Alexander Prosser (Ed.)

EDEM 2011

Proceedings of the 5th International Conference on E-Democracy

8. – 9. September 2011, University of Economics and Business, Vienna

© Österreichische Computer Gesellschaft 2011
Contents

Mobile Government Promotes E-Democracy ......................................................... 11
Roland Traummüller

eParticipation in Administrative Procedures ...................................................... 25
Alexander Prosser

A Next Generation Governance Model for Public Service Delivery ..................... 33
Sotiris Kousouris, Panagiotis Kokkinakos, Dimitrios Panopoulos,
Yannis Charalazidisi, Costas Koutrasi, Dimitrios Askounis, Ydha Taher,
Willem Jan van den Heuvel

Implementing the ECI: Challenges for the Member States .................................. 45
Robert Stein, Gregor Wenda

Evaluating E-Participation Projects in Austria - A Methodological Approach
for a Decision on the Success of E-Participation ............................................. 53
Christine Leitner, Robert Müller-Török

The Political Market and Application of the Internet ....................................... 67
Magdalena Muial-Karg

Content Analysis of Australian Tourkm Facebook Page:
A Case Study of Government Use of Social Media ........................................... 77
Sultana Lubna Alam, Aodah Diamah

Deliberativeness and other important characteristics of e-Participation ................ 89
Cyril Velkano

Guarantor E-Voting System: Convincing the Electors in Election Transparency ..... 101
Sergey Ablameyko, Nikolai Kalosha, Sergey Bratchenya, Vitali Lipen

Towards a Collective Verified Recounting Solution in E-Voting ......................... 111
Alexander Schidl

Identification in Paper-based and Electronic Democracy Processes - A Comparison 121
Robert Müller-Török

Verbesserte eParticipation durch Usability von Electronic
Government Systemen bei Älteren ......................................................... 129
Tamas Molnar

Towards a Participatory Society. A Socio-technological Approach
to ICTs and Participation ........................................................................... 135
Ursula Maier-Rabler, Stefan Huber
GUARANTOR E-VOTING SYSTEM: CONVINCING THE ELECTORS IN ELECTION TRANSPARENCY

Sergey Ablameyko, Nikolai Kalosha, Sergey Bratchenya, Vitali Lipen

Abstract
Characteristics of different types of electoral technologies are considered, as well as the effects of their implementations in different countries. A new approach to organization of election events based on a system of external monitoring of elections is proposed. Model implementation of the servers and the web portal of the proposed 'Guarantor' system is presented, as well as the results of an ongoing effort to create a complete prototype of an Internet voting system.

1. Introduction

Looking through scientific papers and conference presentations of 2000-2005 one can see optimistic expectations that the developed countries will soon switch to e-voting and voting over the Internet (i-voting). Yet, despite the efforts of many researchers, engineers and politicians, more recent publications indicate that citizens of many countries are becoming increasingly apathetic towards elections in general and that e-voting didn’t become as widely adopted as expected due to various reasons.

Electronic voting was a definite success for less developed countries with poor infrastructure, such as Brazil, India, Bangladesh and others. Portable voting tablets can be carried by election officials even to the most distant villages, accumulating votes. This approach certainly proved itself cost-efficient, yet introduction of new technologies did nothing to improve the transparency of the elections. Many specialists have remarked that the intermediate results can be easily tampered with by the officials supervising the voting or after they’ve been collected.

In the US individual states choose their own voting technologies, which range from paper ballots and polling station machines like Diebold’s Accuvote to online voting. Yet the recent emergence of “Trust the evote” project (http://www.trustthevote.org/) indicates that many problems stand in the way of universal adoption of e-voting. Finally, we should mention Ireland, the Netherlands and Germany, where e-voting was approved but not accepted.

