Towards Best Practice for E-election Systems
Lessons from Trial and Error in Australian Elections

Richard Buckland[1], Vanessa Teague[2], and Roland Wen[1]

[1] School of Computer Science and Engineering,
The University of New South Wales,
Sydney, Australia
{richardb,rolandw}@cse.unsw.edu.au
[2] Department of Computer Science and Software Engineering,
The University of Melbourne,
Melbourne, Australia
vjteague@unimelb.edu.au

Abstract. Research on mitigating vulnerabilities in electronic elections has focused mainly on developing cryptographic voting and counting schemes that satisfy strong mathematical requirements. However many practical problems with e-election systems in general cannot be solved by cryptology. In this paper we consider some of these practical problems by examining deficiencies that are common to the many e-election systems currently used in Australia, including but not limited to e-voting and e-counting systems. We identify poor practices in the commissioning, development, operation and scrutiny of these systems, and we then make recommendations for improving practice. We argue that best practice guidelines for e-election systems need to be explicitly articulated and should include four key elements: failure-critical engineering, risk assessment, a culture of audit and strong transparency.

Keywords: Best practice, electronic elections, e-voting, failure-critical engineering, strong transparency.

1 Introduction

Australia has a long tradition of trustworthy election conduct. The manual execution of elections in Australia is professional, carefully performed and open to public scrutiny. However over the past decade much of the conduct of Australian elections has moved from the manual into the electronic realm, without maintaining the level of quality and transparency achieved with paper-based elections. Election administrators throughout Australia (and the rest of the world) will have to decide on the appropriate way to extend their tradition of election quality and transparency to new technologies, or risk eroding election integrity and public confidence. Our aim in this paper is to identify some shortcomings in current practice and offer suggestions on how to make electronic election processes more secure, reliable and transparent.

A. Kiayias and H. Lipmaa (Eds.): VoteID 2011, LNCS 7187, pp. 224–241, 2012.

E-election systems (that is, any IT system used for elections) in Australia date back to the implementation of the world's first electronic electoral roll in 1967 [27,28]. Since then a vast array of e-election systems has been adopted for almost all aspects of election conduct, and Australian elections have become heavily dependent on these systems. Although publicly available information on Australia's e-election systems remains scant, the little that is available reveals systemic problems. It is apparent that e-election systems are commissioned, developed, operated and scrutinised according to standard industry practices for *commercial* IT systems. These practices are entirely inadequate for *failure-critical* e-election systems, where the operation of the systems is infrequent, intensive, based on secrecy, and where mistakes are not publicly visible and often not even privately evident. The risk these factors pose is of course compounded by the considerable financial incentive for malicious agents to fraudulently manipulate system vulnerabilities to affect election outcomes. These shortcomings in IT practices are most evident in e-voting systems, which have the most stringent requirements, but are equally detrimental to the quality of all other e-election systems.

In this paper we shed light on some of the issues that have been made public and discuss how to address the problems that cause them. The focus of this paper is the practical issues that are common to all e-election systems. Our coverage does not include cryptographic protocols — the fact that Australia does not use cryptographically verifiable e-voting and e-counting schemes is a separate concern. The measures we propose are intended to be used in addition to appropriate cryptographic techniques.

The contribution of this paper is two-fold. First, we gather together in one place the publicly available information on recent incidents in e-election systems deployed in Australia. This is important as it permits analysis and discussion of the common underlying systemic causes, rather than allowing the problems to be treated as a series of independent and isolated incidents. Second, we consider best practice for e-election systems and identify four essential elements. Our intention is to propose a reasonable starting point for developing best practice guidelines for e-election systems.

The structure of the paper is as follows. We begin with an overview of the e-election systems used at present in Australia. Then we examine the four proposed elements of best practice for e-election systems in turn: failure-critical engineering, risk assessment, a culture of audit, and strong transparency. For each element we identify current problems and the steps that are necessary to address these problems.

2 E-election Systems in Australia

Each public election in Australia is administered by a centralised independent electoral commission. The Australian Electoral Commission manages federal elections, and state electoral commissions manage state elections and most local government elections. Electoral commissions employ permanent, full-time

election officials and are responsible for all aspects of electoral administration. This includes conducting elections, reporting on election irregularities, enrolling voters, registering candidates and political parties, redrawing electorate boundaries, educating voters and monitoring political donations.

This centralised approach contrasts with the predominantly decentralised arrangement in the US and most European countries, where the responsibility for conducting elections is typically delegated to the level of local government. Centralisation provides opportunities for economies of scale and professional election administration, but also increases the potential impact of flaws in the e-election systems used.

To help perform their numerous duties and to improve access to the democratic process for voters, each electoral commission has developed its own suite of e-election systems for e-voting, e-counting, electoral roll management and general election administration. This section describes a number of these systems. We focus on those of the largest electoral commissions, namely the Australian Electoral Commission (AEC), the New South Wales Electoral Commission (NSWEC) and the Victorian Electoral Commission (VEC), as well as the Australian Capital Territory Electoral Commission (ACTEC), which was the first to introduce e-voting in Australia.

