Assessing the usability of open verifiable e-voting systems: a trial with the system Prêt à Voter

Marco Winckler, Regina Bernhaupt, Philippe Palanque
Institute of Research in Informatics of Toulouse (IRIT) – University Paul Sabatier
E-mail: [winckler, palanque, bernhaupt]@irit.fr

David Lundin
University of Surrey (UK)
E-mail: D.Lundin@surrey.ac.uk

Kieran Leach, Peter Ryan
University of Newcastle (UK)
E-mail: [kieran.leach, Peter.Ryan]@newcastle.ac.uk

Eugenio Alberdi, Lorenzo Strigini
Institution/Affiliation: City University (UK)
E-mail: [eugenio, strigini]@csr.city.ac.uk

Abstract

E-voting systems – the combination of vote-casting, ballot transmission and counting, auditing and monitoring systems – have been gaining much attention from the international community as a suitable solution for preventing errors issued from human reliability on vote counting. Whilst many reports have said about currently available pilots and proposals are sensible, some fundamental issues remain unresolved such as the fact that most of systems are unverifiable by voters, candidates and returning officers. In most proposals, votes disappear into the machine so that it is impossible to audit votes without removing the secrecy of votes.

In more recent years, an electronic voting system called Prêt à Voter has been developed to allow verification of individual casts and audit elections. Prêt à Voter combines paper trail for recounts and a sophisticated cryptography mechanism to ensure secrecy of votes and vote verification. However, as any other e-voting system, the user adoption and the user acceptance of Prêt à Voter not only depend on how technically sound the system is but also how voters perceive the system as trusted. Despite the fact Prêt à Voter has been designed to make the voting process as simpler as possible the introduction of online encrypted vote verification is an unnatural concept for most voters and may affect user’s opinion.

This paper reports some observed user behavior faced to the introduction of new voting system including cryptographically vote verification. In particular, this paper presents the results of a large scale trial with the system Prêt à Voter. We describe some usability problems related to user behaviour that may affect the reliability of E-voting procedures and (by the means of questionnaires specifically designed to assess of user acceptance and user adoption) we collected voters’ opinions about their experience using individual
vote verification. These results are compared with other studies with similar electronic voting systems, which allow us to draw out some recommendations for assessing the usability of E-voting systems.

**Key Words:** e-voting, user acceptance and adoption, usability studies, Prêt à Voter.


1. **INTRODUCTION**

In the last years electronic voting systems (e-voting systems) gained much attention from the international community as a suitable solution for preventing errors issued from human reliability on vote counting. After some successful experiences in many non-governmental elections, many countries are conducting experiments in political areas as well (Geser, 2002). However, the reliability and trustworthiness of E-voting systems is still subject of debate and controversies that slow down the large adoption of such systems (Bryans et al. 2006). Several causes of fraud and misconduct in e-voting systems have been decreasing the trust in e-voting systems (Kocher and Schneier, 2004). As a consequence, many people might accept and use e-voting systems, but they have some doubts about privacy, security and accuracy of the e-voting due to the lack of verification and validation processes (Centinkaya and Centinkaya, 2007).

In order to increase acceptance of e-voting systems, recent research efforts have focused on building trust models for making such systems auditable (or verifiable) so that all actions taken during the elections can be inspected and verified by everyone (Prosser, 2007; Antoniou et al., 2007). Most of current development involves some kind of cryptographic protocol to ensure basic requirements such as privacy (i.e. no link can be made between a vote and a voter) and accuracy (i.e. no vote can be altered, deleted or invalidated) (Adida and Rivest, 2006; Chaum, 2004). However, little is known about how users perceive the introduction of the cryptographic protocol that allows the vote verification.

