Committee: Joint Standing Committee on Electoral Matters

Inquiry: Inquiry into the conduct of the 2007 Federal Election

Questions for Witness 4, Registries Limited and Everyone Counts

Melbourne hearing 12 August 2008

Reply by Craig Burton, EveryoneCounts.com
19 September 2008

Question: How would scrutineers monitor the electronic ongoing voting process?

Scrutineers are needed for the electronic voting process and the scrutiny process should never be automated. Scrutiny in electronic elections is different from the roles a scrutineer plays in a paper election, however, the integrity of the electronic election can be observed by scrutineers nonetheless and the electronic election can fulfil the democratic requirements of an election where the voters are remotely located and are unsupervised.

Everyone Counts' system emits artefacts of the election which are intended for audit and scrutiny. Some artefacts can be digitally signed by an auditor with the resulting signature able to be checked by voters themselves. No artefacts individually or together expose a voter's vote. The system provides various testing facilities to allow tests of system integrity before and during live elections. The system provides a receipt checking service intended to be used by a proportion of voters. This table lists the services and artefacts for scrutiny.

Service, process or artefact	**What is it**	**Who can see it or take part**	**When**	**What does it provide for scrutiny**
Management console	A running computer program on the voting servers	ERO and scrutineers	Before, during and after the election	Set up, monitoring and reporting of the election on the server
Clean PC voter credential creation, election key creation and election vote decryption and authorisation	A running computer	ERO, scrutineers and party officials, observers	Keys and credentials before the election, decryption and authorisation after the election	Secure creation of voter login codes and cryptographic shares used to protect the votes. The same tool also decrypts votes and authorises votes.
Clean PC software sources	Human readable computer program software codes	Software code auditors, academics	Before, during or after the election	That the cryptographic implementation is correct and that the vote handling process is free of bugs

Service, process or artefact	What is it	Who can see it or take part	When	What does it provide for scrutiny
Java applet sources	Human readable computer program software codes	Anyone	Before, during or after the election	That the software that collects the vote on the voter's PC is correctly implemented
Java applet digital signature	A digital signature applied to the Java applet	Anyone	During the election	That the Java applet the voter will vote on is not a fraud and has not been modified after it was audited
Software audit report	A report written by one or more auditors	Anyone	After software code audit	That the software codes for the election were assessed by experts.
Voter records import and update logs	A log emitted by the server when voter records are uploaded or updated	ERO and scrutineers	Before and during the election	That all voter records were imported correctly. That exceptions are trapped and reported.
Voting event log	A log emitted by the server showing all voter-related events in the election	ERO and scrutineers	During and after the election	That every single vote taken aligns with individual voter events such as a voter logging in and logging out.
ERO event log	A log emitted by the server showing all ERO activities on the server	Master account holder on the server. Scrutineers.	Before, during and after the election	That the ERO performed the right tasks at the appropriate times
Logic and accuracy testing	A series of tests which allow a test group to use the system end-to-end	ERO and scrutineers	Before the election	That voter registration, voting, decrypt and counting can be executed and votes output from the system match the test votes that went in
PEN Audit report	A technical audit report of the outcome of controlled attempts to break in to the voting systems	Scrutineers, ERO	Before the election	That the systems have been correctly configured to repel a wide range of Internet-borne attacks
Parallel testing	A testing process which takes place during the election	Scrutineers, ERO	During the election	As per Logic and Accuracy testing but also shows that the "live" system is handling votes as expected
Emitted raw votes	A data file of the voting choices	Scrutineers, ERO	After the election,	Allows the votes to be counted in a third party

Service, process or artefact	**What is it**	**Who can see it or take part**	**When**	**What does it provide for scrutiny**
	collected from voters during the election		after decrypt of the votes	counter or otherwise examined for vote formality. The votes do not carry identifying information.
Emitted votes on paper facsimiles	Votes, one-per-sheet, as emitted from the system	Scrutineers, ERO, local election officers	After the election	Allows the on-line votes to be (anonymously) incorporated with paper vote counting
Emitted votes reports	Reports summarising the emitted paper votes	Scrutineers, ERO and local election officers	After the election	Allows a cross-check of voter eligibility and any duplicate voting between on-line and other (off-line) channels
MD5 signatures of software used	A mathematical "signature" which is made from the server and other software used in the election	Anyone	Before, during and after the election	Allows a check that the server software matches an audited reference copy exactly and that the server software has not changed
Intrusion Detection System and change-detection logs	A log report from the server of security-related events	ERO, technicians and Scrutineers	At any time	Allows analysis of any attempted attacks on the server. Allows identification of files on the server that have changed.
Receipting log	A log report of all voter-verified receipts	ERO, Scrutineers	After the election, during the receipt checking period	Allow analysis of the success of voter's receipt checks. The receipt check demonstrates to the voter that their vote was received and decrypted.
eScript election definition	A document of formal eScript commands defining the election	Anyone	At any time	Shows the candidates, formality rules and other settings. This definition controls all important aspects of the election.

Question: What sort of fall back system would need to be in place in case of technical failure? How would this be combined with the normal voting results?

The system design considers a number of potential technical failures from the voter's PC to the voter's Internet connection right up to large scale failures affecting multiple data centres (where the central server systems are housed).

