any of the provided suggestions

5. Follow-up

- send a personalized acknowledgement message to all suggestion senders with a special status note to the ones for which a government action has already been started
- keep an eye on eventual government measures that directly or indirectly make suggestions. Again, he or she would send a message advertising the measure, mainly to the ones who sent suggestions asking for that type of measure.

These are mechanical tasks that request intelligence, mainly concerning text mining activities. Technology is ready. In accordance with the tasks cited above, the authors proposed a computational helper to assist executives in listening to people’s suggestions.

Some of the current Brazilian experiences use TICs to innovate the PB, however, they make use of strategies such as e-mail and voting/polls [GMP05] [MNG05] not allowing the full use of the Internet technology, and the consequence is a lack of participation of the citizens in the democratic process. On the other hand, experiences with consultative and deliberative processes, engaging citizens by using a virtual community, are being investigated [MG07].

Belo Horizonte (MG) city [BE07], has a significant experience in PB and is discussed in the next section.

3 Participative Budget in Belo Horizonte

Since 1993, the Participative Budget in Belo Horizonte has functioned as an instrument to bridge the interests of the Public Administration and the population, especially in areas with the most urgent need for public constructions and/or services, and, of course, proceeded by city planning (a crucial moment of political participation).

The PB renders effective many democratic goals and is currently, in Belo Horizonte, a biannual process, containing many steps where the population may express its intentions and deliberate on government planning. This process is noticeable for combining the participation of grassroots associations with that of unconnected individual citizens, which ends up representing a much more elevated and significant number of participants.

In 2006, the City of Belo Horizonte made an innovative achievement in the country in the field of public policy for participative democracy. Besides the already consolidated presential PB, an internet-based consulting and voting system, entitled Digital Participative Budget – Digital PB, was available for the population. Using Communication and Information Technology, the voting population of Belo Horizonte may directly, individually and equally define the public construction work that should be executed by the City, thus effectively partaking in the allocation of public spending.

This initiative was aimed at promoting the expansion of political participation, introducing and publicizing the PB to segments that would normally not get involved in its processes, such as middle class and young sectors of the population, and moreover falling upon the promotion of digital inclusion using internet resources. The Digital PB takes place every two years.

It is worth noting that Belo Horizonte, capital of the state of Minas Gerais, is the fifth Brazilian metropolis in terms of population size, which is 2.3 million. The complexity of a process involving such a numerous population was a challenge for the municipal public administration.

For the implementation of this process it was necessary to conceive a web environment projected with user-friendly interaction and communication resources and to promote the migration of the system to the Internet, safeguarding the basic premises of the participative budget. These aspects are discussed below.

3.1 Digital PB

The conception of a system with Belo Horizonte's Digital PB complexity forced the establishment of a careful methodology, as presented, and the selection of communication resources that would provide more interaction with the citizens, who are the targeted public of the application. This environment is available on [Be07].

In this sense, the following interaction and communication resources, among others for supporting additional functionalities, were defined: videos, streaming, forums, chats, contact us, public work perspectives and photographs, flash animation, news articles, weekly newsletters, and voting ballots. In this session, some of these user interaction resources are commented and illustrated:

The **forum** makes citizen-City interaction possible, allowing for the exchange and sharing of ideas, compliments, suggestions and directions. The experience demonstrated that the forum was an interesting and important means for the citizen to defend and debate the public construction works being voted. Free chats with the population also took place, permitting an exchange of ideas in real time. The screen below, in Portuguese Language, displays the discussion forum developed.

| Nome do fórum | Tópico | Respostas | Autor | Visitas | Última mensagem |
|--|---|-----------|-----------|---------|----------------------------------|
| Deixe aqui seus comentários, críticas, elogios e sugestões | OP Digital - Elogio [Ir para a página: 1, 2, 3] | 30 | Anonymous | 654 | 18/12/2006 16:31:18 Anonymous |
| Regional Centro-Sul | Policlínica | 2 | Anonymous | 132 | 07/12/2006 11:36:58 Anonymous |
| Regional Nordeste | Revitalização da Av. José Cândido da Silveira | 4 | Anonymous | 216 | 07/12/2006 11:37:51 Anonymous |
| Regional Nordeste | Na Pampulha vote na preservação das nascentes. | 0 | Anonymous | 80 | 07/12/2006 11:37:51 Anonymous |
| Regional Centro-Sul | Reforma da Policlínica Centro-Sul | 0 | Anonymous | 83 | 06/12/2006 17:56:34 Anonymous |
| Regional Centro-Sul | OP - Digital - Reforma da Policlínica Centro-Sul | 0 | Anonymous | 72 | 06/12/2006 17:56:34 Anonymous |

Figure 1: Forum in Digital PB

The **photographs** and **know more** allow the citizen to develop a more detailed outlook of the public constructions being debated and the subsequent voting process in the Digital PB. The menu topic, **construction perspectives** is a space created to give a future view of the construction, thus showing the before and after. See below the interface that displays pictures of the construction works.



