A Preliminary Study On A DualVote and Prêt à Voter Hybrid System

Damien Mac Namara*, Paul Gibson**, Ken Oakley*

**Department of Information Technology, Limerick Institute of Technology, Limerick, Ireland, mail@dualvote.com.*

*** Le département Logiciels-Réseaux (LOR) Telecom & Management SudParis, 9 rue Charles Fourier,*
91011 Évry cedex, France, Paul.Gibson@it-sudparis.eu.

***Abstract:** Two issues which have signifcantly impeded the widespread adoption and acceptance of modern e-voting solutions are the lack of an intuitive user interface and the inability to verify the results. In recent years there have been efforts made in the development of cryptographic verifiability mechanisms which allow the voter to remove an encrypted receipt of their vote from the polling station. The Prêt à Voter system is a recognized example of this approach. This paper introduces a highly usable user interface termed DualVote with the Prêt à Voter backend. We present both a generic and novel eVoting system whose instantiation is relatively simple and achieves a highusability score.*

Keywords: Usability, Verifiability, User Study.

Acknowledgement: The authors would like to acknowledge the funding support of Enterprise Ireland. The authors would also like to thank Ted Scully, Francis Carmody and David O'Connell for their help.

Introduction This paper presents a novel e-voting system which we have called Dual Vote. With Dual Vote, a voter's preference is simultaneously recorded on both electronic and paper media. The Dual Vote system allows a user to cast a vote using a pen and paper interface and simultaneously records the vote electronically using an optical sensor array and a capacitive-based electronic pen. This novel user interface (UI) addresses the crucial issues of usability and verifiability, which are now widely recognized as deficiencies in many modern e-voting systems. Usability is a commonly used metric for electronic-voting systems. The issue of providing an effective and intuitive UI has proved a significant challenge for modern e-voting solutions. A recent study compared the usability of six prominent e-Voting machine interfaces and identified a number of weaknesses (Conrad, 2009). The problems ranged from increasing the effort required to vote to interfering with the voter's ability to vote as intended. The study showed that voters preferred a short and quick voting experience with a clear inverse relationship between effort and satisfaction. The study also found that paper ballot interfaces required the least amount of actions to vote when compared with other types of voting system. In addition, after the 2008 Finnish Municipal elections, usability problems were blamed for 232 out of 12,234 voters not completing their voting session. The decision by the designers to use two different screens, one for firstly casting the vote and another for validating it, was cited as the cause of the problem by usability experts (Whitmore, 2008). This clearly highlights the ongoing need for improved e-voting interfaces. Increasing emphasis is also being placed on the ability to verify the results of an electronic voting system. For example, it is now a requirement in over thirty states in the US that e-voting systems contain some form of paper audit trail. The Mercuri method is one method used to achieve such verifiability, where a printed version of the electronic ballot is displayed behind a transparent screen. When the voter has verified that the printed and electronic vote match, the printed receipt is dropped into the ballot box by the voting machine (Mercuri, 2002). Extensions of such verifiability are end-to-end mechanisms which allow the individual verification of the single vote and universal verification that all votes have been counted correctly. Typically this individual and universal verification takes place on a web bulletin board. Prêt à Voter implements both universal and individual verifiability by allowing the voter to retain an encrypted receipt of the vote. Prêt à Voter thus allows the voter to verify that their vote was included in the final voting tally without revealing how the voter has voted. In this paper we “plug-in" a generic DualVote frontend to a Prêt à Voter backend and evaluate the subjective usability of the system in a field trial. We demonstrate that this novel and generic interface simplifies the Prêt à Voter voting process and results in a high usability score. We put forward the DualVote interface as a tool for delivering high usaibilty with Prêt à Voter. While we acknowledge that there are many security trade-offs in demonstrating our implementation, (and we make reference to some of these concerns), we are focused on the theme of usability and do not attempt a comprehensive security analysis. Likewise, we regretfully cannot extend our interface to persons with disabilities as this is outside the scope of our research. Section 2 describes the current state-of-the-art in electronic voting systems. Section 3 provides an introduction to the concept of Dual Vote and Prêt à Voter respectively. Section 4 outlines the DualVote Interface Protocol, Section 5 describes the hybrid DualVote / Prêt à Voter system and presents a detailed evaluation of its usability. Finally Section 6 concludes and outlines future directions of research.