Fall back can take two forms - either another technical system is provided, or the system falls back to "all paper". That is, paper is used for the electoral role and the ballots. Both kinds of fall back have been provided with our systems. In isolated circumstances, an "all paper" fall back has actually been used. Technical failures are anticipated and managed via

1. All systems provide redundancy so that failure of a single device or service does not affect overall services to the voters or any other stakeholder. Failures at this level do not affect the election integrity.
2. Typically a second data centre is used in case an entire data centre is lost. The second data centre is ready to take up the voting services at any time. Failures at this level do not affect election integrity.
3. Failure of one remote channel, such as web voting may not prevent electronic voting if voters can also use a second provided channel (such as telephone). Both channels are typically provided. Preventing multiple voting between web and telephone is a central part of the system and is typically achieved by each remote voter holding some unique number or code which works via phone or web. Once the code is spent, subsequent voting attempts on any channel are no longer permitted.
4. If the voter's PC crashes while they are voting (or a phone voter loses their call connection) the balloting system will allow that voter to access the ballot again, until such time as they successfully confirm and submit their vote. After that time, they cannot gain access to the ballot again.
5. If the voter's Internet connection is lost mid-vote, the E1C voting interface which runs in the voter's browser can advise the voter to check their connection and can allow the voter to attempt to submit the vote a number of times. Common web pages would normally fail to submit to the server. The E1C voting interface is a Java applet which is able to detect its environment and handle failures.
6. If technical systems at a polling place are entirely down, E1C has provided a process to reconcile paper ballots and paper registers. A marked register of "paper" voters takes the place of any E1C poll place e-register services. When the electronic system comes back up, the polling staff use it to mark the centralised system from marks on the paper register. If this cannot be done at the poll site, it is done after close of polls, centrally by tabulation staff. Paper ballots collected from poll places that were off-line are hand-counted. If STV were used, each STV ballot would be keyed in to the E1C voting interface so that votes taken off-line are included in the count.
7. Many elections provided by E1C for remote voters have required remote voters be sent paper mail ballots offering that the voter can return the voted paper ballot, vote on-line at a given address with given login codes or vote by phone at a given number with given login codes. Failure of the electronic services does not preclude the voter sending in their paper ballot. The paper ballot is bar-coded and on receipt the paper ballot bar code is read by the E1C system and used to detect multiple voting via the electronic channels or block ongoing electronic voting for the voter who has returned a paper ballot.

Question: What would be the security for the fall back system?

As introduced above, the system using an electronic fall back typically has no implications for the secrecy of votes because the technical fall back is the same service as that which it replaces.

When replacing the electronic voting with a paper fall back, the paper register marks are used as the basis of a cross check that no electronic votes were also taken from the same voters during the time the fall back was operating.

A paper fall back system requires the usual election security of a paper election. If the fall back system collects valid voted ballots, then transport and logistic security for the paper ballots is needed all the way to the count.

Question: How would ongoing technical security audits be managed?

Technical audits need to happen as often as the systems are changed, upgraded or serviced. These audits happen to a greater or lesser extend depending on the changes to the systems. The current model sees the system tested, audited and certified and then any changes to the system are passed through the same auditing process. The first audit is typically large and exhaustive, the subsequent audits are typically small, looking only at the "differences" introduced in the changes and upgrades.

Our system provides the ability to perform an exhaustive audit for every election (taking about a person week at most) and this confirms that the core parts of the election are true and correct in terms of security and integrity. This "per-election" audit has been performed with code auditors in Melbourne and London in other pilots. I describe this method because I think it will not require more effort than the incremental audits above but it will constitute a more practical and complete assessment of the system, even if there have been quite large changes to the software prior to the election.

Question: Given the election date is set and then can't be moved, how would changes (other than the voting software) be managed if they were required immediately before the election date? (i.e. what would you do if Microsoft released a security patch the week before the election)

Firstly, none of the server equipment provided by Everyone Counts uses any Microsoft product and use of third party commercial software is strictly limited and controlled. The systems are built from open source software.

That said, there are security patches released by open source application providers, security related patches are typically reported on CERT and other websites which we receive notifications from when open source software needs updating.

Security patches could be applied to the server close to the election under certain conditions and with the cooperation of the auditor(s) who maintain a reference copy of the system. Those conditions would include what part of the system was being patched (operating system, application software etc), how serious the security vulnerability being addressed was and whether system testing would be needed to confirm end-to-end functionality.

Question: If the voting system is internet based, how would you guard against denial of service attack?

While DDoS defence is an open problem there have been successful defences against large DDoS attacks. Some of these techniques can be applied to the Internet voting servers. They include offloading work (we do this already by having the Java applet manage the voter's session entirely), using authentication and encryption (so that attacking systems need to authenticate and encrypt) or engaging a service that can filter high-bandwidth attacks and forward legitimate traffic to the voting servers.

We have published research on a new approach to DDoS which could be called a "Peer to Peer Internet voting service" which does not rely on central servers. A distributed network of servers (150 were used in the last test) act as pick-up points for votes from voters' PCs. In a real election the electoral agency would offer up its infrastructure or government infrastructure to be the distributed network. Each machine is just a relay to a hidden service that collects the votes. Since all votes are encrypted, they are not at risk as they traverse this network. Our work was published in EGOV05 (see http://www.everyonecounts.com/uploads/File/ivcp.pdf).

Question: If the voting was local based with no network, how would you ensure the vote is recorded as the voter intended?

The vote is recorded as the voter intended if there are adequate controls over the way software is developed, installed and maintained on the off-line voting servers and the computers used as voting client machines. These are the same conditions as are required above for the on-line system with the additional requirement that local servers and clients in a poll station need more security because they are physically more accessible to the general public and are handled by non-technical poll station staff.

Ensuring the vote is recorded (and counted) as the voter intended require adequate proof that the audited local server and client systems have performed as expected and that there has been no changes to these systems since they were audited.

Off-line system such as these do have a limitation the on-line systems do not. The off-line systems cannot allow a third party trust site to be used as the basis of a real-time check by the voter that the voting client software signature is true and correct. However, because the off-line system can enjoy more procedural security and can be set up without unknown software (as one might find on a remote voter's PC), and since there will necessarily be fewer network borne risks, this need to check the voting client software may be somewhat diminished.