When investigating how voters perceive new forms of e-voting systems including cryptographic protocols several factors have to be taken into account. First e-voting systems are a (new) form of information and communication technologies (ICTs) that users are confronted with. Thus work on the acceptance of new forms of ICTs seems relevant to be considered. The area of Human-Computer Interaction (HCI) has been focusing on usability aspects of systems, comparing various forms of election methods in terms of perceived usability, but also in terms of error rates and vote completion time. From the technical perspective usage of cryptography introduces the aspect of security and reliability of the system, and how voters perceive the security and reliability of a system (not being informed about technical details).
Hereafter we report the results of an empirical study using the system Prêt à Voter (Chaum et al, 2005). Prêt à Voter belongs to a category of E-voting systems that are designed to deliver better privacy and accuracy than paper-based elections without requiring the certification of large quantities of voting equipment, that is, by verifying the election rather than the computer system. They achieve this through a high degree of transparency, using a combination of cryptography, monitoring and auditing (via the Web) to ensure privacy while detecting vote tampering. This paper describes some results of the research activity conducted for AROVE-v, a research project developed within the European Network of Excellence, RESIST. The scope of RESIST was the “resilience” of complex socio-technical systems, of which e-voting is a representative example. One of the main goals of AROVE-v was to identify the necessary components of a case supporting the use of a particular e-voting system (Prêt à Voter) from the viewpoint of resilience, and recommend methods for establishing the necessary evidence. The study described here was conducted to obtain part of this evidence, in particular, evidence concerning the usability and acceptance of Prêt à Voter.

2. STATE-OF-THE-ART ON E-VOTING SYSTEMS

The term electronic voting (e-voting) covers a wide range of systems, encompassing any and all systems where some part of the process is carried out electronically. These systems include remote voting systems, where an individual will cast their vote remotely via some electronic means, most commonly via a computer connected to the Internet. These systems can be discounted here, as the intent is to analyze those systems which are used in a traditional polling station.

2.1. Review of Open-Verifiable E-Voting Systems

Within the realm of e-voting systems there is a movement towards requiring such systems to be end to end verifiable. Such systems should be able to provide a high level of assurance that the results of an election correctly reflect the summed intentions of the voters taking part. This generally requires that any individual voter be able to confirm the correct recording of their vote, albeit without any possible breach of the secrecy of their vote. Most traditional approaches to this problem involve placing significant trust in the technology, mechanisms or processes. Thus, for the traditional paper ballot, the handling of the ballot boxes and counting process must be trusted, that the boxes are not lost or manipulated and that the counting process is accurate. Various observers can be introduced to the process which helps to spread the dependence but does not eliminate it (Chaum, 2004).

Many systems rely on cryptographic protocols to provide assurance along with secrecy, although systems such as ThreeBallot (Rivest, 2006) do not require cryptography. Whatever form this takes it can be expected to be a piece of paper representing some unique piece of information the voter will recognize as corresponding to their individual vote. This unique information can then be confirmed against a web bulletin board to give
the voter some assurance that their vote has been properly recorded. The level of assurance garnered is dependent upon the specific information recorded.

In a number of cryptographic, end to end verifiable voting schemes the voter is issued with some type of Voter Verifiable Paper Audit Trail (VVPAT) or Voter Verifiable Encrypted Paper Audit Trail. A simple form of paper audit trails was originally proposed by Rebecca Mercuri and is commonly known as a Voter Verifiable Paper Audit Trail (VVPAT). A direct recording electronic voting system using the Mercuri method for VVPAT (Mercury and Neumann, 2002) would print a paper record of each vote cast at the time of casting. This would be displayed to the voter under some form of transparent case to prevent tampering. If the voter accepts that the paper record properly corresponds to their chosen vote they signify this acceptance to the system and the record is added to other similar records in storage.

One of the few examples of open-verifiable e-voting systems using cryptography mechanisms is Prêt à Voter (Chaum et al, 2005). Prêt à Voter introduces a paper-based ballot form containing two halves to aid user recognition and simplify use. Each ballot form presents in a random order the name of the candidates. As depicted in Figure 1, the candidates’ names are on the left side and the grid boxes which the voter marks her choice are in the right side. Underneath this grid, also on the right hand side of the form, is printed a unique code, also called onion. This onion encapsulates the order of the candidate list in a number of germs, each hidden underneath a layer of encryption. To decipher this code, and thus determine the value of the vote, is required a key which is hold only by the official in charge of the elections or, for extra security, it can be divided among several officials and party representatives.

