Institution: University of Surrey

Unit of Assessment: UOA 11 Computer Science and Informatics

Title of case study:

Introducing a secure electronic voting system to the State of Victoria, Australia

1. Summary of the impact (indicative maximum 100 words)

Researchers at Surrey have designed a new voting system commissioned by the Victorian Electoral Commission, for use in their State election, based on our Prêt à Voter system.

It will be the world's first fully verifiable e-voting system. Surrey's work has had a direct impact on Australian voting public services and on public policy on e-voting. The system provides secure and verifiable electronic support for voting in Victoria's State elections. Benefits include accessibility for blind and vision impaired voters, for those with motor impairments, for those who cannot read English, and greater efficiency and reach for remote voters nationally and internationally.

2. Underpinning research (indicative maximum 500 words)

The Prêt à Voter voter-verifiable voting system was first proposed in 2005 [1], and enhanced in 2006 [2], and developments have been continual since those two papers. The system uses cryptography in a novel way to provide each voter with a receipt which captures how their vote was cast but in a way that does not expose the vote. This is achieved by using a ballot form with the candidate names in a random order on one half, and the boxes to mark the vote on the other half. When the list of candidate names is separated from the voter's selection (and destroyed), then the remaining half constitutes a receipt while maintaining secrecy of the ballot, since the list of names is held only in encrypted form. Research on Prêt à Voter has been focussed on how to provide verifiability on top of this mechanism: that voters and the general public have evidence to verify that the election result is correct. There have been several proposals with respect to this, brought together in [3].

The use of "anonymity mixnets" for processing the votes to provide voter anonymity and verifiability of the end result is also a key element of the approach. A variety of mixnet designs have been explored [1,2], and the approach of [2] is used in the vVote system presented in this case study.

An early proof-of-concept prototype was developed at Surrey (with support from collaborators at the University of Newcastle) for the VoComp University Voting Systems Competition in 2007. This won Best System Design, and was overall runner-up.

Another research contribution provides a general way of encrypting ballot form information to make it much more flexible to deploy in practice [4]. The key idea was to encrypt each candidate separately, and encode votes differently at the back-end to handle the vote processing. This enables first-past-the-post voting (where a single candidate is selected) and preferential voting (where candidates are ranked in order of preference) to be handled within a single unified approach. These ideas were developed over 2009-2010 within the TVS project [P1]. This approach is exactly what is required for Australian elections, and this approach provides the back-end behind the vVote system which is the subject of this case study.

More recent research [5,6] was a collaborative effort involving the Surrey team in conjunction with partners in Australia (including the Victoria Electoral Commission, and academic partners) and in Luxembourg. These developed novel cryptographic protocols for secret ballot generation, and for ballot form print-on-demand (remote printing of ballot forms) required by the Victorian Electoral

Commission.

Key researchers:

Steve Schneider: Professor 2004-date
James Heather: Lecturer 2000-2009; Senior Lecturer 2009-date
David Bismark (nee Lundin): PhD student 2006-2010
Zhe Xia: PhD student 2005-2009; RA 2009-2013
Chris Culnane: RA 2009-2013
Sriram Srinivasan: RA 2009-2012

3. References to the research (indicative maximum of six references)

[1] David Chaum, Peter Ryan, and Steve Schneider, **A practical voter-verifiable election scheme,** European Symposium on Research in Computer Security (ESORICS), pp118-139, Springer LNCS 3679, 2005.

[2] Peter Ryan and Steve Schneider**, Prêt à Voter with re-encryption mixes,** European Symposium on Research in Computer Security (ESORICS), pp313-326, Springer LNCS 4189, 2006.

[3] Peter Ryan, David Bismark, James Heather, Steve Schneider and Zhe Xia, **The Prêt à Voter Verifiable Election System**, IEEE Transactions in Information Security and Forensics, 4(4): 662-673 (2009)

[4] Zhe Xia, Chris Culnane, James Heather, Hugo Jonker, Peter Y. A. Ryan, Steve Schneider, and Sriramkrishnan Srinivasan. **Versatile Prêt à Voter: Handling multiple election methods with a unified interface**. INDOCRYPT, 2010, LNCS 6498

[5] Craig Burton, Chris Culnane, James Heather, Thea Peacock, Peter Y. A. Ryan, Steve Schneider, Sriramkrishnan Srinivasan, Vanessa Teague, Roland Wen, Zhe Xia, **A Supervised Verifiable Voting Protocol for the Victorian Electoral Commission,** 5th International Conference on Electronic Voting (EVOTE), Lecture Notes in Informatics 205 2012.

[6] Craig Burton, Chris Culnane, James Heather, Thea Peacock, Peter Y. A. Ryan, Steve Schneider, Sriramkrishnan Srinivasan, Vanessa Teague, Roland Wen, Zhe Xia, **Using Prêt à Voter for Victorian State Elections,** Electronic Voting Technology (EVT) 2012.

Projects

[P1] James Heather and Steve Schneider (Surrey) and Mark Ryan (Birmingham): **Trustworthy Voting Systems**, EPSRC, April 2009 – October 2014, £1.5M.