The voter using an off-line system is not able to be told that their vote has been received by the central system where the count will take place since that central system is not accessible to the local network. Instead, the local server must emit the votes it has collected in some safe, measurably complete format and this must be sent to the central system. Scrutineers would act on behalf of voters in ensuring that all votes from poll stations were received in this manner. Special controls over the transport of the votes (such as what digital media are used and who accompanies the courier) would be needed as they are deployed in the transport of ballot boxes containing paper ballots.

Questions asked by Dr. Vaness Teague, taken from the Hansard transcript
http://www.aph.gov.au/hansard/joint/commttee/J11099.pdf

page EM57
"My main criticism to make of this trial is that for neither of these systems did the trial meet even basic standards of transparency, and I would like to contrast with the paper based scrutineering system that is familiar, and think about the way that we insist that the Australian Electoral Commission open up all the important parts of a paper based counting process to observation by scrutineers. This is a vital part of the whole process of counting the elections because it provides evidence of having got the right answer at the end of the day. There was no equivalent level of transparency provided for either of these electronic systems, and I strongly believe there should be. In a nutshell, that is my point of view."

We stated that Dr. Teague's concern for transparency is with merit, as we gave in our testimony in the above URL page EM44. It is my opinion that remote electronic voting can meet or exceed the scrutiny ability of postal voting and that remote electronic voting can certainly exceed the security and privacy of postal voting.

I have introduced further above, scrutiny is certainly possible and desirable for remote electronic voting, however we seek to determine the integrity of the system in necessarily different ways to paper voting. The goal is the same, that at base, two or more mutually distrusting observers should be able to seek evidence and observe processes to their mutual satisfaction such that neither party sees the influence of the other(s), that there have been no errors or omissions on the part of electoral staff.

page EM58
"There are two different kinds of transparency that are appropriate for these kinds of electronic voting systems. First, there should be more openness of the details of the system, the source code and the system design, available months before the election to more security experts so that they can look at the system and identify possible security errors and, hopefully, contribute to fixing them. The more security experts who look at the system, the more secure it is likely to become."

We concur and have provided such details in other elections to the electoral agency, academics and others. We would welcome a process such as the above and agree that this needs to happen early enough for there to be a fair right of reply to any identified problems or suggestions made in such an analysis. We would like to see an agreed third party chosen to mediate and help determine if system changes are needed or not, and how intermediate and final outcomes of the analysis process are interpreted for the public. This will ensure a balanced portrayal of the system risks and benefits. Of course the details of the analysis would be made public as well.

page EM58
"The second important kind of transparency is to recognise that the first thing still does not guarantee that the system that was so carefully looked at is necessarily the system that is running on the computers on the day, so the second kind of transparency is to try to design the system so that it provides evidence to voters that what they are asking the computer to do is in fact what the computer is doing for them. This is very difficult for internet voting—in fact, probably basically impossible. I think it is quite feasible for computers in the polling place kind of voting, like voting for visually impaired voters."

We provide a solution where the voter can directly confirm the authenticity and correctness of the the voting system they download and run in their PC browser. This is done by providing the entire balloting process in a signed Java applet with a digital signature the voters can check. Secondly the voters can confirm receipt and decryption of their votes via a receipt checking service. The traffic on this service with the absence of reported receipt mismatches provides an accurate measurement of the integrity of the server which has collected and held encrypted votes. Finally, the "back end" of the system is a dedicated computer which has also been audited and is kept off-line, with strict access controls. Scrutineers observe when the "back end" is used to decrypt and report on the election outcomes, which is only possible when a quorum of officials with keys attend and cooperate to decrypt the votes.

This arrangement, which is neither new nor technically elaborate, provides great confidence that votes are handled by the authentic, unmodified software. Likely there will be more innovations to add more layers of security and more choke points for scrutiny in this promising design. In contrast with off-line voting, there is no way to tell the voter that their vote has been received intact, at the central service that will decrypt their vote, while they are in the voting booth. There is no way to tell the voter that their vote has been received and decrypted by the ERO without using a networked service. The ability of the remote voter to check and validate a digital signature and likewise cooperate with trusted third parties is unique to Internet voting and provides assurances not possible in an off-line machine, nor via postal voting nor via paper voting.

EM59

"You can check to see whether your vote was successfully accepted,' this is not strictly true. You can ask the system whether or not it recorded a vote for you but you cannot check whether it is telling you the truth."

The receipt check provides the receipt the voter saw when they voted. It is practically impossible to obtain a voting receipt without decrypting the vote, and this decryption process is only possible in controlled, supervised conditions, off-line. The software audit ensures the voting applet receipting is performing as advertised on the Java applet. This means it is very difficult for the server to lie to the voter because it provides as proof a receipt only the voter and the ERO have.

Request (page EM54) from Senator Birmingham for supporting material on the Swindon UK electronic voting trial run by Everyone Counts.

Please see http://www.everyonecounts.com/downloads/icegov08_final.pdf

end.

A Thin Client for Networked Access to a Central Register and Electronic Voting Terminals

Craig A. Burton
Everyone Counts Inc

ABSTRACT

Networked terminals for marking the electoral register at poll places has been trialled at a number of sites (most recently [5]) allowing immediate detection of attempted multiple voting even in truly anonymous voting systems. We describe new technology piloted in 2007 in a binding local government election. Our commercial remote voting product eLect [1] was extended to provide new services. Firstly, networked register terminals replaced paper registers. Secondly, the networked register formed the basis of enabling single-vote access for poll-place electronic voting. Finally, poll place electronic voting machines were provided as stateless thin clients which were networked for real-time central aggregation of votes. A central server was charged with the coordination of 400 such voting and register machines at 64 sites. Register terminals also formed the basis of recording the issue of paper votes if the voter so chose, as these were provided to allow voting in the traditional manner. In concert with these systems, votes were also collected via telephone and web-based remote electronic voting services. The pilot has been judged a success by the central government.