2.1 E-voting Systems

E-voting systems are attractive in Australia because their flexibility affords high degrees of accessibility and usability, which makes them well-suited to situations where current voting arrangements are inadequate. This is important in Australia, where very strong emphasis is placed on participation in elections. Indeed voting is compulsory. Consequently electoral commissions provide an unusually wide array of voting arrangements to cater for the diverse circumstances of voters. E-voting is becoming more popular as an additional voting option. To date several systems have been trialled or permanently adopted with the purpose of providing an alternative to paper-based voting for voters with visual impairment, voters from a non-English speaking background, and voters living in remote areas or located interstate or overseas.

In 2001 the ACTEC trialled a voting machine system called the Electronic Voting and Counting System (EVACS), which was developed by Software Improvements [3]. EVACS is now used on a permanent basis in major polling places. Each EVACS voting machine displays instructions in a choice of languages, and certain machines designed for visually impaired voters have special facilities including large screens, headphones and audio instructions. In 2007 the AEC conducted a trial for visually impaired voters using EVACS based voting machines [8], but the system was abandoned because of the excessive cost.

The VEC adopted Scytl's Pnyx.DRE voting machine system for visually impaired voters in 2006 [39] and rolled out the system on a larger scale in 2010. All machines have features for non-English speaking voters and visually impaired voters.

Remote e-voting systems remain less common in Australia but have recently garnered increased interest. The AEC conducted a remote e-voting trial in the 2007 Federal Election using the eLect remote voting system by EveryoneCounts [9]. This was for Australian Defence Force personnel deployed overseas and permitted voting only on designated computers connected to a secure private network. The system was later abandoned again due to cost factors.

Most recently the NSWEC has developed a modified version of eLect, called iVote, for large-scale Internet voting during the 2011 NSW State Election. Initially the iVote system was only intended for visually impaired voters and voters living in remote areas. Shortly before the election the scope was substantially expanded to include interstate and overseas voters, as well as voters with *any* disability, including for example poor literacy skills.

2.2 E-counting Systems

E-counting systems have been used in Australia since the late 1980s for the single transferable vote (STV), which is a preferential system for proportional representation. All upper houses of parliament, some lower houses and many local governments are elected with STV. In most cases the votes are counted electronically. This is because the STV counting procedures are sufficiently complex that manual counting is infeasible in large-scale elections.

As multiple variants of STV are used throughout Australia, each electoral commission has its own e-counting system. These systems perform the vote counting and generate detailed statistical reports, many of which are published on electoral commission websites. In response to the desire for enhanced functionality and frequent changes to the STV counting rules, e-counting systems are constantly upgraded or redeveloped. For example the NSWEC has developed at least five new e-counting systems over the last 20 years [29,31].

The e-counting systems also require data capture systems to convert votes from paper ballots into electronic form. Since it is very difficult to ensure the accuracy of automated data capture for preferential ballot papers, almost all the data capture systems currently in use are for manual data entry. The data capture systems provide extensive reporting functions to enable thorough verification of the electronic data against the paper ballots. In the event that e-voting is permitted, the electronic ballots are printed out and then manually entered along with the paper ballots.

An exception is elections in the ACT, where electronic ballot data from the e-voting system is uploaded directly into the e-counting system. In 2008 the ACTEC began using an intelligent character recognition system to scan all paper ballots, but this still involves intensive manual verification [4].

2.3 E-election Systems for Electoral Roll Management

Australia has long used e-election systems for electoral roll management. The primary purpose of these systems is to ensure the roll is accurate and complete, and this is vital given that enrolment and voting are compulsory.

The AEC maintains the national roll, which until recently was used by all state electoral commissions under a joint roll agreement. Enrolment information is mainly provided by voters, and so e-election systems are used by AEC staff to process these applications. Since 2004 the AEC has been developing the General Enrolment, Elections Support and Information System (GENESIS) to replace several legacy e-election systems, and the module for adding and updating voter enrolment details was launched in 2010 [10].

There are also efforts to improve convenience for voters when enrolling and updating their enrolment. Since 2010 the AEC has provided SmartForm online enrolment applications (interactive Adobe Acrobat forms), and it is currently developing a custom online enrolment system.

The trend though is to fully automate the enrolment process so that voter interaction is no longer required. This approach has been advocated to improve completeness of the roll because roughly eight percent of eligible voters are not currently enrolled [11]. In 2010 the NSWEC ended the joint roll agreement with the AEC and began using its SmartRoll automatic enrolment system to add eligible voters to the roll according to data collected from other sources. The VEC followed soon after with its own system and other states are contemplating similar moves. But federal legislation prohibits the AEC from adopting automatic enrolment.

However automated data collection is nothing new. To enhance roll accuracy, electoral commissions have continually been developing ever more sophisticated systems for data collection and data matching. In addition to basic information such as name, address and date of birth, a wide variety of secondary personal information is collected from numerous sources to facilitate data matching, and this can include occupation, previous addresses, phone numbers, drivers licence numbers, tax file numbers and scanned documents containing signatures.

Electronic systems are also used to extract and distribute electoral roll data, for instance to print certified lists of the voters in each electorate for roll marking during elections. In most elections certified voter lists are printed on optical answer sheets, which are later scanned and then uploaded to electronic reporting systems to check for multiple or non voting. Each polling place has copies of the certified list only for the electorate in which it is located. This leads to difficulties in identifying voters for absent voting, where voters attend polling places outside their own electorate.