1. Related Work

End-to-end verifiability in e-voting terms means that a voter can verify that their vote was included in the election result and that the correctness of that result is based on all the votes cast. Systems which aspire to achieve end-to-end verifiability are generally based on the use of encrypted ballot papers and, usually, part of the ballot paper is removed in order to complete the encryption. The removed part of the ballot can either be retained as a receipt or used to generate a printed receipt. Anonymous voting schemes originate with Chaum's mixnet approach which originally had an application in untraceable electronic mail (Chaum, 1981). Punchscan was later developed as an end-to-end verifiable system for e-voting which evolved into 'Scantegrity' and most recently 'Scantegrity II'. All three schemes are designed to work with optical scanning technology present in most polling stations in the US. Each of the three schemes uses a type of ballot paper encryption where each candidate on the ballot paper is assigned a unique symbol. The assignment of the symbol to the candidate is different on each ballot paper. Additionally, all three schemes contain a ballot paper with a removable section and this section contains a human readable code (Chaum, 2008) (Chaum, 2007) (Herrnson, 2006). Rivest developed an alternative method called 'Three Ballot'. The ThreeBallot method uses a 'Multi Ballot' consisting of three separate ballot papers. Each ballot paper is identical except for a serial number. Rivest proposed ThreeBallot as a means of achieving end-to-end verifiability but without using cryptography.

Rivest describes the outcome of ThreeBallot as 'partially successful' in that the end goal of three ballot is achievable but only through reducing the usability of the system.

In terms of e-voting usability, subjective usability is frequently measured using the System Usability Scale (SUS) (Brooke, 1996). The SUS has been used for many years for global assessment of systems usability and is not unique to e-Voting. SUS uses ten 5-point Likert scales to produce an overall mean usability score. A higher score denotes higher perceived usability. The reason for research into eVoting systems usability has been demonstrated in several studies (Byrne, 2007), (Herrnson, 2006), (Everett, 2006) which have shown that poor usability in e-voting can lead to a complete misinterpretation of the voters intentions leading to a vote for the wrong candidate. In addition, over complex end-to-end verifiability methods when applied to existing e-voting user interfaces can produce the same result. Our Dual Vote interface addresses verifiability and usability issues through one combined interrface. In this paper we build on previous work reporting on the usability of the Dual Vote interface (MacNamara et al., 2010). We are interested if our proposed implementation results in a usable system which encompasses the benefits of end-to-end verifiability and show that our implementation, using a generic user interface, may provide a useful tool for enhancing Prêt à Voter usability.

2. Overview Of DualVote and Prêt à Voter

2.1. DualVote

DualVote is a prototype eVoting system which allows the voter to cast an electronic vote and a paper vote simultaneously. Recent moves toward introducing paper audit trails to eVoting systems have focused on the integration of a scanner and/or printer. The interfaces of these systems (touch-screen, push button etc) may not be instantly familiar to the voter. The Dual Vote system addresses this issue by allowing a voter to cast a vote using a pen and paper. DualVote is intended for use in jurisdictions where voting by pen and paper is the norm or the traditional method of casting a vote. As such, the DualVote interface should already be familiar to the electorate.

We report on the Dual Vote interface termed the optical sensor array reader (OSAR), depicted in Figure 1. The OSAR consists of an optical array of light emitting diodes (LED's) and infrared receivers. A hybrid ink / electronic pen is connected to a transparent digitizer which is laid on top of the sensor array. The optical interface works with a ballot paper which has optical markers' attached to the underside (Figure 2). These optical markers are simply printed directly onto the ballot paper allowing us to construct a ballot paper which can be easily separated in two along a perforation (as is required by our Prêt à Voter implementation).