Categories and Subject Descriptors

J.1 [**Administrative Data Processing**]: Government

General Terms

Experimentation, Security, Human Factors, Legal Aspects, Verification.

Keywords

Electronic voting, Internet voting, elections, voter registers, voter rolls, multi-channel voting, multi-modal voting, systems pilots

ICEGOV2008, December 1-4, 2008, Cairo, Egypt

1.INTRODUCTION

The use of general purpose computers within current Direct recording and Enumeration (DRE) type voting machines theoretically allows any kind of software to run and possibly attack votes collected therein. General purpose computers also require considerable maintenance because of their complexity. This design may be acceptable for ATM banking machines which enjoy perimeter security and are operated by experts. DREs must be set up by members of the general public and are kept warehoused for most of their operational life where they must be closely guarded.

The authors sought to employ a different approach to reduce the risk of insider tampering and provide systems which would be open to scrutiny and meaningful auditing whilst being easy to set up by poll place workers.

This document introduces a design for poll place voting which sees thin-clients used for remote access to a centralized register of electors and aggregation of votes. The solution is a network application making use of an open-source software foundation and asymmetric cryptography techniques. The report defines how the system was successfully deployed in Swindon, a regional UK city with 160,000 voters in concert with the normal Council election cycle. Swindon has been an active electoral modernization pilot site for several years (see for example [7]).

2.LOCAL ELECTIONS

In the United Kingdom, voters are required to attend only one specific poll place where their respective ballots await them, whereas the electronic systems were to be provided allowing any polling place to serve a specific ballot for any constituent in the entire district. A voter could still vote on paper, but this restricted them to their allotted poll station. In 2007 poll-place electronic voting was made available to all voters who could attend *any* station on the 3 May. For seven days prior to this, mini poll stations were provided at four libraries.

Two remote voting methods were also deployed in addition to postal voting: telephone voting and web-based (Internet) voting. Both remote electronic channels were available for 8 days including polling day. At close of polls, all votes were transported from the central aggregating servers to the count, publicly decrypted under supervision and used as the basis of totaling the count of postal and paper ballots at a conventional counting event.

2.1A centralized register

Electronic registers typically provide the basis of data capture, maintenance and publication of elector records (Swindon uses eXpress [3]). The most important task the system performs is the provision of printable registers for voting. The registers allow the Presiding Officer (PO) at the polling station to identify an eligible voter and record their having voted at that specific station. There is no risk of double-voting because registers at other sites do not list the same voter as eligible. The register also reflects whether the voter is a postal (absentee) voter and so should not be issued a ballot at a polling station.

Centralization of the register service required the provision of networked terminals which reproduced lookup of voter records with the same indication of whether the voter had already voted or not. The logistic challenge of this electronic register was not the provision of an electronic lookup service but reliable connectivity so that all register terminals would be on-line continuously throughout polling day as this service would support both e-voters and paper ballot voters.

2.2Network

A challenging aspect of the pilot was the requirement for a robust data network to support 275 voting machines and 125 register machines given that no sensitive information resides on any terminals providing these services. This was intended to reduce the exposure of votes captured on the systems which would otherwise reside locally in a more conventional DRE-type design.

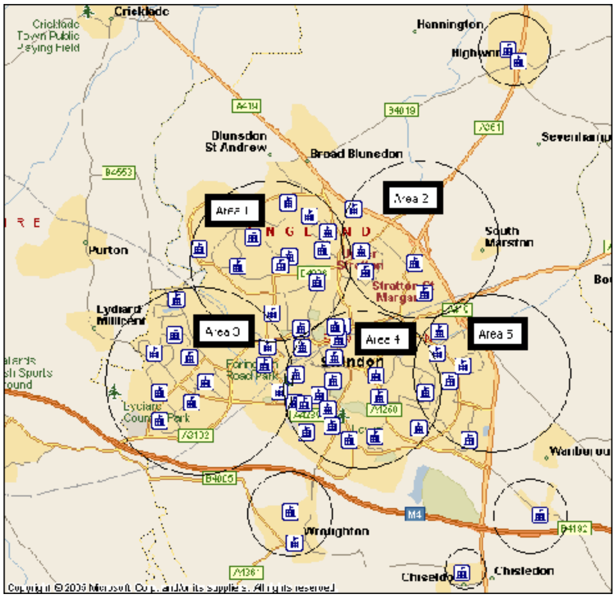


Figure 1. A WiMax network was installed to connect conventional polling stations to a network

To provide the network, the pilot established a 23 square mile WiMax data networking system (figure 1). WiMax is a standard for line-of-sight point-to-point networking which provides high data volumes in comparison to 3G. Given the varying terrain of the Wiltshire countryside and the various observations of poor 3G (and GSM) quality among the pilot staff, and consideration of related work [4] a dedicated WiMax network was built.

A tall building in the center of its business district was used as the WiMax base station. From here data were transmitted to five lesser base stations and from there, short-arc aerials reached each of 52 polling stations. A remaining 12 stations could not be reached by WiMax and alternative arrangements were made via Council-controlled fiber WAN (eight sites) and private broadband (DSL, at 4 sites). The pilot measured whether a satellite link could be used for one very remote site but early tests showed that this approach would not be reliable enough.