Figure 1. Prêt à Voter ballot form

As Prêt à Voter is the voting system of interest for our work, further details about it usage is presented at section 3.1.

2.2. Review on Usability Studies of e-Voting Systems

The evaluation of e-voting systems is a very complex task because there are several dimensions (such as system usability, user acceptance, trust and related concepts like
security, reliability and privacy) that count for the perceived quality of the systems (Carter and Bélanger, 2005).

The term **usability** is often used to describe the perceived ease of use and usefulness of the information technology systems. In fact, poor usability would increase number of errors, reduce tasks performance, increase frustration, and result in the system being used less than it could be (Peters, Janssen and van Engers, 2004). This might be even more critical if the system does not comply with accessibility guidelines (a sub-dimension of usability), now widely advertised, and even a mandatory requirement in many countries that have enacted rules for Accessibility responsibility of content on the Web (Winckler, Xiong and Noirhomme-Fraiture, 2007).

Several studies point out the importance of including the practice of usability evaluation for validating new e-voting systems (Herrnson, 2006). Despite the fact that there is no common agreement on what kind of usability evaluation method should be employed. Most people agree on large scale trials and the use of standard questionnaires like the System Usability Scale (SUS) (Brooke, 1996) for dealing with usability assessments. Usability evaluations have been mainly conducted for the US e-Voting systems. Everett et al. (2008) and Byrne et al (2007) have been presenting an extensive experiment comparing error rates, task completion time and perceived usability (measured using the SUS).

**User acceptance** can be defined as an initial decision made by the individual to interact with the technology and it is increasingly deemed to be a necessary condition for the effective implementation of any information technology project. A number of studies have investigated the adoption of e-government services in developed countries (Titah and Barki, 2006; Carter and Weerakkody, 2008). Studies on user acceptance are mainly based on technology acceptance theories and models such as Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh, 2003) which provide useful insights and implications for understanding an individual’s intention of using e-government services (Dadayan and Ferro, 2005).

**Trust** is also important for e-voting systems because it may influence citizens’ intention to use state e-government services (Tolbert and Mossberger, 2003). However, the concept of trust is hard to formalize as it raises philosophical and social concerns. It is widely demanded that e-voting systems should be secure and accurate (only legitimate voters participate, and only once; protected against fraud and mistakes), should protect privacy (the voter should remain anonymous), and should be verifiable (a transparent process, possibility of recounting). The overall debate of the literature focus on open-verifiable electronic system as a means to ensure transparency throughout the voting process and in the main belief is that in specific contexts a sufficient level of security could be achieved through physical and electronic procedures and standards (Altman and Klass, 2005). Despite extensive ongoing research in the development and analysis of trust models for dependable computer systems, there are only a few models describing trust management
in the domain of e-voting (Antoniou et al. 2007) and they have not been widely employed in empirical studies.

3. EVALUATION OF OPEN VERIFIABLE E-VOTING SYSTEMS

In this section we present the material and method employed to assess the open-verifiable e-voting systems called Prêt à Voter. This trial was run in May 2007, at Newcastle University using the system Prêt à Voter (Chaum et al, 2005).

3.1 Prêt à Voter at glance

Prêt à Voter is a cryptographic End-to-End voting system. It is based upon optical scan technology, with a part of the ballot form being scanned into the system with the voter in attendance. A voter fills in their choices on the right hand side of a ballot form which is perforated down the centre. Upon the left hand side is a randomly ordered list of the candidates taking part in the election. The voter then detaches and destroys the left hand side of the ballot form in order to destroy the candidate ordering information.