To address this problem the NSWEC developed the iRoll system in 2007 [29]. This stores the certified lists for all electorates in the state on PDAs or laptops at every polling place, and thus enables polling officials to verify the enrolment details for absent voters. The ACTEC has adopted an enhanced version of iRoll to mark all voters off the roll directly through PDAs [4].

2.4 E-election Systems for General Election Administration

Many e-election systems have been developed in Australia for a wide range of general election administration tasks. Reporting systems extract information from other systems to generate data for purposes such as verifying election

integrity (for instance by tracking ballot boxes and detecting multiple voting) and internal research to identify problems and plan for future elections. Logistical systems are used for operational issues including managing candidate nominations, ballot draws, polling places, polling staff, postal votes, ballot papers, ballot boxes and manual vote counting.

While most of the e-election systems are for internal use, online systems are becoming more common. Voters can now verify their enrolment details online. For the 2010 Federal Election the AEC deployed two online systems: the Online Recruitment System for the public to apply for temporary employment as polling officials, and the Checkpoint system for training polling officials [10].

Online systems have also been used to promote open and broad consultation. A good example is the procedure for electorate redistributions, where electoral commissions periodically redraw electorate boundaries to reflect population changes. To prevent gerrymandering, redistributions involve public inquiries that take place in multiple stages, and any group or individual can submit comments and objections. These inquiries are now conducted online and all the documents and submissions are located on electoral commission websites.

The large number of e-election systems in use and the desire to provide online interaction with these systems for both voters and electoral commission staff has motivated the need to integrate these systems and expand interoperability. Indeed this is the reason behind the AEC's ongoing GENESIS project. Likewise the NSWEC implemented a web-based Election Management Application for similar purposes, and this was deployed in 2006 [29].

3 Failure-Critical Engineering

E-election systems are failure critical. Failures in any of these systems could have extensive and catastrophic consequences for overall election security and integrity, as well as undermining public confidence in the electoral process. To maintain the quality and trustworthiness of elections, rigorous failure-critical engineering practices need to be followed to ensure that e-election systems are of the highest standard.

3.1 Current Problems

In Australia e-election systems are currently treated as regular commercial IT systems instead of failure-critical systems. This approach has resulted in a large number of systems failing during crucial periods. The problems are most evident throughout the software development process, where "the gap between the best software engineering practice and the average practice is very wide — perhaps wider than in any other engineering discipline" [19].

For example, the NSWEC iVote system suffered multiple failures during the 2011 NSW State Election [33]. The most critical incident was the corruption of votes by problems with the client-side JavaScript.

The iVote user interface required voters to enter their preference rankings in order, starting from 1. This was done by selecting a candidate and then pressing

the letter 'N' to allocate the next preference ranking to this candidate. However the NSWEC discovered 43 ballots where the letter 'N' was stored as a preference in place of some of the numerical preferences. This shows how a single, minor software bug has the power to corrupt votes without being detected by voters, and raises doubts over whether *any* vote at all was cast as the voter intended.

Furthermore the iVote back end had inadequate input validation and error reporting functions to identify invalid votes; the vote corruption was discovered only when election officials noticed a discrepancy between the number of electronic ballots cast and the number of ballots printed for counting.

This incident demonstrates failings in the software design, implementation and testing. In addition we observed that iVote compromised core requirements. Notably iVote was supposed to provide audio instructions, like all other Australian e-voting systems for visually impaired voters. However this requirement was dropped.

Critical incidents have occurred previously in NSW elections. During the 2003 NSW State Election the e-counting system experienced irrecoverable failures, and this led to delays in publishing the final result [31]. The problems were in part due to a lack of input validation and error reporting functions in the vote data entry system. Additionally there were separate problems with database configuration and maintenance. The e-counting system also suffered from less critical bugs such as inexplicable error messages.

These basic defects were not discovered during extensive end-to-end functional testing. The heavy reliance on such high level testing techniques appears to be commonplace. Similar functional testing was performed on the ACTEC's EVACS counting module [3], which likewise experienced failures during the 2001 ACT Election [25].

Of particular concern is that end-to-end testing is used to verify the correctness of the counting algorithm implementation in e-counting systems. The value of black box testing methods for this purpose is highly questionable because STV counting algorithms are extraordinarily complicated and prone to subtle implementation flaws. Indeed there are several instances in Australia where even the legislation specifying the STV counting procedures contains omissions and/or internal conflicts, so that it is mathematically impossible to count the votes according to the prescribed algorithms [40]. The fact that such legislative irregularities were not discovered when the e-counting systems were being specified, developed and tested reflects shortcomings in the testing as well as the specification of these systems.

The lack of testing rigour is widespread. Critical failures have occurred with the iRoll system for marking voters off the roll using PDAs. In the 2007 Tasmanian State Election, iRoll experienced data corruption when uploading the details from the PDAs, which resulted in the inability to determine whether 500 voters had been marked off the roll [37]. To address this problem the ACTEC enhanced iRoll so that the PDAs immediately backed up the data to a master PDA in each polling place via Bluetooth. The backup system failed during the

2008 ACT Election [4]. Fortunately no PDA problems arose on that occasion and no data was lost.

In the 2010 Federal Election AEC staff reported extensive failures with the enrolment processing module of GENESIS, the Online Recruitment System and the Checkpoint online training system [20]. The problems included poor performance (partly due to insufficiently powerful server hardware), poor usability, missing functionality and glitches such as freezes, crashes and outages. This created numerous and unprecedented challenges for AEC staff and required temporary workarounds to counter issues with the systems.

