Mercury ISS- security analysis of iVote

Response to the call for submissions: Report on the iVote system

Written by:	Edward Farrell
Version:	v1.0
Date:	29/12/2017

www.mercuryiss.com.au

Table of Contents

Executive Summary

The NSW Electoral Commission is in the process of undertaking an inquiry concerning its iVote internet and telephone voting system. This follows the NSW Government's response to the NSW Parliament's Joint Standing Committee on Electoral Matters report on the 2015 State election.

In support of this activity, Mercury Information Security Services have compiled the following submission to detail an analysis of the current system with consideration to the terms of reference published in November 2017.

The submission below details concerns about the lack of transparency and other security shortfalls in 2015. We've provided a series of observations of events that have taken place that are relevant to the 2019 election. To conclude, a series of concerns on the transparency, security and auditing functions have been detailed, alongside improvements to future increments of the system.

Should the panel or the electoral commission have any questions on the report, do not hesitate to contact me.

Regards,

[redacted]

Edward Farrell
Director
Mercury Information Security Services
email: edward.farrell@mercuryiss.com.au

Submission

Introduction

The purpose of this submission is to detail security shortfalls and possible responses to the deficiencies in a digital election platform known as iVote. As an element of critical infrastructure and an enabler for democracy in New South Wales (NSW), the authors of this paper have divided the analysis into three areas:

- The conduct of previous audits
- Observations of the security landscape
- Considerations given the terms of reference

The approach has evaluated the evidence presented from a threat oriented standpoint with information that was publicly available. The analysis and considerations are detailed below.

Security audit & maintenance of the iVote system in 2015

An analysis of previous audits conducted by the NSW electoral commission indicates that they were not as effective as they could have been. Reporting from the 2015 security implementation statement lacked detail which was reflected in follow on activities by security researchers whom identified a significant issue during the election[1]. From the analysis, the following shortfalls were observed:

- The 2015 audit appears to have been compiled by Alastair James under the direction of Ian Brightwell, neither of whom came from a security background;
- No consideration towards malicious threat actors is detailed in section 9.4 of the implementation statement[2], and thus the threat modelling is insufficient;
- Information detailing the testing and evaluation regime, such as methodologies, personnel undertaking testing & details on findings are not forthcoming and cannot be deduced as transparent; and
- Information on the monitoring and audit function lack detail, and positive assurance as to the maintained security state of the system can be asserted.

To that end, the auditing process of 2015 was effective, which was evidenced by the discovery of a vulnerability by Alex Halderman and Vanessa Teague[3]. The vulnerability identified that a man in the middle attack could be exploited during the 2015 election, and that this risk was not remediated for 2 weeks following its publication. Furthermore, Vanessa Teagues talk at Ruxcon in 2015 had identified that in her experience the system had lacked

[1] https://www.elections.nsw.gov.au/__data/assets/pdf_file/0007/193219/iVote-Security_Implementation_Statement-Mar2015.pdf

[2] Section 9.4 https://www.elections.nsw.gov.au/__data/assets/pdf_file/0007/193219/iVote-Security_Implementation_Statement-Mar2015.pdf

[3] https://www.elections.nsw.gov.au/__data/assets/pdf_file/0019/205066/Security_Disclosure.pdf

transparency and responsiveness[4]. If two university researchers identified a significant risk with limited information and resources, it is likely that a more sophisticated threat actor could have exploited additional risks without the knowledge of the NSW electoral commission.

An exploration of the test system (available at https://bypractise.ivote.nsw.gov.au) had identified that the recommendation of the report does not appear to have been implemented against the test environment. The original risk, and proof of concept might still be exploitable however this was not tested during the conduct of research. Furthermore, the response is somewhat lacking; the response presented by the NSW electoral system appeared more concerned with participant feelings on security than detailed research presented by academics that demonstrated flaws in the system, and the response does not identify the expertise, qualification or reasoning of the independent auditors[5].