1 Belarusian State University, Nezavisimosti av. 4, 220030 Minsk, Republic of Belarus
2 Institute of Mathematics, National Academy of Sciences of Belarus, Surgazova 11, 220072 Minsk, Republic of Belarus
3 Institute of Informatics Problems, National Academy of Sciences of Belarus, Surgazova 6, 220012 Minsk, Republic of Belarus
post-soviet countries, we would like to mention the example of Kazakhstan, where the president Nursultan Nazarbayev supervised the development of “Sailau” electronic voting, which was subsequently approved and used at many of the Kazakh polling stations. However, with e-voting as well, and in a recent interview [7], the Russian President Medvedev has confirmed his intention to replace paper ballot voting by a modern e-Voting system. Yet the biggest step forward was made in Estonia, where every citizen was issued an ID card that can be used for remote authentication and generation of digital signatures. A new ID card was developed as well, and the number of its users has been steadily growing from 317 in 2005 to 140,846 out of 913,346 today). Still, most of the voters preferred to use paper ballots, and polls have shown that many electorates think that the Estonian e-voting system does not guarantee vote secrecy and fairness of the elections. Several Estonian activists have spoken of e-voting in the press. They call e-voting a form of i-voting in the area of e-Voting, has harshly criticized the Estonian e-voting protocols developed in [9], of the approach can be also found in [8], where it is emphasized that personal ID cards n’t be used in e-Voting protocols due to public concerns about vote secrecy. Similar results are observed in Kazakhstan, where only 14% of the voters chose electronic voting instead of paper ballot.

up to the reconciliation of the electorate to electronic and internet voting should become an object of interest to e-voting experts. The authors will attempt to analyze the i-voting protocols developed in a and Austria, indicating the stages that may cause mistrust. A comparison with the earlier systems (such as Sailau) will be made, and both new and old ideas that are the foundation of the e-voting system being developed by the authors will be presented.

uses with existing voting technologies in troubled countries

ite easy to imagine the factors that define the peoples’ attitude to the institute of elections in local countries ruled by authoritarian dictators or a single dominant political party (such as post-Soviet republics, countries of Northern Africa, Central Asia etc.). The less educated part of the population will generally trust the official propaganda, voting for the current government by the socially active and politically educated citizens, seeing the evidence of fraud during elections, will often demonstratively ignore elections, becoming apathetic to political life. These people are well aware of the methods that can be used by state-appointed election officials to influence local election results, as well as the instances when local government officials are reprimanded or even fired from their jobs because of unfavorable election outcomes. This knowledge leads to the obvious conclusion that local election committees have both the opportunity to commit election fraud and a strong motivation to do so, making foul play at the polls a near certainty.

uld be noted that many democratic instruments such as “primaries”, polls, free debates on
ion and in printed media, collection of signatures in support of petitions or collection of exit
atae are either unused or similarly controlled by the governments of troubled countries. Some procedure that doesn’t protect the respondents’ anonymity is affected by the “X-factor of the displeasure of the government or local authorities. This becomes evident, for example, during the nomination of presidential candidates, when many citizens express concerns about supporting an opposition candidate.

Troubled countries usually hold elections using traditional paper ballots. The ballots are marked by the elector and cast into sealed receptacles to be subsequently counted by local election committees. As stated in the report [11], the only issue arising during traditional voting is long-established democracies are ones related to the tediousness and inefficiency of the procedure. In troubled countries, on the other hand, the biggest problem of traditional paper ballot voting is the lack of transparency and susceptibility to fraud, as evidenced by routine post-election protests.

Neither winners nor losers of election events held by using paper ballots can prove beyond reasonable doubt to the society, media or an impartial court if the data gathered by local election committees (which is eventually aggregated to determine the nationwide election outcome) was accurate or falsified. Indeed, the election protocols are signed by heads of local election committees which answer to local administration; there’s no guarantee that the ballots have been marked by electors themselves, and the signatures supposedly left by the voters during registration could just as well have been falsified, whilst at the same time a number of ballots has been “thrown in” by the election committee. This type of fraud cannot be discovered by mandated procedures for verifying the election results, such as recounting the ballots.

It must be noted that despite the widespread expectations to resolve the issues identified with traditional voting by implementing electronic voting protocols, the actual results of introducing electronic elections are not entirely encouraging. Despite quick acceptance of electronic voting in USA, Canada, Australia, India, Brazil, Venezuela and several other countries, Ireland, the Netherlands and Germany have halted their e-Voting programs.