The testing processes for these projects had serious shortcomings. AEC staff identified problems with GENESIS in early user testing but these were dismissed, and the Online Recruitment System did not undergo any live testing prior to launch despite concerns raised by staff [20].

Many of the problems with GENESIS have stemmed from inadequate requirements analysis. An audit of the AEC's conduct of the 2007 Federal Election by the Australian Auditor-General found that a poor understanding of the requirements for GENESIS contributed to a delay of over three years to the completion date so far (now estimated to be the end of 2014) and a cost blowout from $27 million originally to between $56 and $60 million now expected [2].

There are also indications of problems with code design and implementation. The public source code for the ACTEC's EVACS was separately reviewed by researchers from the Australian National University [1] and the University of California, Davis [23]. Their studies found unclear design, large amounts of duplicate code, complex control flow, minimal error checking, memory leaks and hard-coded values. It seems fair to expect similar software risks in other e-election systems in Australia. EVACS has at least had the advantage of allowing open scrutiny, and as a result some of these problems have since been fixed. Given that no source code for any other systems has been publicly disclosed, the quality of the code for these systems is likely to be worse.

One of the main reasons behind all these failures is that electoral commissions are not equipped with the requisite expertise and resources to establish and implement failure-critical engineering practices. Although the NSWEC acknowledged this when assessing the failures of its e-counting system [31], the same practices still persist in Australia.

At present it is commonplace for electoral commissions to engage consultants to manage e-election projects, and to outsource part or all of the development, evaluation and operation of e-election systems to private contractors or vendors. However these external parties are general IT practitioners rather than specialists in failure-critical systems. Consequently electoral commissions have very limited capabilities to ensure the quality of these systems.

Outsourcing in this manner has had catastrophic consequences for Dutch e-voting systems [32]. The problem is even more concerning in Australia because of the heavy usage of and reliance on e-election systems for almost all facets of election conduct.

3.2 Towards Best Practice

E-election systems must be commissioned and managed as failure-critical systems. The inherent complexity of IT systems makes it very easy to inadvertently or deliberately introduce defects into a system during the development process, and at the same time makes it notoriously difficult to detect and eliminate all the defects. Likewise the operation and use of IT systems is highly vulnerable to human error and malicious activity. Best practice for e-election systems must adhere to engineering practices that are specifically designed to mitigate these problems from the outset and to ensure security, reliability and usability.

In more mature domains, failure-critical engineering has proven to be successful in developing the highest quality systems such as avionics systems, medical equipment and even computer hardware. For example comprehensive and systematic techniques (such as formal specification and verification) are employed to minimise the introduction of defects and produce objective evidence that the systems are secure and reliable. Robust safeguards are built into the systems so that potential failures can be detected, reported and handled gracefully, rather than causing a total and possibly unnoticed collapse.

Best practice guidelines for the engineering of e-election systems can adopt many of these well-established practices and principles. Once these guidelines have been prescribed, the practices need to be overseen and implemented by a diverse range of suitably qualified experts with extensive training and experience in the necessary areas, including software engineering, failure-critical engineering and security engineering.

4 Risk Assessment

Risk assessment lays the foundation for sensibly managing and appropriately dealing with the risks involved in the development, operation and use of e-election systems. E-election systems have unique threats and vulnerabilities, with serious irreversible and far-reaching implications that may even extend beyond the electoral realm and into the public sphere. It is essential to enumerate all the risks and consider their potential impact. This permits well-informed management decisions to be made about whether or not to commission a system in the first place, and then if so what development processes are best adopted and what further technical and procedural safeguards are needed.

4.1 Current Problems

Current e-election system risk assessments in Australia suffer from multiple inadequacies, most notably in their narrow scope and lack of rigour. This has led to poor decision making that has exposed elections to high risks, and in a number of instances these risks have been realised.

There has been a consistent failure to properly assess the risks in software development, often resulting in foreseeable IT problems. In particular it has become the norm for new e-election systems to be developed on a tight schedule and

then to be deployed at the most crucial point of the electoral cycle. For example development started roughly *six months* before the election for the NSWEC's iVote, the AEC's trial e-voting systems and the ACTEC's EVACS. Given that this leaves little margin for error and that IT projects have the propensity to be delayed, such a short time frame poses a serious risk of compromising the quality of these systems in order to meet critical deadlines. In the case of iVote, the auditor noted that this resulted in "incomplete documentation, restricted test case formulation and compressed testing activities" [33].

Long term projects have also experienced the same problem. Many of the deficiencies with the AEC's systems during the 2010 Federal Election were aggravated because there was insufficient time scheduled to perform live testing. Furthermore the decision was made to launch some of these systems even after problems were identified.

Accurate risk assessments are vital for security. Risk profiles can change subtly and unexpectedly, yet at present the risks are not reassessed on an ongoing basis. This is especially problematic with function creep.

A recent case is the expansion of the NSWEC iVote system to include interstate and overseas voters. As a result almost 50 000 votes were cast over the Internet, which was ten times the number anticipated and predominantly comprised votes from interstate and overseas. This drastically changed the risk profile from a controlled small-scale trial, where problems would likely have a reasonably minor impact, to an uncontrolled large-scale event, where problems could have a major impact.