Observations of the security landscape

Lessons learnt from the Defcon 2017 voting village

Defcon is one of the world's largest hacker conventions. held annually in Las Vegas, Nevada, in 2017 the conference holds a number of smaller conferences with specific subject domains referred to as villages, one of which focused on U.S. Election Equipment, Databases, and Infrastructure. The voting village provided an opportunity to study the US election systems and infrastructure from an adversarial standpoint, stimulate discussion and provide an environment to learn and discover what the systems and processes for an election look like in the United States, an opportunity rarely afforded due to the sensitive nature of such systems.

The open scrutiny of the infrastructure, especially the hardware systems, identified that with limited time and resources these systems could be readily compromised. Additional concerns around the supply chain, the need for collaboration and policy/regulatory issues were also identified and discussed. Ultimately the open and public discourse that had taken place will ensure that ongoing activities will improve and enhance the security of voting systems within the United States.

A synopsis of the village and its findings can be found here: https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf

[4] https://2015.ruxcon.org.au/assets/2015/slides/iVote2015Ruxcon.ppt

[5] https://www.elections.nsw.gov.au/__data/assets/pdf_file/0011/205688/2015_NSWEC_Report_on_the_Conduct_of_the_2015_State_General_Election_AC.pdf p77,p80-81

Experiences with vulnerability research and discovery in Australia

Vulnerability research and discovery in Australia has been problematic when the discovery of security issues occurs. In 2016 the author of this paper was threatened with legal action after the discovery and proposed disclosure of a vulnerability that had affected a number of sensitive facilities in Canberra. The outcome of this event was that the issue is yet to be published and some 47% of facilities that were identified are still affected by the vulnerability. This was contrasted with the positive experience where the collaboration and publication of a security issue that impacted the Lucas Heights nuclear facility was quickly remediated with the involvement of all stakeholders[6]. A collaborative and inclusive approach to the identification and remediation of security issues within the Australian cybersecurity landscape will result in a better outcome for affected systems[7].

Efficacy of security governance for critical infrastructure

Security governance in critical infrastructure has been evolving in the aftermath of the September 11 attacks in 2001. In 2011 the National Research Council in the United States were commissioned to evaluate how risk is understood and managed in US Department of Energy facilities, especially given the unsustainable costs in what was a resourced constrained environment at the time and the effectiveness of that expenditure. The report had evaluated that the solution to balancing cost and security was *not to assess security risks more quantitatively or more precisely* but to take a *"total systems approach" to characterize the interactions and dependencies of security countermeasures at its facilities*[8] including the application of exercises, developing an understanding of the threats faced and a prioritisation of risks and vulnerabilities to mitigate. This approach may yield a more appropriate defensive posture than one dependent upon risk and implementation guides, the shortfalls for which are discussed elsewhere in this report.

[6] https://www.itnews.com.au/news/the-it-flaw-that-left-an-aussie-natsec-agency-base-open-to-attack-459743

[7] https://www.youtube.com/watch?v=ey2mZA4EQzg

[8] Understanding and Managing Risk in Security Systems for the DOE Nuclear Weapons Complex, available here: http://www.nap.edu/catalog.php?record_id=13108

Crowdsourced assurance activities

Crowdsourced assurance has been an evolving concept over the past five years. Companies such as Australian cybersecurity start up Bugcrowd have found that crowdsourced security programs outperform traditional methods, with a typical engagement by Bugcrowd identifying upwards of 70 vulnerabilities within the first two weeks[9]. The application of such a concept against critical infrastructure is nothing new, with a similar program against the Pentagon in the united states contributing to the US Department of Defence's overall security posture[10]. If such activities were to occur against the iVote system, issues such as the one discovered in 2015 (and others) would be discovered and remediated long before the election and would be in control of the NSW electoral commission.

US response- cyber protection teams

A noticeable shortfall in the audits of 2015 was the presence of a defensive team. Whilst the report discusses the application of a helpdesk team, a tier 1 security operations centre and a third-party auditor, these may not be entirely appropriate. Whilst such defensive practices are applicable for an information security activity or generic network, the nature of the electoral process should require a more in-depth approach given the anticipated threat actors. The United States have formed a response capability given this problem.