All poll place sites were provisioned with a 2Mb or better link. The WiMax network provided centralized DHCP for three private networks. The trunk of the network was provided by redundant feeds (a BT 5Mb DSL subscription and a spare capacity on the established network for SBC (8Mb unallocated on a 10Mb private feed from BT)). However, given the regional location of the pilot, both feeds originated from the one BT backbone.

Outside the WiMax trunk the voting network traffic traveled across the public Internet to a regional data center where a server array was installed in a private rack provided on managed (multi-homed) bandwidth and managed power. A secondary site was provided in London on stand-by if the primary failed.

At poll sites, the WiMax network was terminated by a local WiFi access point (Alvarion IDU). These were mounted in tamper-proof boxes within range of polling place desks and equipment planned for polling day. At non-WiMax sites, conventional WiFi routers were used (Netgear WGT64) and kept out of public areas.

2.3Poll place terminals

The pilot council rented 400 Hewlett Packard NC and NX-series laptops to form the basis of voting and register terminals at polling places. In all, fourteen models of laptops were provided, although all were recent models with at least 256MB RAM, 1.5GHz processors and WiFi (80211.b) hardware. All laptops were ordered without operating systems and with BIOS set to not allow Plug and Play, with a password. The hard drive of each laptop was provided blank. Time did not permit the removal of hard drives but this was the intention.

We provided boot images for laptops assigned as Polling Officer (PO) or Voter (VO) machines via CDR disks which booted laptops to become either register or voting kiosks. The boot image was created from a minimal build of the 2.4 Linux kernel. This was stripped to only allow it to boot the laptop, and activate the laptop's Ethernet and 80211.b hardware. The system relied on remote DHCP and external DNS services. Linux activated USB support for a computer mouse. No other services were activated. The there was a strong local firewall on each laptop.

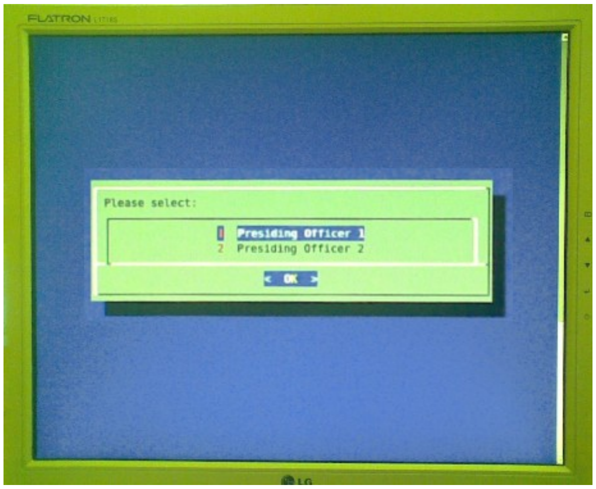
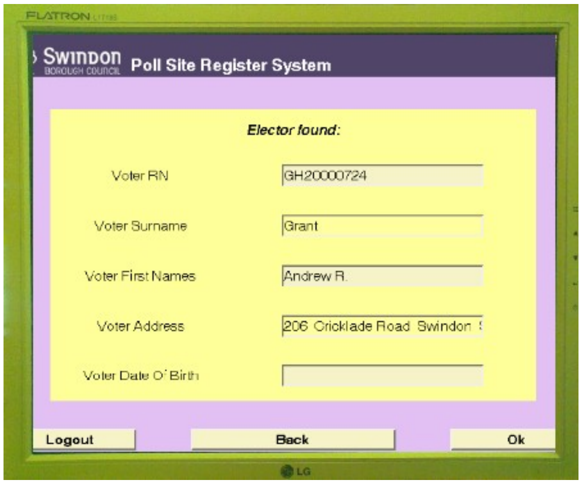


Figure 2. Boot sequence for a PO terminal: PO staff boot laptops from a CDR. A bash shell menu allowed the PO to choose a machine identity for each particular laptop. From this point, the Xfree86 windowing system provided the graphic interface, keyboard and pointer support. The system then launched Mozilla Firefox 2.0.0.2 in kiosk mode from the binary in memory. The system authenticated the PC to the server via an HTTPS client certificate challenge. The PO provided a prearranged terminal password.



Swindon Borough Council Poll Site Register System

Elector found:

Voter RN: GH20000724
Voter Surname: Grant
Voter First Names: Andrew R.
Voter Address: 206 Cricklade Road Swindon
Voter Date O' Birth:

Figure 3. The PO search interface. Once the terminal was authenticated to the server, the PO then provided a personal password for their particular session. Any session left idle for 15 minutes timed out and the PO password was required again.

The VO boot sequence was similar but required no PO password, with the machine instead going in to a polling loop for an authenticated session (described next).From either the voting or PO interfaces it was not possible to access the operating system or browser settings.

2.4Security

An existing remote voting application, "eLect" written by the authors in 2003[1] was adapted to allow polling officer-moderated voter authentication at poll places. As in 2003, voters voting over the Internet (remotely) keyed in their access codes. For telephone voting these codes are keyed in via the telephone keypad. Voter access codes were only issued to voters who had registered to use the web and telephone voting systems. The system was extended so that access codes would not be required in polling stations: it was a requirement that, like paper, the voter could attend, provide name and address and then vote electronically if they so wished without having to furnish any other information.

The PO terminal was given the ability to remotely activate a voting machine for a voter. The voting machines booted up and then polled a scheduler ("Sched" from here down) regularly to allow them to be activated for a voter.