In the tightly contested seat of Balmain, the winning margin was around 100 votes. Over 900 votes for this seat were cast with iVote, and so relatively minor problems could have affected the outcome. In close elections similar scope changes could have implications for the integrity of the overall election result.

Standard security vulnerabilities are also frequently overlooked or underestimated. Many e-election systems have been developed without protection against even basic attacks. For instance the ACTEC's EVACS uses voting clients that send unencrypted votes to a ballot box server within the polling place via a local network [23]. Hence vote privacy and integrity could easily be compromised by even an unsophisticated attacker who gains access to the network. Also the voting clients do not store an independent audit trail of the votes cast, and so the ballot server presents a single point of failure against malicious attack or hardware failure.

In a similar way the use of highly insecure Bluetooth wireless technology in the ACTEC's iRoll backup system provides a vector for an attacker to gain unauthorised access to the PDAs containing the certified voter lists. An attacker could potentially violate the privacy and integrity of the certified lists, for instance to facilitate multiple voting by 'unmarking' voters from the certified lists. The nature of Bluetooth wireless communication means this attack could happen anonymously and at a distance. Again the attacker need not be particularly sophisticated or well resourced to carry out such a multiple voting attack.

The combined usage of multiple e-election systems has introduced new risks that have not been considered. For instance the simultaneous use of iRoll and EVACS by the ACTEC has created the potential for voter privacy to be violated through exploiting electronic metadata, in this case timestamps. The ACTEC's version of iRoll tracks voter flow in polling places by storing timestamps of when the voters were marked off the roll [4]. Also EVACS electronic vote records include timestamps of when the votes were cast. Cross-referencing iRoll timestamps with vote timestamps could then reveal potential matches between voters and votes. This technique would be effective when there are large gaps between timestamps, which will be the case during the three week pre-poll period and at quiet times on election day, particularly in smaller polling places. This vulnerability also highlights the subtle dangers of function creep, in this instance through minor feature enhancements.

The possible impact of individual e-election systems on overall election quality tends to be overlooked. Many systems are not even recognised as being failure critical. This is compounded by the ongoing trend to integrate all e-election systems. Systems deemed critical are placed at greater risk because an outside attacker could exploit a vulnerability in a 'non-critical' system to gain inside access. For example the AEC assumed its e-counting system was secure as the system was (in theory) only operated on a standalone machine isolated from the network, when in fact the system was designed with the capability to operate in a networked environment [5]. Such intrinsically insecure systems may be permanently exposed to higher risk because there may be limited scope to later harden them against attack.

There has also been a failure to consider the threats that e-election systems may pose outside elections. A prominent example is the privacy implications of e-election systems for the electoral roll such as the NSWEC's SmartRoll automatic enrolment system. These continue the expansion of function creep in electronic electoral roll systems, where a series of seemingly minor and insignificant changes has ended up having a large and unanticipated compound effect, not only on elections but also potentially on the everyday lives of voters.

The increasingly large volume and variety of data collected for the electoral roll has not only amplified the scale of the risks of violating the privacy of personal voter information, but has also changed the very nature of the risks. The secondary personal information now stored on voters is highly sensitive, and so leaking roll data can have extremely harmful consequences including identity fraud. Moreover the introduction of distributed systems such as iRoll and the growth in authorised third party access to the roll have increased the risk for roll data to be leaked through loss or theft.

4.2 Towards Best Practice

Risk assessments must be performed on all e-election systems, and these assessments must be comprehensive, ongoing and involve broad consultation. An overarching framework is necessary to set out the appropriate methodologies for conducting accurate risk assessments.

This framework should specify a systematic approach to identifying and gauging the full range and extent of the constantly evolving risks, especially in relation to low-probability, high-impact events. It needs to ensure broad consideration of the technologies, procedures and policies associated with e-election systems. Furthermore it must provide a holistic examination of the risks each system can pose to other systems and the entire election process, rather than dealing with the risks of each system in isolation.

5 A Culture of Audit

Rigorous independent audits are crucial for assuring the quality of e-election systems by critically reviewing all aspects of the systems. These audits cannot be a last-minute and secondary concern whose role is to tick the box or otherwise on an already delivered system. Instead a culture of audit needs to be adopted throughout the design, development, operation and post-mortem of e-election systems to develop high quality and an assurance of that high quality.

5.1 Current Problems

Audits in Australia are not conducted with sufficient time or expertise, and this has allowed problems with e-election systems and engineering practices to be overlooked. In many instances audits are not even performed. This was the case for all of the AEC's new systems and the NSWEC's e-counting system. Furthermore the Australian Auditor-General commented on the poor documentation of the AEC's systems and development processes [2], which would make it very difficult to perform audits if desired.

Even for the most critical systems, audits are often treated as an afterthought. In the case of the NSWEC iVote system, the feasibility study [30] originally scheduled less than eight days in total for conducting the audit and addressing the findings, with the voting period commencing just 10 days later! It would be unreasonable to expect that major flaws with such a complex system could be discovered and fixed in such a short time frame.

Note that voter registration for iVote was scheduled to open two weeks before the audit was due to be completed. Thus in the face of adverse findings, the NSWEC would have faced a very difficult decision between proceeding with using a vulnerable system in a failure-critical environment, or abandoning the system and potentially disfranchising 50 000 voters who planned to use iVote.