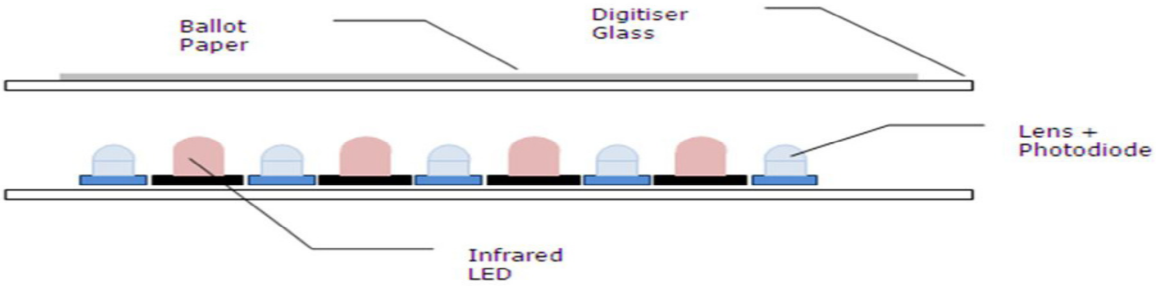


Figure 1: DualVote Optical Sensor Interface

When the voter wishes to cast their vote, they place their ballot paper on the digitizer glass and simply mark their preference with the hybrid ink / electronic pen. The system records all the pen stroke coordinates and cross references them with the coordinates of the ballot paper as detected by the optical sensor array. By superimposing both coordinates, the system can determine where the voter has placed their mark on the ballot sheet and hence, for whom the voter has voted. Each ballot paper is also affixed with a Radio Frequency Identification (RFID) tag. The RFID tag contains a value which is unique to each ballot paper. The tag value is stored with the pen and ballot paper coordinates. If necessary, an electronic vote can be tracked to the ballot paper, which is useful when resolving inconsistencies and spoiled votes. The RFID tag does not contain any vote data or data which can be used to identify the voter. When the voter places the ballot paper into the ballot box, an embedded RFID reader detects the ballot paper. When the ballot paper is successfully detected, the voting session is complete. If the electronic vote has no corresponding ballot paper then the vote is not counted.

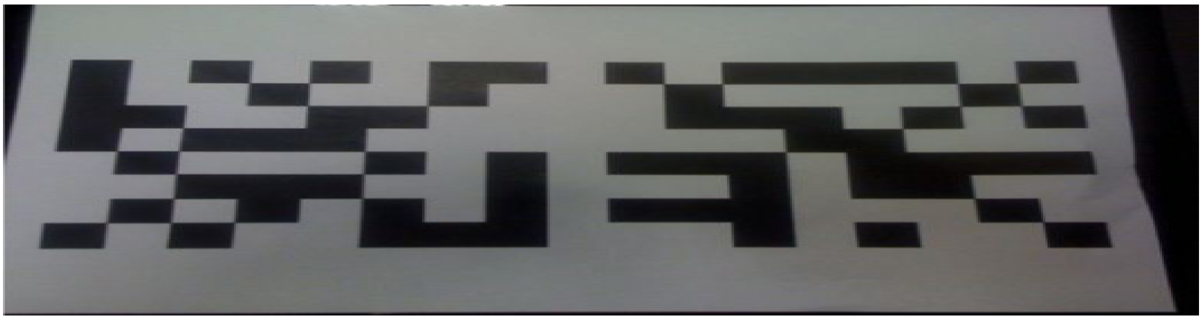


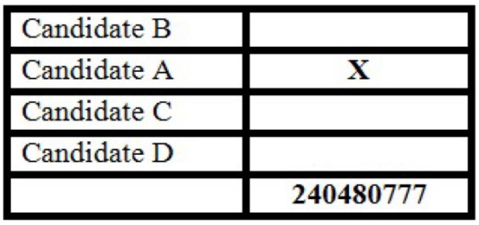
Figure 2: DualVote Optical Markers

2.2. Prêt à Voter

Prêt à Voter was developed as a means of achieving end-to-end verifiability in eVoting systems (Chaum, 2004). Prêt à Voter is ideally designed to work with existing optical scan voting systems with little or no modification of the actual voting machine. Similar to the other end-to-end verifiability mechanisms, Prêt à Voter consists of a ballot paper with a removable section which may be retained by the voter as a receipt. In the case of Prêt à Voter, this receipt incorporates the right-hand-side of the ballot paper containing the preference boxes and a human readable code called an 'onion'. The key innovation of the Prêt à Voter scheme is to encode the vote using a randomized order of the candidate list (assuming that the randomization is done honestly). This randomized order is encoded cryptographically in the onion. Buried within the onion are a number of 'germs' each hidden behind a layer of encryption. To decrypt the onion, a key is intended to be distributed between a number of tellers who must work together in order to decrypt each layer of the onion and hence determine the original ordering of the candidates on the ballot.

Principle of Operation

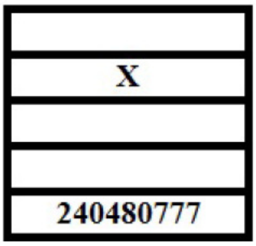
Depending on the implementation, the voter either chooses a random ballot paper (Figure 3) sealed in an envelope or the ballot paper is printed on demand. We assume an implementation where a random ballot paper is given to the voter and the first-past-the-post vote counting rules are in effect.