During the 2016 election the United States employed national guard (Army Reserve) cyber protection teams to evaluate and defend electoral systems[11]. These teams are often in a better state to provide internal defensive and detection measures & response actions, and are capable of providing threat specific responses. As a surge capability, such a team could be applied in the lead up to an election. Furthermore, as these teams are often intelligence driven instead of focused on generic network defence; as such they are often more capable than regular defenders in protecting critical infrastructure against specific threats. Whilst such teams are still in development in Australia[12], some consideration might be given to their use in the defence of the NSW electoral system under provisions for aid to civil authority.

[9] https://www.bugcrowd.com/resource/2017-state-of-bug-bounty/

[10] https://www.wired.com/story/hack-the-pentagon-bug-bounty-results/

[11] http://edition.cnn.com/2016/11/01/politics/election-hacking-cyberattack/index.html

[12] http://www.abc.net.au/news/2017-06-30/cyber-warfare-unit-to-be-launched-by-australian-defence-forces/8665230

Considerations of the terms of reference

Whether the security of the iVote system is appropriate and sufficient?

As illustrated in *Security audit & maintenance of the iVote system in 2015*, the audits are not appropriate or sufficient given the nature of the system. In addition to lacking any appreciation of malicious threats, the audits present does not go into specifics, provide subsequent references nor does it provide an in-depth analysis of threats and risks an electoral system is likely to encounter. The impact of this was the discovery of risks by two researchers and it is likely that additional threats and risks exist that have not been realised. Without more in depth & transparent audit activities, positive assurance cannot be asserted for the iVote system.

Whether the transparency and provisions for auditing the iVote system are appropriate.

As discussed in *Security audit & maintenance of the iVote system in 2015,* the obtuse nature of security reporting for the iVote system obscures the transparency of the iVote system. The provisions for auditing are focused on information technology governance that is wholly inappropriate for a voting system. If an opportunity to interact and collectively validate the security of the iVote system were available, the effects of this response would ensure a higher degree of transparency and assurance.

Whether adequate opportunity for scrutineering of the iVote system is provided to candidates and political parties?

Whilst the analysis did not consider the opportunities available to candidates and political parties, the discussions in the *Security audit & maintenance of the iVote system in 2015* part of the report highlight the lack of opportunity, to which the recommendations below would remediate this issue.

What improvements to the iVote system would be appropriate before its use at the 2019 State General Election?

Three improvements are suggested as part of this submission:

1. A more focused effort on understanding and responding to likely threats is required which, in turn, will reduce costs and enhance the security of the iVote system.
2. Consider the applicability of a crowdsourced model for evaluating for the iVote system that will facilitate a more transparent, effective scrutineering process and lead to a higher level of assurance.
3. Explore the opportunity of more sophisticated teams for defensive activities as a surge capability during the lead up to, and during the conduct of the election.

About the authors

Edward Farrell

Edward Farrell is a cybersecurity consultant and lecturer at the Australian Defence Force Academy with over 10 years' experience in technology and security. His expertise lies in threat emulation, wireless technologies and defensive practices in the face of sophisticated adversaries. In 2015 Edward Sought to go out on his own and create Mercury Information Security Services. Edwards new organisation seeks to provide a comprehensive range of customised information security services and advice that enables businesses to secure and protect all aspects of their organisation.

About Mercury

Mercury Information Security Services are a leading provider of information security services, advice and consulting in Australia.

Founded in 2015, Mercury seeks to provide sound and independent expertise across an array of technical security domains. It achieves this by synchronising and customising our services to meet our clients' business requirements and engaging with them as trusted advisors, providing constructive and pragmatic security advice.

For more information, visit their website or get in contact with them:

Website:	www.mercuryiss.com.au
Twitter:	twitter.com/mercuryiss
Email:	info@mercuryiss.com.au