[P2] James Heather: **Real World Secure Elections,** Leverhulme Trust, £40,660

[P3] Steve Schneider and James Heather: **Software for the Verifiable Election System Demonstrator,** Victorian Electoral Commission, March 2012-July 2012, £13,000

[P4] Steve Schneider and James Heather: **Design Specification for the Verifiable Election System,** Victorian Electoral Commission, August 2012 – December 2012, £5,770

[P5] Steve Schneider and James Heather: **vVote voting system implementation,** Victorian Electoral Commission, July 2013 – December 2014, £103K

4. Details of the impact (indicative maximum 750 words)

The design of the Prêt à Voter verifiable voting system provides the foundation for the vVote voting

system developed in conjunction with the Victorian Electoral Commission (VEC) for local and state elections in Victoria, Australia. The key impact at this stage has been on Victorian public policy, whereby the VEC, under the scrutiny of the Victorian Parliament, took a decision in June 2012 to develop the world's first voter verifiable electronic election system as the best way of delivering their key objectives for the election. It was the prototype developed by Surrey [P3] in conjunction with the VEC which was used in June 2012 as the basis for a decision by the VEC to proceed to full production development of the system to run the Victorian State Election in November 2014. The Surrey team have since led on the development of this system, and are implementing the back end.

The vVote project has also contributed to public policy debate in Australia with respect to guiding principles for e-voting, in the context of problems with non-verifiable election systems elsewhere in the world (especially the US, but also the Netherlands, Finland and Ireland) [Source 5]. A recent Victorian Parliamentary Inquiry [Source 6] has noted *"the VEC's involvement in the world's largest universally verifiable public e-voting system, based on "Prêt à Voter". The Committee appreciates the potential of this project and looks forward to receiving evidence from the VEC about it as the inquiry progresses."* Other Australian states [see e.g. Source 7] are closely watching the VEC activity. The Australian Electoral Commission organised a workshop in July 2012 to discuss guiding principles for e-voting. This was attended by senior representatives from electoral administration (Electoral Commissioners and Deputies) and IT (typically IT Director) from all but one of the States in Australia, and also New Zealand, and with academic participation from Australian academics as well as from Surrey. The existence of the vVote prototype introduced the concept of *verifiability* into the discussions and this is framing part of the standard currently being developed in Australia for electronic voting. The standards activity was initiated after the July 2012 workshop and is ongoing.

Australian elections pose a unique set of challenges which motivate the introduction of electronic systems for capturing and processing votes, and which vVote addresses, delivering impact in public services through improvements to accessibility and inclusion. Firstly, voters can vote from anywhere, not just their registered district. This has previously been managed using paper ballots, but this introduces delays in returning the ballots promptly, particularly from overseas. Secondly, the complexity of ballot forms means that a percentage of voters inadvertently spoil their ballots (this is estimated to be around 2.5%), which would be mitigated by electronic assistance for completing the ballot form. It is unknown how many people vote without spoiling but fail to have their intent captured. Thirdly, disabled voters must be given equal opportunities to vote secretly and independently. Fourthly, voters who do not speak English must also be catered for in any of 19 non-English languages.

Working with the VEC, with Vanessa Teague of the University of Melbourne, with Peter Ryan of the University of Luxembourg, and others, the Surrey team applied the Prêt à Voter design to the particular requirements of the Victorian Election System, including large candidate lists (30-40 candidates), preferential voting, complex ballot forms (with 'above the line' tickets and 'below the line' candidate lists), and the associated desire for electronic assistance for voters. Surrey developed the back end of the system, including distributed ballot form generation (to distribute trust), incorporation of the mixnets, mixing and decrypting the votes, and the print on demand protocol. We maintained a constant interaction with the front end developers and accordingly influenced aspects of the front-end design.

However, electronic voting introduces new risks to the security and integrity of elections, and the VEC were concerned that existing e-voting systems did not properly address these. The novelty of the Prêt à Voter approach is the introduction of *universal verifiability*, which enables all parts of the

processing of the votes to be verified, either by the voter or by independent auditors, while maintaining ballot secrecy by use of cryptography. This is at the heart of the VEC's vVote system. VEC decided that a verifiable system was required, and identified that Prêt à Voter was the only proposed scheme in the literature which was flexible enough to handle preferential voting on a large scale while maintaining usability for the voters and supporting the existing voting ceremony. VEC approached Surrey as the natural partner, as a direct result of our research activity in this area.

The impact of this system is that it provides more accessibility to voters while preserving security of the system and integrity of the election. Voters can now vote on customised tablets in polling stations, upload their (encrypted) vote to a public bulletin board, and retain a receipt of their encrypted vote for verifiability. This provides an improved handling of early and out of district votes – there are approximately 400,000 such voters in Victoria, of a total of around 3,600,000 voters.

On the basis of the demonstrator produced at Surrey backed up by the underpinning research, VEC took the decision to develop a system to run a politically binding voter-verifiable election, the first time this has been done anywhere in the world at this scale, even on supervised electronic voting services. Victoria has a proud history of electoral innovation, having introduced the secret ballot to the world (known as the `Australian Ballot') in 1856.

5. Sources to corroborate the impact (indicative maximum of 10 references)

1. Manager, E-voting, Victorian Electoral Commission (contact details provided)
2. Deputy Electoral Commissioner, Victorian Electoral Commission (contact details provided)
3. Blind technical expert on W3C (contact details provided)
4. Electoral Commissioner for Australia, Australian Electoral Commission (provided statement)
5. http://en.wikipedia.org/wiki/Electronic_voting
6. Inquiry into the future of Victoria's electoral administration, Discussion Paper, Electoral Matters Committee, Parliament of Victoria, 2012, http://www.parliament.vic.gov.au/images/stories/committees/emc/ifvea/emc.ifvea.discussionpaper.pdf
7. Administration of the 2011 NSW Election and Related Matters, Joint Standing Committee on Electoral Matters, Parliament of New South Wales, December 2012.

   http://www.parliament.nsw.gov.au/electoralmatters
8. http://tabtimes.com/news/government/2012/04/05/australian-state-enable-tablet-voting-next-election
9. http://www.computerworld.com.au/article/420681/vec_develops_tablet-based_e-voting_system/
10. http://thevotingnews.com/victorians-to-vote-online-next-year-sc-magazine-australia/