Candidate B	
Candidate A	X
Candidate C	
Candidate D	
	240480777

Figure 3: Example Prêt à Voter Ballot

In the polling booth, the voter extracts his ballot form from the envelope and selects his preference by placing an 'X' in the right hand column against the candidate of choice.



X
240480777

Figure 4: Example Prêt à Voter Ballot RHS Showing Voter Preference and Ballot Onion

The voter then separates the left and right hand strips along the provided perforation and destroys the left hand strip. The voter presents the right hand strip (Figure 4) to the poll-worker who optically scans it and issues the voter with a printed receipt. This printed receipt becomes the voters' receipt. The receipt can be stamped and digitally signed before being returned to the voter. The random order of the candidates on each ballot paper ensures that the receipt does not reveal how the voter has voted and as a consequence also removes any bias towards the top candidate that could occur if the candidate list were fixed. After the election, a voter or a person nominated by the voter, can visit the online bulletin board and confirm the onion value printed on their receipt appears correctly.

3. DualVote Interface Protocol

Having outlined the individual Dual Vote and Prêt à Voter systems in the previous section, we now outline the interface protocol which allows these systems to come together. In this implementation, we considered (for the first time) the engineering requirement that our design be 'generic'. Our claims for a generic design are justified by showing a "clean" separation between the interface and the back end. Based on our current design the DualVote/ Prêt à Voter back-end is divided into 3 components:

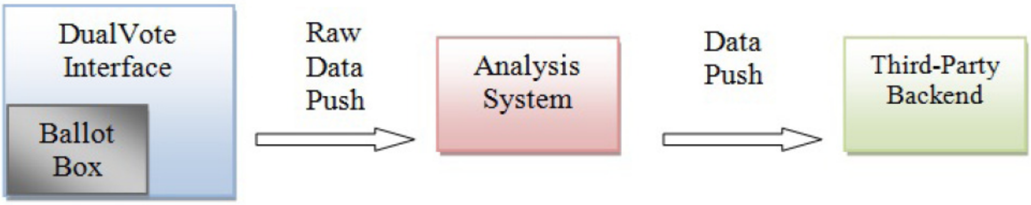


Figure 5: Componenets of the DualVote / Prêt à Voter

The DualVote Interface, (including the ballot box) sends the following Raw Interface Data to the Analysis System:

- Authentication data, confirming connectivity;
- Session Identification data (derived from the RFID tag);
- Time stamped OSAR data (the coordinates of the ballot paper);
- Time stamped digitizer/hybrid pen data (the coordinates of the handwritten data);
- RFID tag value via the ballot box (closes the voting session).

In our previous prototypes, the analysis system and the backend are on the same machine. Within the interface, a data acquisition unit (DAQ) interprets the signals from each optical sensor and converts these to digital format which are interpreted as coordinates by the analysis system. A similar process is conducted for the digital pen and digitizer. The analysis system overlays both sets of coordinates and stores them in a database (indexed by the RFID tag). At this phase, the backend analyses each set of coordinate data in the database in order to form an image of the ballot paper with the corresponding pen marks, (there can be many hundreds of such images per voting session). When this analysis is complete, the backend software should have enough data to determine the vote. For uncertain data, the vote is marked for attention by a poll worker.

For a third-party backend configuration, the interface must return only which preference boxes have written preferences. This data is in an acceptable format for counting as the backend is only required to count the preferences for each candidate. When connecting to a third-party backend, our interface sends the following data to the back end:

- Authentication data, confirming connectivity [Auth];
- Voting Session Identification data (derived from the RFID tag) [sID];
- An array of the preference box ID's where the voter has made their mark [Pref].

This resulting data packet results in the DualVote Interface protocol (Auth, sID, Pref), which is output to the Prêt à Voter backend. The backend software can look-up the Session Identification data [sID] and find its corresponding onion value (each sID is related to a ballot onion in the backend database). The onion is then decrypted to apply the correct cyclic shift to the candidate ordering allowing the vote to be counted correctly.

3.1. Meeting the Pluggability Requirement

In order to see how well we meet the generic design (“plugability") requirement we retrospectively analyze the DualVote/ Prêt à Voter prototype by asking the following questions of our system:

- How close did we get to independent/parallel development of front and back ends?
  As no modification to the DualVote and/or Analysis system was required in order to implement the Prêt à Voter backend and considering that all communication between the frontend and backend is one way; independent / parallel development of both systems was achieved.
- Did the front-end have to change much in order to facilitate Prêt à Voter ballots?
  From an analysis of the DualVote raw interface Data we see that it is completely independent of the election rules. The Analysis system is only interested in the unique

identification of the ballot, its orientation and the pen coordinates made by the voter. With specific reference to the Prêt à Voter voting process; the interface could accurately determine the raw data without hardware or software modification while the onion value, could be determined from the attached RFID tag.