Figure 2: Pictures of the construction works in Digital PB

The **video and streaming (DMP)** resources available in the Digital PB allow a good level of interactivity, since they synchronize voice, image, and text resources in a single application, providing a complete and dynamic overview of the construction work, besides providing accessibility to people with special needs. Streaming is a technology that permits watching the video while it is still downloading.

The **flash animations** were developed as a simpler visualization option than the videos of the construction works, geared towards the computers that do not possess the necessary resources to access the DMP video.

The **newsletter** is an electronic bulletin, by means of which the City of Belo Horizonte would send, via emails to registered citizens, information about the running of the voting process, construction works, testimonials, etc.,

In the voting stage, the citizen only needed to type the name and number of his/her voter registration in the Digital PB in order to access the ballot, which contained the list of construction works for voting. The projected interface was based on the design of a printed voter registration, as can be seen in the image below.



Figure 3: Ballot vote in Digital PB

This system was developed with state-of-the-art technology, with JAVA (J2EE) as the programming language, Oracle 10g as the database, web data security through HTTPS protocol, easy interactivity, accessibility and robustness.

With regards to system security, it is worth emphasizing that the captcha resource was used to avoid frauds (anti-robot function) in the voting screen, as well as a secure HTTPS system and certified digitals in the servers where the application was hosted.

3.2 Methodology implementation

The Digital PB project was divided in three moments: the pre-voting period, the voting period and the post-voting period, each one of them detailed below.

Pre-voting period

This period had three great marks, which are the selection of constructions that would be put to vote; the development of TIC tools and the establishment of partnerships; and publicizing the constructions to the population.

First of all, the government realized a pre-selection of 63 endeavors, seven in each one of the nine administrative districts in the city, according to criteria of social scope and relevance. After that, the COMFORCA (commissions formed by community leaders of each district, which follow and oversee the execution of the Participative Budget) were consulted for choosing 36 construction works, four per district, who would be submitted to vote. Contemplated in these constructions are the urbanization and renovation of avenues, construction/reform of leisure and cultural centers, and health center reforms, among others.

Correspondingly, partnerships were established for the project, among which began the partnership with the Regional Electoral Court. This Court provided the City with a database of all the voting population of Belo Horizonte. This database made it possible to create a solution based on the rule that limits voters to one single vote in each district, according to its voter registration; this provided more control, security and transparency to the voting process.

From the beginning of the second semester of 2006, the web system was developed for the publicizing and voting of the 36 pre-selected public construction works. By means of this system, the city's population could have access, in detail, to the information of 36 constructions, all of which have a great impact on Belo Horizonte; its responsibility is therefore to choose nine endeavors (one in each of the nine city districts) to be executed by the City.

Voting period

During the voting period, for those who did not possess Internet access, the City of Belo Horizonte installed 158 public and free voting stands in infocenters, schools and administrative agencies in all of the city's districts, with the presence of monitors to assist the citizen who was otherwise unfamiliar with the computer. Portable booths with various computers connected to the Internet were positioned in strategic places in the city during the voting period.

It is interesting to emphasize that the voting of Digital PB construction work gained so much ground that, in many locations, the community and companies installed, autonomously, voting stands; furthermore creating websites for publicizing and campaigning certain construction works, distribution of fliers in the streets, mobilizations, etc.