An additional 850,000 dummy access codes were created and added to the application server database. These excess codes obfuscated the "live" access codes. If any of the dummy codes were used, they would be detected and excluded at the decryption stage. This would also show that there ad been attempts to guess access codes or that the access code database was compromised. The chance of an ordinary voter accidentally keying in one of these dummy codes is extremely low, but a hacker with access to the database picking ballot codes at random would have a high likelihood of using a dummy code and triggering the alert.

For poll place voting, we hosted a reduced version of the register on a remote database server ("Reg" from here down). This was physically separate from the database containing Ballot codes. This Reg database captured voter full name, address and DOB. This was keyed on the elector ID, a publicly known index of the voter's location within the Council district. The voter record also contained an asymmetrically encrypted voting codes.

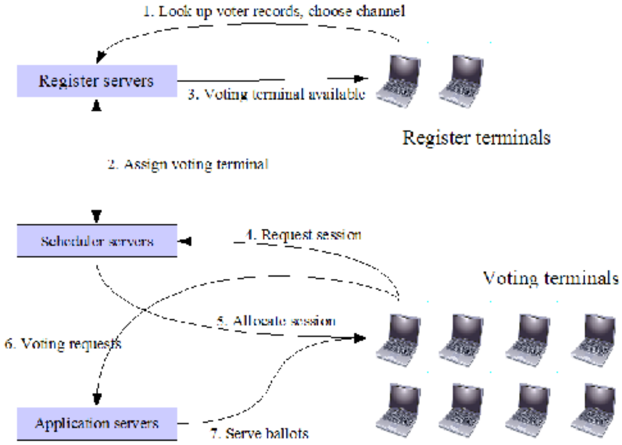
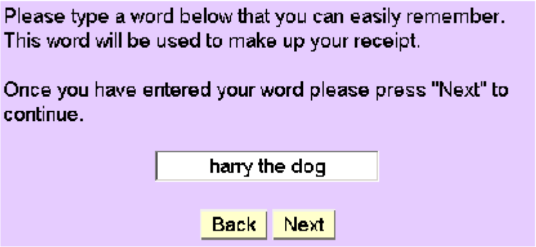


Figure 4. Allocating a voting machine. A PO having located a voter within the Register database 1. and having had a voting terminal allocated 3. first caused this encrypted access code to be sent to Sched 2. which was capable of decrypting the the code. All voting machines continually query Sched for active sessions 4. When a decrypted code is present for a voting machine this voting machine then logged in to the remote voting server 5. and the voting session begins in as if the voter were a remote voter 6., 7..

For remote voters who could not use the Java system in their web browser, an accessible alternative was provided using HTTPS and HTML forms for the browser which used the same Java applet running on the web server. The voter was also able to provide a keyword and get a receipt. The vote was encrypted on the server. We refer to this method as the "fail-over" and "SSL" voting interface. Note that users of the telephone voting system also had their votes encrypted but the receipting was not provided.

2.5Receipting

A tamper-proofing mechanism was provided which relied on voter receipting. Receipt creation and checking involved the voter providing a "keyword" they could easily recall (figure 5) and then checking a receipt after close of polls (figure 6).

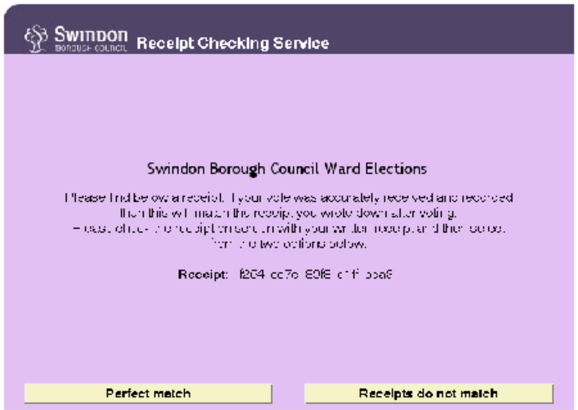


Please type a word below that you can easily remember.
This word will be used to make up your receipt.

Once you have entered your word please press "Next" to continue.

harry the dog

Figure 5. Voter entry of a 'keyword' they make up. A 12 digit alphanumeric receipt is created from this keyword, server salt and voter codes. The receipt travels back in the encrypted vote.



Receipt Checking Service

Swindon Borough Council Ward Elections

Please find below a receipt. If your vote was accurately received and recorded then this will match the receipt you wrote down after voting.
Please check the receipt on screen with your written receipt and then choose from the two options below.

Receipt: f204 cc7c 80f8 c1f bba8

Figure 6. Receipt checking services available at close-of-polls. The voter can log in to this services and check the receipt displayed to them matches. If the vote has been received and decrypted the receipt is correctly shown.

If there is a challenge to the election, a random sample of voters can be called to provide receipt keywords to give statistical proof of the correct carriage of the votes. Voters checking receipts as above forms the basis of a statistical measure of system correctness as receipt check "fails" and "passes" are reported by the system and the voters. By Bayesian product, if roughly 1% of voters check receipts and report no mis-matches, then there is a 99.94% likelihood of detecting damage or corruption to 0.5% of all votes.

2.6Testing and Audit

As previously covered [1] the system provides for distributed trust among a code-auditor and election officials controlling cryptographic keys. It is anticipated that a code audit of the entire code base would not be practical or complete enough due to its size. The need for incremental security patching at a far greater frequency than comparable DRE maintenance requires a more incremental certification, at least one with reduced scope that will cover a specific election. The Java software source codes for a specific election are exportable from the management system. These source codes are intended for independent audit and publication, compilation on a known good compiler and then end-user verification of an auditors digital signature for a Java applet that provides the election. The voters themselves can verify the audit by examining the Java applet signature in their web browser before they start voting. This prevents changes on the server being able to affect the election.