- Could we change the front-end technology without having to change the back-end?

  We expect that the front-end technology can be changed or upgraded (to produce a higher resolution for example) without having to change the back-end configuration. Our protocol is only interested in returning preference box identifiers and a ballot ID and such data is abstracted away from individual sensor values.

- Can we extend the protocol (eg. to incorporate user feedback) without having to make major changes to front/back ends?

  Currently the communication from the DualVote Interface/Analysis System to the backend is one-way (hence anonymity is fully perserved). In order to give feedback to the voter (via a graphical user interface for example) we need to apply some election rules (pertaining to what constitutes a valid/spoiled vote) to our vote data. We can provide for this feedback while maintaining adherence to our generic design requirement. We put forward two potential approaches:

  1. Process the election rules in the backend and connect the backend directly to the voter feedback device. This would require connectivity to the backend throughout the election, which could introduce substantial security concerns (such as a potential breach of anonymity). However the current DualVote interface protocol is unchanged and one-way communication between the front and back ends is preserved.
  2. Process the election rules in the DualVote Interface / Analysis System by connecting to a data storage device which contains the election rules. This will increase the number of potential outputs from the Interface / Analysis System; an output to the graphical user interface and an input/output to the data storage device (and hence potentially increase coupling). Using this approach requires a minor modification to the Interface Protocol to include a value relating to the spoiled/unspoiled nature of the vote and reduces the risk of weakening voter anonymity.

From our analysis we found that independent and parallel development of the front and backends was facilitated due to the low coupling between the two systems. The DualVote raw interface data shows that the interface is 'blind' to the election rules making modification to the interface software and/or hardware unnecessary. Our analysis of the DualVote protocol shows an abstraction away from any technology dependant variables (we only return preference box idenidifiers). Finally we found that future enhancements to the system pertaining to voter feedback would require only minor changes to our protocol.

4. DualVote + Prêt à Voter Hybrid System

We created a hybrid DualVote / Prêt à Voter system for the purpose of our study. The DualVote element consists of the following two components:

- DualVote Interface;
- Administration Computer.

The interface allows the voter to cast their vote using the hybrid-pen and optical sensor array. The administration computer stores and translates the ballot and pen coordinate data for each vote and allows the poll-worker to activate the interface. The administration computer was not connected to the back end and cannot decrypt the ballot onions. The Prêt à Voter element consists of the following two components:

- Prêt à Voter Back End
- Ballot Checking Station.

The Prêt à Voter back end is responsible for generating the ballot onions and counting of the votes. As we are interested only in the usability of the system we do not report on the cryptographic methods involved in the generation of these onions. The ballot checker consists of an RFID antenna and a visual display unit. This checker allows any voter to verify a ballot paper by confirming that the onion value relates to the correct ordering of candidates. When the voter places a randomly chosen sample ballot paper on the RFID antenna, the ballot RFID tag is read and its corresponding onion value is retrieved from the checker database. This onion value is then sent to the back end and decrypted so that the correct ordering of the candidates can be displayed on the visual display unit together with the onion value.

Unique Aspects of our Prêt à Voter Implementation

Passive Scanning of the Complete Ballot Paper In our hybrid system, the ballot paper is passively scanned by the optical sensor grid when the entire ballot paper is placed on the DualVote writing surface. Traditionally, Prêt à Voter implementations scan only the right-hand-side of the ballot so that the voting machine cannot learn the original candidate ordering. The DualVote interface is only able to determine the optical markers on the underside of the ballot paper and the pen markings made by the voter. The onion value cannot be detected and so it is possible that the entire ballot paper can be placed on the writing surface/sensor grid. In optical pen-based systems which also use optical markers encoded on the ballot paper, it may be possible for the ordering of the candidates to be encoded in some way within the pattern. The DualVote optical pattern is visible to the human-eye and so a visual inspection would reveal a fraudulent ballot paper as every optical pattern should be identical regardless of the printed candidate ordering. We acknowledge that considering the uniqueness of our optical pattern, relying on voters to accurately inspect and identify a fraudulent pattern may be impractical. Making such an inspection part of the voting process may introduce further complication unless a simpler way of identifying the pattern (or indeed using a simpler pattern) is investigated.