Simultaneously, the City launched a campaign on TV, Internet, radio, billboards, and bus advertisements in order to further stimulate political participation. Such parallel strategies are very important for the consolidation of the process. At the end of the voting process, the level of political participation in Belo Horizonte overcame the expectations, as can be seen by the data below:

- Number of voters – 172,938 (which corresponds to about 10% of the city's voting population).
- Number of votes – 503,266 (a citizen could vote up to nine times. The possibility of one vote for each district, with each district having four competing public constructions, was considered. Thus, each citizen could choose up to nine public works).
- Average votes per voter – 2.91 (the voters tended to vote more in the construction works of their region/district and less in other regions)
- Number of messages in the "Forum" – 912

- E-mails sent to “Contact Us” – 951

As a way to protect the transparency and control of the process, the individualization of votes was not held. Therefore, the profile of each elected person was not known and the vote was secret. It is important to emphasize that such information is part of the Regional Electoral Court’s database.

It is worthwhile listing the public constructions that won most votes in order to show their diversity:

- Barreiro Region – Implementation of a Sports Complex
- South-Center Region– Renovation of Praça Raul Soares (a square that holds a relevant historical significance for the city) and surroundings
- East Region – Renovation of the Medical Station
- Northeast Region – Linking the North and Northeast Regions (bridge construction and complementary construction)
- Northwest Region – Construction of a Hostel
- North Region – Construction of a Multiuse Cultural Center
- West Region – Implementation of a Medical Specialty Center
- Pampulha Region – Construction of an Ecological Park
- Venda Nova Region– Construction of an Ecological Park

Post-voting period

The nine endeavors chosen by the population of Belo Horizonte started to compose the City’s construction planning, and its execution estimated for the next two years.

The City Council of Belo Horizonte’s initiative of the Digital Participative Budget was approved by its government and population. In relation to the government, the General Auditor certified the reliability of the solution, ensuring transparency and security to citizens. The population met the administrative expectations, participating actively and taking the decision collectively. It is interesting to observe that the Digital PB stimulated the creation of collective and individual campaigns in favour of the works under discussion.

Data Access

Since the publication of the PB Digital website, 195,077 visits were registered up to the voting period, coming from 50 the countries highlighted in the map below, covering all five continents.



195.077 visitas vieram de 50 países/territórios

Figure 4: Countries that access the PB Digital

Fonte: *Google Analytics*. Acessado em 01/03/2008.

Surprisingly, access to the system exceeded the boundaries of Belo Horizonte. In Brazil, 24 out of 27 Brazilian states registered access. Other than Brazil, where the largest visitor concentration (193,527) logically occurred, the following visits were also registered: 1,077 from the United States, 126 from Portugal, 90 from France, 87 from Germany, 82 from Spain, among other countries. This shows that the experience of Belo Horizonte exceeds geographic limitations, generating worldwide interest in this political practice. The impact of this innovation can also be noticed by the various contacts and visits that the City has received from other cities and educational institutions that seek more detailed information about the Digital Participative Budget.

It is expected that this experience can serve as a trigger for other initiatives involving popular consulting initiatives in the sphere of Belo Horizonte. In this regard, the City Council of Belo Horizonte recently launched an Internet survey so as to collect the opinion of the city's inhabitants on whether shops should be open on Sundays and holidays. Participation in this survey was successful, despite being simple. Another aim is to contribute to the enhancement of discussions and to the implementation of concrete participative democracy practices in other governments.

The large participation registered in the first edition of the Digital PB brought a great challenge: how to expand even more the participation and discussion of the public construction work in the new edition, which will take place next November. For this new edition, citizens, instead of choosing a work in each region, will vote for only one, among the 10 largest investments demanded by the city. It is expected that the experience of the first Digital PB realized will allow this public policy of popular participation via Internet to acquire even greater relevance for people from Belo Horizonte and to become a common practice, as time goes by, in the interaction between Public Administration and citizens.

4 Conclusions

Due to the growing need to include every citizen in the digital world, it is advisable to map the languages used and accepted by the public in various means of communication, so as to improve interaction with the products offered by the government. The diagnosis of current participation initiatives and the citizens' true expectations converge on the need for an interactive environment. Digital inclusion will then be introduced in effect, considering not only the need for infrastructure but also facilitating active participation from citizens in the cyberspace. This paper discusses issues in the provision of e-Democracy, in particular in participative budget.

It is noticed that e-Democracy offers benefits for citizen and government alike. The citizens can assume a more active role in society, exercising their opinion power with ease and agility. Therefore, the digital revolution means more power for the people. For the government, unable as it is to turn its back on digital society, e-Democracy allows administration gains, transparency and more control over society through Internet-centralized data.