After destroying the left hand part of the ballot form the only store of the information remaining is in the cryptographically encrypted data underneath the boxes. This 'onion' has been encrypted with the public keys of a number of tellers, and will required that all tellers cooperate in order to decrypt this information and the close and tallying stage of the election.

The remaining part of the ballot is scanned into the system by polling station staff and the voter issued a receipt which indicates which boxes on the ballot form they filled in and also lists the cryptographic onion. There is likely also to be a serial number to assist in tracking the record of their vote online. This receipt is in effect a Voter Verifiable Encrypted Paper Audit Trail.

Following the issue of this receipt the voter can access a website which will display to them their record from the Web Bulletin Board (WBB), allowing them to assure themselves that their vote has been properly recorded. The WBB is not simply a display of the various recorded votes but is in fact the primary store and as all votes are encrypted it is possible to allow this to be publicly viewable.

3.1. Hypothesis

To evaluate the Prêt à Voter system beyond the technical feasibility (which will be reported elsewhere) we focused on the following dimensions that are typically referred to in the literature: trust and related concepts like security and privacy, usability of the system and overall acceptance of the voting method. To investigate possible dependencies we used the following working hypothesis:

*H1: The overall usability of the system must be high to favor usage of Prêt à Voter over other voting methods.*
H2: The higher the usability, the more people will accept the system.

H3: A high perception of security leads to a higher acceptance of the system.

To answer hypothesis one a comparison of the usability of the system with other systems that have been investigated by others will be performed. Hypothesis two and three will be investigated based on user’s perception of the system.

3.3. Method, Set-up and Procedure

To answer these questions a field trial was establish, which was set up in May 2007, at Newcastle University, during one day. The trial included a real-life voting: people were asked to volunteer to vote for a donation that should be given to one of the social institutions connected to the University of Newcastle. To evaluate Prêt à Voter in terms of usability and acceptance (reliability, trust, privacy) the real-life voting was accompanied by several methodological measurements:

- **Usability**: To understand to what extend people perceive the voting procedure as usable, we used the Standard Usability Scale (SUS) with 10 items, adapting the questions by replacing system with Prêt à Voter, and slightly rephrasing sentences to make them correspond to the voting procedure. Additionally we asked 5 questions directly related to the voting procedure (e.g. It was clear to me why I need to destroy half of the voting ballot).

- **User acceptance and Trust**: Based on the UTAUT model (Venkatesh et al, 2003) acceptance was evaluated in terms of performance expectancy, effort expectancy (ease of use), social influence and facilitation conditions. We additionally included questions on Security, Trust, Privacy and Usability. 49 questions were developed to investigate these factors.

- **Demographic data**: Age, education and voting experiences were asked for in the demographic questionnaire.

3.4 Trial Set-Up

The trial was set-up in a large university room with four different stations. Station 1 was the registration station and where the demographic questionnaire was filled out. Station 2 was the voting area, with large boards, explaining additionally the voting procedure with Prêt à Voter; while Station 3 consisted of several scanners for scanning the votes and verifying the used voting system (see Figure 2). Station 4 consisted of several PCs allowing each voter to verify the vote on the web. Questionnaires on usability and acceptance were filled out at station 4 (after the voting procedure).

**Figure 2.** Left: A participant during the voting procedure; Right: Scanning of the Vote at the voting area (Station 3).
Procedure

For the voting trial participants were recruited within the university by a combination of emails being sent through departmental mailing lists and volunteers encouraging individuals to participate and vote for a particular charity.

Each volunteer was asked to fill out the demographic questionnaire, and this took the place of presenting identification to prevent double voting in a genuine election. The participants were briefly explained that the voting procedure was different from paper and pencil voting, allowing them to verify their vote after the voting procedure and to also allow them to verify the voting procedure (printed voting cards). Figure 3 presents a sample of ballot forms used during the trial.

Figure 3. Samples of ballot forms used in the trial.
The voters were asked to vote for one of the charity organizations (i.e. Oxfam, Barnardos or UNICEF) by making a cross mark next to the name of the charity of their choice, in the location indicated. The paper used for voting is consisting of two parts, the left side with the random order of the charity organizations and the right hand side, used for voting.