Depositing the Left-Hand-Side of the Ballot into the Ballot Box All existing Prêt à Voter implementations require the left-hand-side or candidate side of the ballot paper to be destroyed after separation. This is to ensure that no voter can leave the polling station with the entire ballot paper. The left-hand- side of our ballot paper contains an RFID tag which is detected by the ballot box. If an entire ballot paper is removed from the polling station no RFID value will have been detected in the ballot box and the vote is not included in the final tally(likewise the vote will not be counted if a voter places the ballot into the ballot box without casting the vote electronically). We acknowledge that the depositing of the left hand side of the ballot, while novel, presents potential issues with regards to compromising the identity of the voter. By simple observation, it is theoretically possible that a fraudulent poll-worker could catch a glimpse of the ballot onion and use this knowledge later on to determine how the voter has voted. Conversely, negating the need for the poll-worker to scan the ballot and return a printed copy to the voter may present some security benifits in this regard. Depending on the construction of the ballot box, it may be possible for a voter to cause the embedded RFID reader to scan the RFD tag and still allow them to remove the ballot paper. In a future design it may be benificial to use a larger ballot box where the RFID reader is plaecd deeper within the housing, forcing the voter to deposit the ballot fully before the RFID tag value can be read. Alternatively, the ballot box could be constructed using a shielding material, however this would prevent a transparent design.

Use of RFID Tags There has been much recent discussion regarding the use of RFID tags in voting systems (Oren, 2010) In many contexts, RFID tags can introduce significant security concerns and their use in elections should be heavily scrutinized. While we are looking at this implementation of Prêt à Voter purely from a usability perspective, we are aware of the potential security concerns that RFID tags introduce. In retrospective analysis we identified the possibility that a fraudulent poll-worker, using relatively simple technology, could intercept the RFID tag on a voters ballot paper. Later, after the close of the election, the poll-worker could compromise the identity of the voter by locating his RFID tag within the voting database. As a potential solution to this problem, we could implement a special mylar privacy folder (in essence an RF-shielded folder) to prevent such an interception. Additionally we could introduce a mix-net within the software that separates the link between the RFID tag and the vote data. As an alternative to the RFID approach, a QR-code solution may provide extra security as the voter only has to protect this code from being read.

Lack of Receipt Issuing In our experiment we purposely wanted to remove the need for printing and scanning (even by the poll-worker) as this adds a further step to the voting process and so increases complexity. We acknowledge however that the need to issue a voter with an official receipt of their vote is of paramount importance in an actual election. We kept the voting process as straightforward as possible while retaining the core functionality of the system to achieve end-to-end verifiability. However further work is merited and is discussed in the conclusions.

5. Usability Study

Participants The field study consisted of 88 participants who voted using the Hybrid System. Of these participants 84 completed an SUS and demographic survey after they had voted. Regarding gender; 72.6% of respondents were male, 27.4% were female. The age demographic was: 21.4% of respondents were aged 15-24, 36.9% were 25-44, 35.% were 45-64 and 6% were 65+. The education demographic was; 33.3% had completed second level, 35.7% had a degree, 27.4% had a masters degree and 3.6% had a PhD. Additionally the participants were asked to rate their computer experience on a Likert scale of 1 to 10, a higher value reflected more experience. The average self assessed rating was 6.94.

Ballot Design The ballot paper was a single A4 sheet consisting of the following:

- The underside of the ballot paper is encoded with an optical marker so that the orientation of the ballot paper can be detected by the optical interface.
- The candidate side of the ballot paper (the left side on Figure 3) has an affixed RFID tag.
- The preference box side of the ballot paper (right hand side on Figure 3)
  contained the ballot onion.

A choice from four countries could be selected and the voter was instructed to place an "X" in one of the preference boxes to indicate their favorite country. We acknowledge that the ballot paper was not suitable for a large candidate list. Improvements to Prêt à Voter aiming to address this and other issues have been discussed in other research, for example (Xia et al., 2008).

Configuration Before the election four different orderings of the candidate list were determined using a cyclic shift of an original candidate ordering. A database was created on the back end and ballot checking station linking each RFID tag to a particular onion value (relating to a particular ordering of candidates). When the vote data was received from the polling station at the end of the election, the RFID value for each vote was looked up in this database so the corresponding onion value could be decrypted revealing the ordering of the candidates. Neither the administration computer nor the DualVote interface at the polling station knew the assignment of RFID tags to onion values or could decrypt the onions.