Using web-based Technologies and rendering possible a real citizen participation in the governmental questions is propitiating one Strong e-Democracy model with consensus, public debate, opinion-making, interactivity and discussion.

The participative budget proposal discussed here received the public administration's and population's approval. As for the government, the General Auditor guaranteed that it was trustworthy, attesting to its transparency and security. The population matched up to the administrative desiderate, participating actively and reaching a decision collectively. It is interesting to note that the Digital PB estimated the creation of collective and individual campaigns in favour of the works in debate. The strategies of winning voters for the preferred projects are varied, including the production of websites, advertisements and fliers, as well as face-to-face conversations in the streets.

A challenge of an e-participative environment such as this one is the extension of the scope of discussion. In this way, a good use of registered information, for instance, is in the forums, which could be better exploited since they contain additional information about community needs regarding the public works.

A user satisfaction study, by means of public research, will be conducted in view of offering improvements to the environment. Soon the next edition of the Digital PB will be initiated and will hopefully be as successful as this first version, increasing political participation in the definition of public policies in the municipal level.

Acknowledgements

We would like to express thanks to Marina Pombo de Oliveira and Vinicius Carvalho Pereira for the contributions regarding the translation of this paper.

References

- [As01] Astrom, J. Should democracy online be quick, strong, or thin? *Communications of the ACM* 44,1, 2001, pg. 49-51.
- [Be07] Belo Horizonte. OP Digital. Assessed in November 2007. Available in [http://opdigital.pbh.gov.br /in Portuguese/](http://opdigital.pbh.gov.br/in/Portuguese/)
- [Ca64] Catlin, G.E.G. *Tratado de Política*. Rio de Janeiro: ZAHAR Editores. 1964. 489 p. /in Portuguese/
- [GMP05] Garcia, A.C.B. Maciel, C.; Pinto, B.P. A Quality Inspection Method to Evaluate E-Government Sites. *Electronic Government*. In M.A. Wimmer et al. (Eds.): *Proceedings of the International Conference on Electronic Government EGOV2005*, 4, 2005, Copenhagen, Dinamarca. *Lecture Notes in Computer Science*, V. 3591, p. 198–209, Berlin Heidelberg: Springer-Verlag Ed., 2005.
- [GPF05] Garcia, A. C. B.; Pinto, F.; Ferraz, I. N. Eletronic Participatory Budgeting (E-PPB): increasing people participation in the decision-making process. *International Journal of Web Based Communities IJWBC*, Inderscience, v.1, n. 4, p. 504-517, 2005.
- [LC07] Lourenço, R. P.; Costa, J. P. Incorporating citizens' views in local policy decision making processes. *Elsevier: Decision Support Systems* 43, 4 (Aug. 2007), 1499-1511. 2007.
- [MNG05] Maciel, C; Nogueira, J.L.T; Garcia, A.C.B. An X-Ray of the Brazilian e-Gov Web Sites. *Human-Computer Interaction, INTERACT2005*, 13, 2005, Rome, Italy. *Lecture Notes in Computer Science*, V. 3585, p. 1138 – 1141, 2005.
- [MG07] Maciel, C., Garcia, A.C.B. Design and Metrics of a ‘Democratic Citizenship Community’ in Support of Deliberative Decision-Making. In M.A. Wimmer, H.J. Scholl and A. Grönlund (Eds.): *Proceedings of the International Conference on Electronic Government, EGOV 2007*, 6, *Lecture Notes in Computer Science*, V. 4656, pp. 388–400. Berlin Heidelberg: Springer-Verlag Ed., 2007.
- [OV04] Oostveen, A; Van den Besselaar, P. From Small Scale to Large Scale User Participation: A Case Study of Partipatory Design in e-Government Systems. *Proceedings Participatory Design Conference 2004*. Toronto, Canada. ACM, 2004.
- [PC05] Price, V., Cappella, J. Health care, i.t. and e-government: Constructing electronic interactions among citizens, issue publics, and elites: the healthcare dialogue project. *ACM International Conference Proceeding Series*; Vol. 89. pp. 139-140, 2005.
- [UK02] UK. In the service of democracy, a consultation paper on a policy for eletronic democracy. Acesso em 22/02/2005. Available on <http://www.e-democracy.gov.uk/downloads>. 2002.
- [Wo00] Wolton, D. *Internet: petit manuel de survie*. CNRS/França. Paris, Flammarion, 2000.