The iVote audit reports revealed that critical issues still remained one week prior to going live [34] and several vulnerabilities were not addressed in time [33]. There is no publicly available information on the nature or gravity of these vulnerabilities, but it appears that the final decision to launch iVote was made with knowledge that the system had significant security and quality shortcomings.

We observed that iVote was highly vulnerable to malicious hacking and to automated malware because there was no client-side encryption of the votes (aside from TLS/SSL encryption for HTTPS), and so voters' PCs sent, and

the NSWEC's voting servers received, the votes in plaintext form. This obvious security vulnerability was evident through our brief inspection of the live system.

The superficial nature of audits appears to be common. The ACTEC's EVACS counting module was certified by an independent auditor despite having serious defects that caused failures during the 2001 ACT Election [25]. Also the auditor failed to identify numerous other defects that could have caused incorrect election results and segmentation faults, and may have permitted penetration by malware. Many of these were obvious and elementary software defects that were later identified using standard testing methods and very simple test cases by the Australian National University review of EVACS [1].

Threats and vulnerabilities are consistently overlooked in security audits. For instance in examining the eLect source code for the AEC's remote e-voting trial system, the auditor only considered the possibility of malicious source code rather than inadvertent faults that could create security vulnerabilities [21]. This had longer term consequences extending beyond the AEC trial because the NSWEC iVote system was subsequently based on eLect.

Even when well-known security vulnerabilities are identified, their significance is not always properly understood by non-expert auditors. For example the e-voting system for the 2010 Victorian State Election used a weak, non-standard method for seeding pseudorandom number generators for some cryptographic keys [22]. The auditor (and, unsurprisingly, the vendor) dismissed this vulnerability as being negligible [18,36], in spite of the fact that it belongs to a well-known class of security vulnerabilities. Such weaknesses have been famously exploited in other systems, for instance the Netscape SSL attack [26].

5.2 Towards Best Practice

Comprehensive and continuous expert audits must be integrated into e-election systems practice, as they are for other failure-critical systems. Given the large number and variety of complex issues that all need to be examined, this approach to auditing is necessary to assure the high quality of e-election systems.

A culture of audit provides an essential layer of defence for directly identifying problems with the technology and operational procedures, as well as uncovering systematic weaknesses in the engineering and risk assessment practices that are likely to cause or overlook problems. It prevents failures and vulnerabilities by discovering and rectifying problems early on, rather than simply detecting them when it is too late.

6 Strong Transparency

Strong transparency is a fundamental feature of trustworthy elections. It promotes public understanding and involvement in the scrutiny process. By enabling such broad scrutiny of all aspects of elections, transparency also assures and enhances election integrity. This unique requirement for the highest level of transparency has even greater importance for e-election systems, which by nature are incredibly hard to understand and scrutinise.

6.1 Current Problems

So far the use of e-election systems in Australia has substantially eroded election transparency. The mere usage of these systems has managed to obscure many formerly manual election processes. There is minimal information on what e-elections systems are used by electoral commissions, how these systems operate and what failures occurred during elections.

For example most of the public details regarding problems with the AEC's e-election systems in the 2010 Federal Election only came to light through a parliamentary submission by the union that represents AEC staff [20]. It seems likely that many other problems were not reported at all.

Even for the most critical failures, few or no details are made public. This is particularly concerning in the case of the vote corruption in iVote, where the NSWEC determined some of the corrupted votes to be invalid, whilst also determining the intent of others [33]. The NSWEC has no intention to publish any of the documentation relating to the iVote incidents, why they occurred and how they were resolved.

In many instances the outsourcing of e-election systems has created barriers to transparency because of the intellectual property issues. Private vendors are reluctant to make source code or any other details of their systems publicly available. Even independent experts and auditors engaged in evaluating the security and reliability of an e-election system are usually forced to sign non-disclosure agreements with the vendor in order to gain access to source code. These agreements typically prohibit any comments from being made about the system without the vendor's prior approval, and naturally this can severely limit the public disclosure of adverse findings.

No technical documentation on any Australian e-election systems is publicly available. Audit reports and other high level reports have been published for the e-voting systems used in the 2007 Federal Election [7,9,6,8,16,17], the 2010 Victorian State Election [18,22,36] and the 2011 NSW State Election [33,34]. However most contain minimal technical detail and some refer to unpublished primary documents, including security and code reviews. In addition these reports were all released well after the elections took place (six months later for the Victorian reports).

The only publicly available source code is for the ACTEC's EVACS, but code for some parts of the system has not been disclosed. Other electoral commissions have repeatedly resisted calls to publish source code for their systems. For example a parliamentary inquiry recommended that the VEC should publish the source code for its e-counting system on its website and collect comments and bug reports from the public [35]. But this recommendation was disregarded. Instead the VEC has so far maintained that it is sufficient to have the system independently audited and then to provide electronic ballot data to scrutineers, who can calculate the election result and compare it to the published results [38]. Yet the e-counting system audit report was never published.

Furthermore giving the ballot data to scrutineers does not guarantee that the counting will be thoroughly scrutinised. Political parties may lack the expertise

and resources to develop complex STV software that counts the votes and generates the highly detailed data necessary to verify the official results data.