Voting from the user perspective thus consisted of the following steps:

- The user votes putting a cross
- He splits the ballot form in two, the left hand side is destroyed, the right hand side is scanned
- A receipt (including a possible tracking number for web-site look-up) is handed over.

As described above the voter could also verify the voting process using his ballot form and also verify the vote using the Web Bulletin Board (WBB) available next to the voting room.

Additionally two observers noted problems and irregularities in the voting process during the trial.

**Participants**

105 people participated in the voting procedure, 100 people agreed to fill out the demographic questionnaire, showing an average age of 27.97 (SD= 10.5 N=100), where three participants were between 62 and 59 years, all other participants ranged between 43 years and 19 years. 96 participants stated their gender, 32 were female, 64 male.

42 participants had a High School Degree, 27 stated to have a University Master Degree, 19 a PhD and 8 people indicated other education. 6 participants said they had been never voting before, while 85 participants stated that they have been voting in elections using paper voting, 13 were familiar with electronic voting with pre-authentication, 3 used electronic voting without pre-identification, 31 indicated experiences with personal voting. 14 participants state other forms of voting, e.g. voting by raising hands, postal voting. Voters in the trial had on average been voting about 2 times in national elections (M=1.93; SD=2.77; N=100) with a maximum of 14 national elections. Additionally people reported that they had been participating in local elections on average 2.6 times (SD=4.24) with a maximum of 20 local elections.

Participants thus do represent a typical voting population in terms of voting behavior; they are not representative for the population in Great Britain.

**3.4 Results**

**Technical Evaluation**

There were some initial difficulties with the specific computer systems being used at the outset of the trial, which caused the start of the trial to be delayed by approximately two
hours. After these issues were resolved there were occasional sporadic issues with some of the scanners and those scanners which regularly malfunctioned were removed. After the malfunctioning scanners had been removed there were fairly few issues.

Some votes would fail to be properly read throughout the trial, however this was generally down to a failure on the part of the participants to mark a cross properly in the place indicated, and to fully cover the intended cross area.

No problems were had with the tallying of the results or with accessing and viewing records on the Web Bulletin Board.

Voting results was 51 to Oxfam, 29 to Barnardos and 25 to UNICEF.

105 votes were recorded.

**Acceptance, Trust and Usability**

People were free to fill out the final questionnaires. 70 participants answered the 15 questions on system usability, 53 participants answered the questionnaire related to acceptance.

The SUS questionnaire (10 items) shows that the usability of Prêt-á-Voter is in an acceptable range but could be improved. The SUS shows a mean of 68.5 (SD=17.8; N=65). For the five additional questions on the system, we asked people on a 5-point scale ranging from very much, quite a lot, partially, A little, to Not at all People reported that they understood the voting instruction (75.8%) compared to 24.2% reporting in the categories partially, a little or not at all. Why half of the ballot has to be destroyed was understood by 51.5%, 16.7% reported that the only partially understood, 10.6% reported a little and 21.2% (representing 14 participants) and nine participants did not understand at all. People felt reassurred when they saw the marks on the half of the ballot that kept coincided with the marks on the receipt (63.3%). The voting method was rated trustworthy by 53% (N=35), 18 participants reported that they found the system only partially trustworthy, and nine and four participants found the voting method a little or not at all trustworthy. In general people tended to feel confident using the voting method (48.5%), 30.3% partially, 21.2% a little or not at all.