There are six auditing tasks which can be executed against the eLect system to provide assurance that the system does what it is meant to do. With increasing scope they are

1. functional, load and end-to-end testing with dummy configurations – a black box suite of tests
2. parallel testing during an election – black-box testing
3. source code analysis for a specific election – a deep code-level audit of software and configuration
4. encryption-decryption system audit - a deep code-level audit of software libraries discussed in [2].
5. forensic analysis during and after an election – forensics
6. code base and system configuration auditing – a white box suite of tests

The system created Java applets with all Swindon candidates, graphics, instructions and other election-specific content and had the applet's source code analyzed and certified as containing no malicious software nor logical errors or omissions. The Electoral Returning Officer (ERO) for Swindon viewed the ballot faces rendered by these applets for their legal accuracy and completeness. A contracted penetration (PEN) tester ran scheduled PEN tests against all servers in both Birmingham and London, right up to the election. The Ministry of Justice engaged its own PEN testers who, informed by our auditor PEN report, performed other tests. The consortium lead ran other tests against this system including scripted load tests, boundary tests, black box and end-to-end tests in a variety of scenarios.

3.LIVE VOTING

Voters who wanted to use telephone and remote Internet voting were required to register. This registration process was executed over 30 days and was closed 8 days before polls opened. The process involved the voters submitting a DOB and a six-digit password to SBC. In a reply paper letter the voter was issued with a Ballot Code (BC). This exchange provided an out-of-channel registration and being two-way meant that the secrets required for voting were shared between the voter (who set their own PIN) and SBC (who set the BC). Intervening in this registration process would require observing (but not interrupting) both the incoming and outgoing letters. Voting with a voter's remote login codes would be detected as a voting session can only occur once and a spent session is reported to the legitimate voter when he/she attempts to log in.

A voter either organized to remote vote with their own login codes, or they could attend a polling station as they had in the past and vote electronically without any prearranged codes to access the system. It was possible for a voter to vote electronically at any of the 65 polling stations. A voter who wanted to vote on paper had to attend their local polling station. It was not possible to vote more than once by using multiple channels.

The electronic voting process progressed in five stages:

1. Authentication (for telephone and remote Internet users)
2. Voting steps for Borough and/or Parish ballots (and candidate information via Internet)
3. Confirmation of the voting choices
4. Creation and issue of a receipt (except for telephone voting)
5. (optionally) confirmation of the voting receipt after close of polls

3.1Presiding Officer Process

Volunteer Presiding Officers (POs) were trained by the pilot site staff using the pilot system set-up to practice the assembly of a large polling station. POs were trained in the set-up of both voting and register machines. This training was an adjunct to their normal training for paper processes, held some days in advance of polling day. POs were then allocated laptops which were assigned to their polling stations. The laptop bags had seals on them which were examined when removed on polling day. The day before polling day, POs were issued the boot disks and instructions for their polling station.

The PO received a person wishing to vote and asked for their surname or British Register Number (RN). The service allowed queries on either and returned a single result (for RN) or possibly several results if searching on surname. The PO could then resolve a unique record by asking the voter for their forename and address. If the voter was eligible to vote, the system would advise the PO to offer electronic voting. If the voter was attending their registered poll place the system advised the PO to also also offer the voter a paper ballot. If the voter requested an on-line vote, the PO pressed the appropriate button on the interface and the system advised the PO to direct the voter to an available machine. If the voter asked for a paper ballot, the PO pressed a button on the interface and the voter having voted paper was recorded. If the voter had already voted, or was not eligible, the system reported this.

3.2Polling Data

Twenty borough wards had elections in 2007. Two of these wards also held parish council elections. A total of 142,317 electors representing 95.8% of the Council's 148,603 electors were able to participate.

At 7am on the 26th of April 2007 remote telephone and web voting were opened. In addition, from 9am, five libraries provided early voting via a poll-place setup. Because the libraries were not conventional polling places, they did not offer paper ballots. The poll place early voting ran until 6pm on the 2nd of May. During this time, we captured 296 votes which matched expectations for the new poll sites. Early voting via phone and Internet captured 8,163 votes for 13,234 registrations. On polling day, the combined services captured another 3,106 votes, making up 24.1% of all collected votes.

We experienced no security events apart from a basic port scans of the server. The server system was available 100% during the polling period. There were no issues at decrypt to indicate the use of dummy codes.

On polling day, overall service availability at poll stations was 96% with only two sites using all-paper registers and ballots. Of the 36,425 votes collected overall, 4010 were collected on fall-back paper registers outside of both the electronic register. These inked registers were cross-checked before decrypt for duplicate botes and none were found. The register took 151,963 requests, the voting system took 90,857 requests.

3.3Issues and Resolutions

A configuration issue constricted the duration of a telephone voting session to 180 seconds. This was resolved at 10am on Apr 28. Logins to both telephone and Internet systems were initially not possible for about 10% of remote applicants because of a printing error which resulted in login codes missing digits. The Council re-issued these voting codes within 24 hours.

Providing e-voting and register terminals prior to voting allowed us to see and fix early problems with this new voting method. There was an early configuration issue which caused one of the two e-voting interfaces to not work. Instead, voters voted the "fail-over" SSL method. This was identified and resolved after 3 days. For voters who had already voted, the system presented an unintended "logout" button. If the voter clicked this, they were taken out of the intended series of pages of the interface and the terminal had to be reset. This happened infrequently and was not addressed during live voting.

Library and poll station sites experienced connectivity issues. It was determined that laptops requesting DHCP needed to request longer than 10 seconds as the WiMax network at some locations dropped DHCP broadcast and reply packets. Any loss of network for either voting or register machines was re-established with browser CTRL-R or by resetting the machine in question.