It is interesting to note that despite public concern about vote secrecy many e-Voting protocols feature the same immediate depersonalization of votes as during traditional voting, leaving no opportunity to demonstrate to an individual voter that his choice has been properly recorded. Another major issue with current protocols is the impossibility of post-election audits or recounts of votes, raising questions about legality of electronic elections. For a recent example, one can look at the Austrian student elections of 2009 [10], which were later declared invalid [13]. The situation is analyzed in depth in [2, 3]. An in-depth analysis of implementations of e-Voting in developing and transitional countries can be found in [5], and proposals toward trusted voting can be found in [12].

3. Possible reasons for mistrust in e-voting and the proposed solutions

Let us list the possible reasons why many of the developed e-voting and i-voting systems were unsuccessful.

1. New voting technologies are very often introduced by the ruling power in an attempt to increase the efficiency of elections or to maintain the image of their country being technologically advanced. In the transitional countries, this immediately seems suspicious to the political opposition, leading to claims that new technologies are introduced to better control election results and to spy on the citizens.

The proposed solution is development and assessment of voting systems by independent researchers and their certification by reputable international organizations. Elections in troubled countries could even be held using portable equipment and servers controlled by one of such organizations. In turn, the organization would legitimize the election results.
Network authentication using ID cards and digitally signed votes can lead to the voters at vote secrecy having been compromised.

To alleviate this problem would be using one-time authorization codes in place of ID cards events, as well as clearly separating the authorization and the casting of votes. The fact that several time-limited codes would be issued and displayed to a voter upon $\alpha$, allowing him or her to use any of them for casting the vote, possibly using a different

casting leave no paper trail. A 100% guarantee that a system is free of programming flaws was the deciding reason in the decision of the German court that electronic elections are secure. The proposed answer is to replace immediate depersonalization of votes by hidden allocation, issuing each of the voters a code that can be used to verify the vote. Thus, the in become transparent to the individual electors as well as observers.

It is also proposed to introduce, in addition to the electorate and the various election results, an outside system of election monitoring acting as a trusted third party. The system would include the following:

- forming the necessary cryptographic routines during the elections;
- ceasing of a request to hold an election event;
- allocation of secure identifiers (SID) for all electors;
- sending of the information on the subjects of the voting;
- port of the receiving station and on-line voting;
- selective collection of local personalized results from standalone polling stations;
- playing of the results of an election event on the web-portal, including the individual results in personalization that can be verified by the electors.

The responsibility for aggregation of voting event results is shifted from election committees to an automated system of monitoring and supervision that can be certified both by the state and independent specialists. In addition, both electors themselves and remote election can use the web portal to monitor the collection and aggregation of votes. The results of a event are then accepted if no protests have been raised during a certain period of time or if a satisfactory response to such protests was given by the administrators of the organization holding the election event. This approach is similar to the principles of major sports events, where certified automated systems are used for the performance of the contests and displaying the intermediate and final results in on the “Guarantor” system or its analogue in the electoral process as the trusted third party.

The principles of trusted elections using the ‘Guarantor’ system

The proposed system is based on the authors’ previous experience in developing electronic voting technologies for emerging democracies. Notable developments include the mock-up designs of electronic polling stations made for the Central Election Committee of Belarus as well as development of the prototype of “Sailas” election system currently used in Kazakhstan [3]. The principles used in designing the latter have been patented [6].

In the previous year the authors have finalized the development of the complex of equipment to be used at the polling stations in the proposed voting system. The complex has been approved and can be manufactured on demand [4]. It is designed to be fully integrated with the ‘Guarantor’ system, employing the same authentication procedure based on SIDs and personal data and the ‘hidden’ personalization of votes by a vote confirmation number (VCN). Presented below in Fig. 1 is the approach to verifying events described in [1] that supports voting at polling stations, over the Internet, by mail and by SMS. Authentication of voters, as well as collection and aggregation of votes, is facilitated by the ‘Guarantor’ servers, allowing for centralized publishing of election event results and individual vote verification.