Acceptance was measured in terms of trust, security, usability and reliability. The initial questions of the questionnaire were derived from the UTAUT model, but as some questions did not fit for e-voting scenarios they were omitted or changed. The validation of the original scales shows a Cronbach-alpha of 0.6 for the scales on security and trust, but did not show reasonable results for the other scales. The changes and adoptions made to original questions used in the UTAUT model thus resulted in loosing the original scales. A factor analysis did not show any sufficient outcome. Hypothesis 2 thus can not be answered based on the UTAUT factors as the factor analysis does not show clearly the original factors contributing to the questionnaire.
In terms of acceptance the system would be used by most participants in elections on national or local level (36.2% agree to use the system, 34.5% neither/nor, 29.3% would not agree to use), but preferably other types of elections (56.9% agree, 27.6% neither/nor, 15.5% do not agree). If the system acceptance can be increased by an increased usability has to be investigated in future studies.

Within the extended UTAUT model we added eight questions on security. Security seems to be measure independent of the other factors in the questionnaire. Security in general is perceived rather low. Asked on a scale ranging from 1 (very much agree) to 5 (do not agree at all) security was perceived as vulnerable. Asked if they think that Prêt à Voter is vulnerable to hackers, 41.5% agreed (categories agree and very much agree), 41.5% chose neither nor and only 17.0% reported that they think the system is not vulnerable (M=3.35; SD=0.96 for reversed item). Security might be an important aspect for the acceptance of the system. The role of security as a determining factor of acceptance of a voting method should be investigated in more detail for Prêt à Voter in a follow up study. Based on the current available data we found a positive correlation between the mean value for acceptance (based on 29 questions) and security (r=0.549, p=0.000).

4. INTERPRETATION

The SUS scores with a mean of 68.5 is below typically reported usability values for other forms of Voting. Everett (2008) report average SUS scores for DRE voting being 86.1 (SD=16.6) for Bubble Ballot 81.3 (SD=22.2) for Lever Machines 71.5 (SD=14.8) and for Punch cards 69 (SD=22.2). The usability of Prêt à Voter is thus lower than comparable voting systems in the US. Usability should be increased by extending the explanations of the voting procedure (half to the participants did not fully understand why the ballot has to be destroyed). Answering hypothesis 1 we have to state that Prêt à Voter does not reach the goal of providing a high usability (compared to other system) and thus might not be accepted over other traditional paper and pencil forms of voting or other e-voting systems, even giving the benefit of verifiability of vote and voting process (ballots).

The questionnaire originally based on the UTAUT model with an extension of security should be verified with larger amounts of data, to understand possible other influencing factors related to acceptability of e-voting systems like security.

5. DISCUSSION AND CONCLUSION

This trial allowed us to observe voters behavior when faced to an open-verifiable system such as Prêt à Voter. More specifically, we could observe their difficulties and hazardous situations leading to failures when scanning votes, which is typically a constraint introduced into the system to improve secrecy of votes using cryptographic protocol. These situations gave us some insights on how to improve the system. Interestingly enough, voters did not encounter many difficulties in using the Web Bulletin Board even if the individual vote verification after election was a totally new experience for them.
Overall the evaluation showed that Prêt à Voter is comparable in terms of usability with other e-voting systems. We intend to improve the usability of the system, especially related to instructions around the voting process and information about the functioning of the system. Based on a first version of an extended UTAUT questionnaire we investigated acceptance of Prêt à Voter. Acceptance of e-voting systems highly depends on factors like usability and trust (measured in terms of privacy, reliability), and might also be influenced by the perception of security.

There are several studies in the literature reporting assessment of many different e-voting systems; however, most of them focus on just one of the following dimension: usability, user acceptance, trust and related concepts like security, reliability and privacy. This paper presents the results of evaluation covering all these dimensions in evaluation. One of the general results is such as evaluation is to identify the factors that count for each dimension in order to avoid overlapping during the analysis. The lack of widely agreed quality models is a big barrier for comparing the different e-voting systems across several dimensions. Nevertheless, our results favors toward a multidisciplinary research for determining the factors affecting the perceived quality of e-voting systems.

Acknowledgments

This work is partly funded by the European commission via the Network of Excellence ReSIST IST-4-026764-NOE (www.resist-noe.org) and the AROVE-v project.

BIBLIOGRAPHY