Moreover revealing ballot data in preferential electoral systems can expose voters to coercion through signature attacks [24], which are easy to carry out given the electronic ballot data. In an attempt to allow some verification of the count (though not of the ballot data), the AEC and ACTEC publish ballot data on their websites. It remains unclear how best to provide meaningful verification of electronic STV counting while mitigating the risk of large-scale voter coercion.

A lack of transparency has in certain instances created a great deal of voter confusion. This has been the case with automatic enrolment in NSW and Victoria. For example the NSWEC SmartRoll system notifies voters of automatically added enrolments and updated addresses. But few of these voters realise that this is only for the state roll and that they must still manually update their details for the federal roll [10]. Consequently the NSW state electoral roll has diverged substantially from the federal roll for NSW.

Non-transparency of e-election systems has also had an impact outside of elections. For example the use of highly sophisticated systems to collect vast volumes of voter data for the electoral roll has created a situation where the public has little idea of what types of personal information are gathered, which sources they come from, when the data is collected and to which third parties they are subsequently provided. Although individuals can inspect roll information that is available to the general public (primarily names and addresses), they do not have any means to verify or identify the secondary information collected and maintained on themselves. Concerns over privacy violations stemming from the lack of transparency over roll data have been raised on multiple occasions, for instance by the Australian Privacy Commissioner [12,13,14,15] and Australian Auditor-General [2], but the issues have yet to be properly addressed.

This privacy risk highlights the dilemma where on the one hand electoral commissions are under pressure to develop e-election systems to improve the democratic process; but on the other these systems may unexpectedly come into conflict with the public interest. The absence of transparency has hampered public debate over whether the risks and trade-offs are acceptable.

6.2 Towards Best Practice

E-election systems must be strongly transparent. The existing commitment and dedication to the transparency of manual election processes need to be applied to e-election systems as well. While the underlying principles of transparency remain the same, the challenge is that the complexity and capabilities of electronic systems make them inherently obfuscated compared to manual systems.

As a result concerted effort is necessary to make e-election systems transparent *by design*, so that there is openness as well as supporting material for this openness. The highest level of disclosure is needed to reveal the full details of the systems well in advance of an election. This includes source code and technical documentation, user and training manuals, and reports for the development processes, operational processes, risk assessments, reviews and audits. For this to be

possible the engineering, risk assessment and auditing processes must generate high quality documentation that is promptly released for public inspection.

Only through strong transparency can the public gain a clearer understanding of e-election systems and participate in the scrutiny process. This will then improve the quality and trustworthiness of e-election systems by allowing the benefits and problems with these systems to be accurately identified, and enabling well-informed public discussion about whether the right decisions are made in developing and using the systems.

7 Conclusion

In this paper we have set out four elements of best practice in the development, deployment and scrutiny of e-election systems. By encouraging the development and adherence to a process of best practice, our hope is to sustain the current high level of quality and public confidence in the conduct of Australian elections as they increasingly move away from manual systems over the coming decade.

So far Australia has embraced the benefits of e-election systems without sufficient consideration of how they fundamentally change the nature of elections and how to address these issues. The regularity and scale with which serious problems occur in e-election systems and their development is a clear and present danger to the security of Australian elections.

These problems demonstrate the need for cultural change to establish and adopt best practices that guarantee rigour in the engineering, risk assessment and auditing processes for e-election systems, and that provide strong transparency of these technologies and processes. This is becoming increasingly urgent as many systems are currently being rapidly (re)developed, in particular for e-voting.

Best practice is still essential when good cryptographic solutions are adopted. Most of Australia's e-election systems lie outside the scope of advanced cryptographic protocols, which are only for e-voting and e-counting. As a result the overall election process cannot be protected by cryptographic means alone. Even with strong cryptographic verifiability through protocols such as Helios, some vote corruption would still go unnoticed by many voters. Furthermore there is no satisfactory way to recover from catastrophic failures when (or if!) detected by diligent voters. In a sense cryptographic verifiability is a last line of defence to help *detect* failures and assure election integrity if that was indeed maintained. Additional layers of defence are equally important to help *prevent* failures.

Best practices for e-election systems do not need radical new or prohibitively expensive methods, but can be largely based on well-established best practices for IT, failure-critical systems and traditional paper-based elections. Common sense dictates that these very straightforward and proven practices should be applied to e-election systems. Yet they are not followed in Australia and it seems likely that the situation is similar elsewhere, considering the controversies over the general poor quality of e-voting systems worldwide. This motivates the broader need to establish guidelines that explicitly stipulate what constitutes best practice.