![Figure 1: Structure of an integrated state-scale voting system](image-url)
The authors have focused their attention on Internet voting, considering that it's currently used by over 4 million Belarusians (even if you consider the public Internet access by schools and post offices) and that a wide-scale approval can be organized easily over the Internet. Similar advantages of Internet voting have been pointed out in an article [7], which contains a number of proposals for the president of Russia Dmitry Medvedev concerning reforms of the election system. The authors feel that it is important to have a system ready in short order so that its advantages can be directly the technologies that will be developed by our Russian colleagues.

\textbf{Guarantor} system

\begin{itemize}
  \item Cryptoserver
  \item Database
  \item Web portal server
  \item Casting server
  \item Front-office
  \item SMS server
  \item Mobile network
  \item Election event organizers
  \item Database of personal details
  \item Distributor of secure identifiers
  \item Elector groups
\end{itemize}

\textbf{Internet}

\textbf{Back-office}

\textbf{Figure 2: Internet voting using the ‘Guarantor’ system}

A key feature of the proposed voting system is the mechanism used to authenticate the voter. Our proposal consists of using personal data in conjunction with SID (secure identifier) IDs to the voters in confidence before the election. A detailed description of SID in can be found in [1]. To briefly describe the properties of SID, we will note that each SID is formed as \( SID = EID, \oplus F_{\text{crypt}}(EID, K, R) \), where \( EID \) is a unique number identifying the voter, \( \oplus \) is the concatenation operator, and \( F_{\text{crypt}} \) is a secure cryptographic function taking as input the identifier \( EID \), the secret key \( K \), and a randomly generated number \( R \), which is sent to the database accessible only to the cryptoserver. The function \( F_{\text{crypt}} \) is designed so that generation of valid SID requires not only the knowledge of the secret key \( K \), but also the random numbers used in the procedure and thus access to the database storing these numbers.

These properties make generation of counterfeit SID (S) impossible. At the same time, secrecy of SIDs is only essential before voting has ended. After the voting server has been closed and the results of the election have been published and made final, it is possible to allow public access to the cryptoserver, the key \( K \) and the database of random numbers \( R \), so that every remote observer can verify that only valid SIDs have been used in the voting.

Presented in Fig. 2 is an outline of the interactions between the subjects of the electoral process with the ‘Guarantor’ system acting as the trusted third party.

Stages of election events using the ‘Guarantor’ systems can be formally described as follows.

\textbf{i. Pre-election stage.}

Input: complete information about the election event, personal data of the voters.
Output: credentials for managing the election event.

At the pre-election stage, the organizer of the election event uses the administrative interface of the ‘Guarantor’ system to create a new election event and to submit the complete information about the event and the personal data of the electors. He then receives the login and password valid for managing the election event.

\textbf{ii. Preliminary stage.}

Input: confirmaton of the data input during the pre-election stage.
Output: a set of SIDs used for voter authentication.

The preliminary stage of the election event is started immediately after the information gathered in the pre-election stage has been processed by the ‘Guarantor’ system. A web portal of the election event is created, containing the information about the election event. The organizer reviews the web portal and authorizes publishing it online. From this moment the information about the election event becomes accessible to the public and is recorded by the voting server.

At the same time, a request is placed for the cryptoserver to generate an SID for each of the electors. The generated SIDs are assigned to electors and delivered to them in confidence.

\textbf{iii. Voting stage.}

Authentication/registration server input: SID.
Authentication/registration server output: randomized voting token and password.
Voting server input: randomized voting token and password, vote.
Voting server output: confirmation that the vote has been received.

Voting begins and ends at a specific time set by the organizer of the election event. In order to place his or her vote, the voter must perform the following steps:

1. Input the SID received at the preliminary stage using the web interface of the authentication/registration server. The SID is sent to the cryptoserver for verification. If the SID
It must be noted that in the proposed system every honest voter can use the RVT used for voting to ensure that his or her vote has been tallied correctly. Unfortunately, unless every vote is accompanied by an elector’s electronic signature, it is impossible to prevent dishonest voters from claiming that the system doesn’t work as intended. However, the authors believe that such dishonest voters will be a small minority, and that their efforts will be wasted. After all, unlike the case of traditional paper ballot voting, every honest voter can use his RVT to see that the vote has been properly recorded, and every honest elector who didn’t vote can verify that his or her SID has not been captured by the authentication/registration server.