Polling officers at a number sites reported they had problems with the system identifying some eligible voters. This was identified as a training issue and was exacerbated by the constraints of the pilot. Specifically, the system identified that a voter had voted Ward but no Parish and this was misinterpreted as the voter having already voted. An information sheet was sent to all voting stations during polling.

4.DISCUSSION

Providing e-voting and register terminals prior to voting allowed us to see and fix early problems with this new voting method. There was an early configuration issue which caused one of the two browser e-voting interfaces to not work. Instead, voters voted the "fail-over" SSL method. This was identified and resolved after 3 days. For voters who had already voted, the system presented an unintended "logout" button. If the voter clicked this, they were taken out of the intended series of pages of the interface and the terminal had to be reset. This happened infrequently and was not addressed during live voting.

Library and poll station sites experienced connectivity issues. It was determined that laptops requesting DHCP needed to request longer than 10 seconds as the WiMax network at some locations dropped DHCP broadcast and reply packets. Any loss of network for either voting or register machines was re-established with browser CTRL-R or by resetting the machine in question.

Polling officers at a number sites reported they had problems with the system identifying some eligible voters. This was identified as a training issue and was exacerbated by the constraints of the pilot. Specifically, the system identified that a voter had voted Ward but no Parish and this was misinterpreted as the voter having already voted. An information sheet was sent to all voting stations during polling.

Twice as many voters voted on the Java applet than the SSL "fail-over" system, the opposite was true in a similar run in [8]. Telephone votes were judged to be quite low given the number of calls through the VoIP provider. This is possibly due to early problems for remote voters and an issue with telephone voting session length being initially constricted.

Early voting in libraries matched expectations for uptake. As a proportion of library customers at those sites in the designated times, few people chose to vote. However, libraries have not traditionally been a site for voting, which takes place at prescribed polling places; and citizens attend libraries for other reasons and e-voting may seems incongruous.

Use of the laptops for voting at poll places was lower than expected, with the majority of people requesting paper ballots. It is likely that older voters chose paper over electronic voting, however, the analysis of this data is yet to be provided and young people were observed to also request paper. Swindon too had greater rate of postal voters this year, but the UK has publicized postal voting via all-postal pilots in other regions which is likely to have made this voting option more visible.

5.CONCLUSION

Using cheap, available hardware and open source software, the authors created voting and register terminals from PC laptops with the Internet as the backbone for services. This service allowed voters from any locality to attend and receive the right ballots no matter where they voted. The service also reinforced the traditional paper voting process with electronic register terminals being used for lookup of voters.

Uptake of the services was fairly modest but was in keeping with previous pilots locally and nationally and is not surprising given the novelty and scale of this pilot e-voting which was offered to all voters in one form or another in addition to paper balloting and postal balloting.

Minor problems may have affected overall attendance on the e-voting systems, however, given the compressed delivery times, limited publicity and the novelty of the “vote anywhere” service, citizen uptake was encouraging with nearly a quarter of all votes cast electronically.

Training of the polling officers is, in our estimation, the lynch pin in a new provision of services which the general public must use. Presiding Officers are the front-line to the general public and must present as competent providers of the systems. Time for Swindon training was adequate for the traditional voting process and most staff were experienced, but it is our assessment that a half-day training period be provided to staff where the entire voting cycle is enacted many times and various system warnings and errors are elicited and discussed. A hurdle should be provided for staff who would be appointed as the 'Technical Presiding Officer' at voting sites.

6.ACKNOWLEDGMENTS

We would like to thank the UK Ministry of Justice for including us in Electoral Modernization Program and the feedback and guidance it has provided to make this pilot successful. We would like to thank Alan Winchcombe, Deputy Returning Officer of Swindon Borough Council and his staff for their cooperation and support. We would like to thank TATA Consultancy Services for its role in consortium lead and the various logistic, evaluation and management support people it provided. We would like to thank eXpress for its support in integration with UK electoral registers.

7.REFERENCES

[1] Burton C. A Virtual Private Network for Internet Voting, 2003, http://www.everyonecounts.com/uploads/File/Virtual-Private-Network.pdf cited 28 August 2007

[2] Burton C. An emitted-code model of configuration control and practical audit of e-voting software, 2006, http://www.everyonecounts.com/uploads/File/emitted-code.pdf cited 28 August 2007

[3] eXpress Software Solutions Products http://www.xssl.co.uk/Products/register.htm cited 30 October 2007

[4] Miles S.Milton Keynes to get blanket WiMax coverage (2006) http://www.pocket-lint.co.uk/news/news.phtml/4384/5408/milton-keynes-gets-wimax-coverage.phtml cited 28 August 2007

[5] United Kingdom Electoral Commission Electoral pilot scheme evaluation Sheffield City Council August 2007 http://www.electoralcommission.org.uk/files/dms/Sheffieldstatutoryevaluationreport_27185-20105__E__N__S__W__.pdf Cited 28 August 2007

[6] United Kingdom Electoral Commission Pilot scheme evaluation Sheffield City Council 1 May 2003 Part A. http://www.electoralcommission.org.uk/files/dms/Sheffield_PartA_10204-8253__E__N__S__W__.pdf Cited 28 August 2007

[7] United Kingdom Electoral Commission Pilot scheme evaluation Swindon Borough Council 2 May 2002 http://www.electoralcommission.org.uk/files/dms/Swindon-final_6707-6259__E__N__S__W__.pdf cited 28 August 2007

[8] United Kingdom Electoral Commission Pilot scheme evaluation Stratford on Avon District Council 1 May 2003 Part A

http://www.electoralcommission.org.uk/files/dms/Stratford_PartA_10218-8267__E__N__S__W__.pdf cited 28 August 2007