References

1. Abate, P., Dawson, J., Goré, R., Gray, M., Norrish, M., Slater, A.: Formal Methods Applied To Electronic Voting Systems. Tech. rep., College of Engineering and Computer Science, The Australian National University (2004)
2. Australian Auditor-General: The Australian Electoral Commission's Preparation for and Conduct of the 2007 Federal General Election. Audit Report No. 28 2009–2010, Australian National Audit Office (2010)
3. Australian Capital Territory Electoral Commission: The 2001 ACT Legislative Assembly Election: Electronic Voting and Counting System Review (2002)
4. Australian Capital Territory Electoral Commission: Report on the ACT Legislative Assembly Election 2008 (2009)
5. Australian Electoral Commission: Submission 181 (supplementary), Inquiry into the 2001 Federal Election. Joint Standing Committee on Electoral Matters, Parliament of Australia (2003)
6. Australian Electoral Commission: Final Evaluation Report: Evaluation of the Electronic Voting Trial for Blind and Sight Impaired Electors at the 2007 Federal Election (2008)
7. Australian Electoral Commission: Final Evaluation Report: Evaluation of the Remote Electronic Voting Trial for Overseas Based ADF Personnel Electors at the 2007 Federal Election (2008)
8. Australian Electoral Commission: Report into Electronically Assisted Voting at the 2007 Federal Election for Electors who are Blind or Have Low Vision (2008)
9. Australian Electoral Commission: Report into Remote Electronic Voting at the 2007 Federal Election for Overseas Australian Defence Force Personnel (2008)
10. Australian Electoral Commission: Submission 87, Inquiry into the 2010 Federal Election. Joint Standing Committee on Electoral Matters, Parliament of Australia (2011)
11. Australian Government: Strengthening Australia's Democracy. Electoral Reform Green Paper (2009)
12. Australian Privacy Commissioner: Submission 42, Inquiry into the Integrity of the Electoral Roll. Joint Standing Committee on Electoral Matters, Parliament of Australia (2000)
13. Australian Privacy Commissioner: Submission 154, Inquiry into the 2001 Federal Election. Joint Standing Committee on Electoral Matters, Parliament of Australia (2002)
14. Australian Privacy Commissioner: Submission 164 (supplementary), Inquiry into the 2001 Federal Election. Joint Standing Committee on Electoral Matters, Parliament of Australia (2002)
15. Australian Privacy Commissioner: Submission 172 (supplementary), Inquiry into the 2001 Federal Election. Joint Standing Committee on Electoral Matters, Parliament of Australia (2002)
16. BMM Australia: Audit and Certification of a Remote Electronic Voting System for Overseas Australian Defence Force Personnel. Australian Electoral Commission (2007)
17. BMM Australia: Audit of AEC's Electronic Voting Machine for Blind and Vision Impaired Voters. Australian Electoral Commission (2007)
18. BMM Australia: Electronically Assisted Voting Audit. Victorian Electoral Commission (2010)

19. Brooks Jr., F.P.: No Silver Bullet - Essence and Accidents of Software Engineering. IEEE Computer 20(4), 10–19 (1987)
20. Community and Public Sector Union: Submission 95, Inquiry into the 2010 Federal Election. Joint Standing Committee on Electoral Matters, Parliament of Australia (2011)
21. Computing Research and Education Association of Australasia: Submission 116.1 (supplementary), Inquiry into the 2007 Federal Election. Joint Standing Committee on Electoral Matters, Parliament of Australia (2008)
22. Computing Research and Education Association of Australasia: Report on the VEC-Scytl Electronic Voting System for the 2010 Victorian Election. Victorian Electoral Commission (2010)
23. Das, A., Niu, Y., Stegers, T.: Security Analysis of the eVACS Open-Source Voting System. Tech. rep., Department of Computer Science. University of California, Davis (2005)
24. Di Cosmo, R.: On Privacy and Anonymity in Electronic and Non Electronic Voting: the Ballot-As-Signature Attack. HAL Open Archive Document hal-00142440, version 2 (2007)
25. Downie, G.: Libs set to take third seat in Molonglo. The Canberra Times (October 2001)
26. Goldberg, I., Wagner, D.: Randomness and the Netscape Browser. Dr. Dobb's Journal (1996)
27. Joint Standing Committee on Electoral Matters, Parliament of Australia: The Conduct of Elections: New Boundaries for Cooperation (1992)
28. Macilwain, M.: History of the State Electoral Office, 1907-2007. South Australian Electoral Office (2007)
29. New South Wales Electoral Commission: Annual Report 2006-2007 (2007)
30. New South Wales Electoral Commission: Report on the Feasibility of Providing iVote Remote Electronic Voting System (2010)
31. New South Wales Electoral Office: Submission 10, Inquiry into the Administration of the 2003 NSW Election. Joint Standing Committee on Electoral Matters, Parliament of New South Wales (2005)
32. Oostveen, A.M.: Outsourcing Democracy: Losing Control of E-Voting in the Netherlands. Policy & Internet 2(4), 201–220 (2010)
33. PricewaterhouseCoopers: iVote Post Implementation Report. New South Wales Electoral Commission (2011)
34. PricewaterhouseCoopers: iVote Pre Implementation Report. New South Wales Electoral Commission (2011)
35. Scrutiny of Acts and Regulations Committee, Parliament of Victoria: Final Report on the Inquiry into Electronic Democracy (2005)
36. Scytl: Comments from Scytl on the CORE Report from the Electronic Voting Solution Used in 2010 Victorian Election. Victorian Electoral Commission (2011)
37. Tasmanian Electoral Commission: Annual Report 2006-2007 (2007)
38. Victorian Electoral Commission: Submission 27, Inquiry into Electronic Democracy. Scrutiny of Acts and Regulations Committee, Parliament of Victoria (2005)
39. Victorian Electoral Commission: Report to Parliament on the 2006 Victorian State Election — Submission 20, Inquiry into the 2006 Victorian State Election. Electoral Matters Committee, Parliament of Victoria (2007)
40. Wen, R.: Online Elections in Terra Australis. Ph.D. thesis, School of Computer Science and Engineering, The University of New South Wales (2010)