5. Conclusion

The main concern of the authors is that despite giant advances in information technology, paper ballot voting remains as the primary (or the only) mode of voting in most of the countries of the world. Numerous well-known and well-documented techniques of committing fraud during paper ballot elections are a major reason why citizens of developing countries and emerging democracies lose their faith in elections, leading to either elector apathy or the opposite effect: anger at the ruling government manifested in various forms of civil unrest. In many countries it has become customary for the losing side to declare the elections fraudulent after the results have been announced, rallying their supporters for actions of mass protest. It is characteristic of paper ballot elections that nobody, including the ruling government, is aware of the exact extent of the machinations and, consequently, the true results of the voting. This situation leads to political instability, delegitimization of the government in the eyes of the citizens and, ultimately, doubts in the very principles of democratic government.

The proposed alternative is the use of modern transparent electronic voting technologies specifically designed to address the issues that have become identified with traditional technologies. The authors realize that they don’t have the manpower or the resources required to develop a working state-scale election system based on the principles outlined in the paper. Nonetheless, it is our hope that the presented ideas and the prototypes that have been developed will lead to a joint project by various IT experts to create a pilot e-Voting framework that would fully comply with the OSCE requirements and which could be approved under international supervision. It is our firm belief that realizing the proposed ideas could benefit not only the troubled countries of Africa, Asia and Middle East, but also the ex-soviet countries and even the countries of the European Union where use of electronic voting has been limited or banned legally (Ireland, the Netherlands, Germany) or where electors have shown mistrust or lack of interest in electronic voting (Estonia, Austria).

The presented internet voting system incorporates numerous new approaches to internve voting. Key advantages of the proposed approach compared to existing e-voting technologies include:
- it is an independent Internet-based e-Voting system not affiliated with any corporate body or a single government;
- vote secrecy is guaranteed through independent interaction with the server performing authentication/registration and the server receiving the votes;
- compiling each stage of the voting process results in immediate feedback from the system;
- intermediate and final results are published at a web portal, which also supports individual vote verification through hidden personalization;
- final results of elections are based not on the whims of election committees, but on a consensus of election organizers, voters and independent observers.
Currently the proposed system is available as the early prototype hosted at http://e-vote.basnet.by. The authors would welcome any comments or suggestions as well as proposals for joint testing of the system at small-scale election events.

5. References


1 University of Economics and Business, Vienna

Abstract

This paper gives an introduction into an approach to increase the trust in e-Voting solution based on an independent recount which is called "Public Source Counting ready-to-use. Thereafter this paper shows a refinement and revision method that is made community-based. This report also tries to point out the benefits of such verification. The main objective is to receive a fully verified, i.e. proved and not only The difference between testing and proving will also be shown.

1. Introduction

It seems obvious that such an important democratic right like the right to vote must and guaranteed to be general, free, personal, secret, equal and auditable [6, p.66 ff]. These basic principles must also be true for an electronic vote. Unfortunately, e-Voting some problems, especially with a view to traceability and auditability, in the recent past have caused some controversy. In the UK in 2007, staff manually had to edit not encrypted ballots in order to ensure into the counting application [9][17]. It is apparent that this should not be the normal way of audibility or transparency. In Finland in 2008, more than 200 votes disappeared had to be repeated on paper [18]. All these votes were regional elections. In the Austr Union of Students election in 2009, there were wrong or missing parts of affiliation as to a dispute [1].

What such developments have shown is that there is a common denominator - a loss order to re-establish this trust it is necessary to mention some key elements.

Prosser points out such elements of a successful, i.e. auditable, e-Voting system. Thus independent verification of the voters right to vote, anonymity must be guaranteed, voting, control by the election commission and an independent recount [12].

A computer program that supports such an independent recount could offer an addle keeps the necessary rules, i.e. its workflow must be transparent and thus retraceable. It would be that the whole program is verified so that its methods are proved. A verifies simple testing, e.g. random test cases, but a procedure of proving the workflow with mathematical rules.