Procedure

- The voter presented a student identity card or drivers license in order to be issued with a randomly selected ballot paper.
- The ballot paper was passed over a contactless RFID reader which made the voting machine ready for use.
- The voter was instructed to place the ballot paper on the DualVote writing surface and cast their vote with the electronic pen.
- The voter placed their ballot paper on the writing surface and marked their preference using the hybrid ink/electronic pen. After the voter had completed voting, they separated the ballot paper into two halves of equal size by tearing along the perforation. This separated the candidate list from the preference boxes.
- The voter deposited the candidate side of the ballot paper into the DualVote ballot box. The RFID reader within the ballot box detected the RFID tag on the ballot paper and closes the voting session. If the voter did not complete this step, their vote is not counted.
- At the end of the election, the voter could check that their ballot onion had appeared on the web bulletin board (the RFID value is not displayed).

Electronic Data Collection When the voter placed his ballot paper on the writing surface, a binary image of the ballot paper was generated based on the position of the optical markers. All pen strokes made by the hybrid pen and digitizer were overlaid on this image. Therefore for each voting session the following data was recorded:

- Pen coordinates;
- Paper orientation coordinates;
- RFID tag value.

In the event that the RFID reader within the ballot failed to read the RFID tag on the ballot paper, we required that each ballot paper is manually passed over the contactless RFID reader by the poll-worker at the end of the election. In retrospect, it may have been beneficial to provide a feedback mechanism to the voter informing them that their ballot paper was successfully read).

Subjective Usability Evaluation

The SUS survey produced a mean result for the Hybrid DualVote / Prêt à Voter system of 84.85 which indicates that the usability of the system is relatively high for e-Voting Systems. (Everett, 2008) (Winckler, 2009). An earlier DualVote usability study showed an SUS score of 86.1 which is only slightly higher than the DualVote / Prêt à Voter hybrid. From a usability perspective, the only difference between the earlier study and the hybrid study was the requirement that the voter separate the ballot paper after voting and deposit the candidate portion of the ballot paper into the ballot box. The action of depositing a ballot paper into a ballot box is also likely to be familiar to our participants, as this action is also required when voting in real elections. The action of separating the ballot paper along the perforation after voting is completely unfamiliar to our participants in the context of voting. This unfamiliar action, which is at the core of the Prêt à Voter voting procedure seemed to result in only a minimal change to our previous SUS score.

6. Conclusions and Future Work

In this paper we present a subjective usability evaluation of a hybrid DualVote/ Prêt à Voter system which achieves a high SUS score for eVoting systems. We also demonstrate the generic nature of our interface through the definition of an interface protocol. Our hybrid system differed from previous Prêt à Voter implementations by negating the need to actively scan the ballot paper through the use of our novel optical sensor array. Additionally the voter was required to deposit the candidate side of the ballot paper into a ballot box containing an RFID reader which detected the corresponding RFID tag on the ballot. This change negated the need for the poll-worker or voter to shred the ballot. These two adjustments to the traditional Prêt à Voter procedure would appear to simplify the process for both the voter and poll-worker. By comparison to the traditional method of casting a vote on pen and paper, the only new action to be performed by the voter is the separation of the ballot paper along the perforation. The 'separation' action caused only a minimal decrease in the SUS score of the system when compared to an earlier DualVote usability study. We showed that the DualVote system is generic in nature which is capable of being used in any election type where the candidate list is fixed. We successfully demonstrate how the DualVote front end was not modified in any way in order to plug into the Prêt à Voter back end. This is a significant finding because we were able to demonstrate that a generic system, whose instantiation is relatively simple, achieves a resulting usability which is similar to the previous implementation. Additionally, we demonstrate that with only little extra development (to plug together front and back ends) we were able to "guarantee" similar usability. A limitation of our study was that the voter did not receive feedback as to the state of their vote (spoiled/unspoiled), however we demonstrate that voter feedback may be implemented with only minor changes to our protocol. Additionally, the voter was not issued with a printed receipt of their vote and simply retained the right-side of the ballot paper. In theory, a fraudulent voter could create a fraudulent receipt by retaining the same ballot onion but changing the candidate selection. The ballot checking station presents a further issue due to the sensitive nature of the data travelling from the checker to the backend. Future work needs to address these issues and include the facilitation of a signed or stamped receipt.

References

Brooke, J.: (1996) *SUS: A quick and dirty usability scale*, In P. W. Jordan, B. Thomas, B. A. Weerdmeester & A. L. McClelland (eds.) Usability Evaluation in Industry. London: Taylor and Francis.

Byrne, M.D., Greene, K.K., Everett, S.P.: (2007) *Usability of voting systems: baseline data for paper, punch cards, and lever machines*. In: CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems. pp. 171-180. ACM, New York, NY, USA

Chaum, D. (1981) *Untraceable electronic mail, return addresses, and digital pseudonyms*. Commun. ACM 24(2), 84{88 (1981)

Chaum, D., Carback, R., Clark, J., Essex, A., Popoveniuc, S., Rivest, R.L., Ryan, P.Y.A., Shen, E., Sherman, A.T.: (2008) *Scantegrity ii: End-to-end verifiability for optical scan election systems using invisible ink con_rmation codes.* In: Dill, D.L., Kohno, T. (eds.) EVT. USENIX Association

Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A., Vora, P.: (2008*) Scantegrity: End-to-end voter-verifiable optical- scan voting. Security & Privacy*, IEEE 6(3), 40{46

Chaum, D, P.Y.A. Ryan and S. Schneider (2004). *A practical, voter verifiable election scheme.* Technical Report CS-TR-880, University of Newcastle upon Tyne.

Conrad, F.G., Bederson, B.B., Lewis, B., Peytcheva, E., Traugott, M.W., Hanmer, M.J., Herrnson, P.S., Niemi, R.G.: (2009) *Electronic vot ing eliminates hanging chads but introduces new usability challenges.* International Journal of Human-Computer Studies 67(1), 111 { 124

Everett, S.P., Byrne, M.D., Greene, K.K.: (2006) *Measuring the usability of paper ballots: Efficiency, effectiveness, and satisfaction.* In: Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting.

Fisher, K., Carback, R., Sherman, A.: (2006) *Punchscan: Introduction and system definnition of a high-integrity election system.* In: Preproceedings of the IAVoSSWorkshop on Trustworthy Elections. IAVoSS, International Association for Voting System Sciences, Robinson College, Cambridge, United Kingdom

Herrnson, P., Niemi, R., Hanmer, M., Bederson, B., Conrad, F., Traugott, M.(2006) *The importance of usability testing of voting systems.* In: USENIX/ACCURATE Electronic Voting Technology Workshop. pp. 87{121

MacNamara D, Carmody F, Scully T, Oakley K, Quane E and Gibson P. *Dual Vote: A Novel User Interface For E-Voting Systems.* Proceedings of the IADIS International Conference on Interfaces and Human Computer Interaction 2010 (pp 129-138)

Mercuri, R.: (2002) A *better ballot box*? IEEE Spectr. 39(10), 46{50

Oren Y. and Wool A., (2010) *RFID-based electronic voting: What could possibly go wrong?* in 2010 IEEE International Conference on RFID, april 2010, pp. 118 –125.

Rivest, R.L., Smith, W.D.: (2007) *Three voting protocols: ThreeBallot, VAV, and Twin.* In: EVT'07: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2007 on Electronic Voting Technology Workshop. USENIX Association, Berkeley, CA, USA

Whitmore, K.: (2008)*I nformation report on the electronic voting in the Finnish municipal elections observed on 26 october 2008.* (2008)

Winckler, M., Bernhaupt, R., Palanque, P., Lundin, D., Leach, K., Ryan, P., E., A., Strigini, L.: (2009) *Assessing the usability of open verifiable e-voting systems: a trial with the system prt voter.* In: Proc. of ICE-GOV, Turksat. pp. 281{296

Zhe Xia, Steve A. Schneider, James Heather, and Jacques Traor'e. *Analysis, improvement, and simplification of Prêt à Voter with paillier encryption.* In Proc.USENIX ACCURATE Electronic VotingTechnology Workshop, 2008.

About the Author/s

Damien Mac Namara.

Damien is the Principal Investigator on the Dual Vote Research Project since 2007. He is currently completing his PhD themed on e-voting usability issues at the Limerick Institute of Technology.

Paul Gibson

Paul is a Maître de conferences at TSP, Evry, France. He has been carrying out research into all aspects of e-voting for the last 7 years, and is the main supervisor to Damien on his PhD.

Ken Oakley

Ken Oakley is a senior lecturer in information technology with the Limerick Institute of Technology. He has over 20 years of system engineering experience.