SGE17 Sub 9
Rec'd 07/08/2017

Submission to the Parliament of Western Australia Inquiry into the Administration and Management of the 2017 State General Election

Dr Chris Culnane and Dr Vanessa Teague
School of Computing and Information Systems
University of Melbourne
{cculnane, vjteague}@unimelb.edu.au
+61 3 8344 1274

This submission was prepared in the authors' personal capacity.

Dr Chris Culnane has been a Research Fellow in verifiable voting since 2009, first at the University of Surrey and, since May 2016, at the University of Melbourne. From 2012-2015 he was also the Technical Lead for the University of Surrey on the vVote project run by the Victorian Electoral Commission (VEC) to develop an end-to-end Verifiable Election System. The system was deployed as the Electronically Assisted Voting solution for the 2014 State election. Culnane led the design and implementation of the back-end systems and protocols for the project and provided on-site support at the VEC in the run-up to, and throughout, the election period.

Dr Vanessa Teague is a cryptographer with an interest in cryptographic protocols that support a free and democratic society. She is on the advisory board of Verified Voting, a non-governmental US organization working toward accuracy, integrity and verifiability of elections.

This submission addresses the security of electronic ballots, particularly the privacy, verifiability and integrity of votes cast over the iVote system in the 2017 Western Australian state election.

We would be happy to discuss any of these issues with the committee.

Summary of recommendations

1. Internet voting should be discontinued. At worst, it should not be extended beyond its current very limited scope.
2. If iVote is continued, voters should be informed much more clearly that their votes are not private, cannot be truly verified, and may be subject to tampering.
3. If iVote is continued, its source code should be public, and its complete output votes, verification success and failure statistics, and number of deleted votes, should be published as soon as polls close.[1]
4. The earlier Western Australian *VoteAssist* solution offered genuine verifiability and reasonable privacy for disabled voters. That system, or some similar system with a voter-verifiable paper record, should be reinstated.
5. A system in which electronic blank ballots were sent to voters who printed and posted them back would be a much better tradeoff between access and electoral integrity for most remote voters.

[1] There may be some cases when the number of iVotes in some electorates is too small to allow publication without breaching privacy. In these cases, there is a conflict between protecting privacy and checking the output.

Transparency, scrutiny and verification

Internet voting is not only insecure, it is also unavailable to meaningful scrutiny. There is no way to verify that the votes produced by iVote accurately reflect the intentions of Western Australian voters.

Some electronic voting systems such as Helios[2] and Victoria's vVote system [2] provide voters and candidates with a meaningful opportunity to verify mathematical proofs of the accurate recording, transmission and tallying of the vote. vVote ran in polling places and used a preprinted paper ballot. However, there are significant obstacles to deploying genuinely end-to-end verifiable systems over the Internet for government elections. Verification can be subverted if voters do not understand how to do it, and even the best systems do not address coercion and vote buying.

iVote has no meaningful verification. The telephone-based vote checking system is described as a "verification" system but gives voters no evidence that their votes will be properly handled even if they have been queried. It was revealed more than a year after the New South Wales state election that 10% of verification attempts had failed to retrieve any vote—at the time the NSWEC announced that "Some 1.7% of electors who voted using iVote also used the verification service and none of them identified any anomalies with their vote."[3] Verification statistics for the 2017 Western Australian state election remain unavailable. A system in which a large verification failure rate can simply not be noticed or communicated is not a verifiable system.

Even if the verification statistics in Western Australia are comforting when they appear, there is no way for scrutineers to check that the votes that have been queried from the verification service match those entered in to the count. Instead of being available to scrutiny, this check relies on "auditing" by a number of third parties appointed by the electoral commission. This is a process audit, not an audit of paper evidence, which the iVote system does not produce. This is a substantial departure from Australia's tradition of candidate-appointed scrutineering. Why should all candidates trust the judgement of electoral commission appointees? Some errors or problems may not be evident at all, even to diligent and experienced examiners. In practice, the quality of these reports typically does not engender confidence—the auditor commissioned by the WAEC does not seem to have noticed a number of serious issues we later identified in the WA 2017 configuration of iVote. Indeed, the audit report indicates that in some cases he did not understand the issues even when he read our explanation.

Voting data

iVote's Legislative Council vote distribution in the NSW 2015 state election was noticeably different from the paper returns[4]. Although this was attributed to a "donkey vote," there is no firm evidence of the cause of the problem: it could have been user error, a user interface design problem, a software fault, or deliberate manipulation.

No iVote output votes from the Western Australian 2017 state election are yet available. This prevents scrutineers and the public from making the most basic assessment of whether iVote's outputs seem plausibly similar to the votes cast on paper.

Both the NSW and WA runs of iVote allowed voters to cancel their votes, re-register and vote again. Cancelled votes must be removed from the final tally, but there is no way for external parties to check that the correct votes have been removed. Neither the NSWEC nor WAEC have ever stated how many votes were deleted.

[2] https://heliosvoting.org/

[3] http://www.elections.nsw.gov.au/about_us/plans_and_reports/ivote_reports/response_from_the_nsw_electoral_commission_to_ivote_security_allegations

[4] http://blogs.abc.net.au/antonygreen/2015/04/does-electronic-voting-increase-the-donkey-vote.html

Source code

Although the code for encrypting and sending the vote is available to all voters (via their web browsers), no source code is available for the internal processing of iVote, including the verification service, the decryption, or the reconciliation of verified votes with those being entered into the count. This does nothing for security but makes external scrutiny prohibitively difficult. If there was a security problem or a software error in that part of the process, how would anyone be able to detect it?

Section 99I of Western Australia's *Electoral Act (1997)* states, " (2) A person must not disclose to any other person any source code or other computer software that relates to technology assisted voting ..." except under certain limited circumstances. Keeping the source code secret does nothing to protect security, but it does make it impossible for ordinary citizens to understand how the voting system works, or for someone who finds a problem to explain what it is. Suppose that someone found source code for iVote on a public website and discovered errors or security vulnerabilities in the code. (US Researchers found source code for Diebold electronic voting systems on a public FTP server [4]). It should not be illegal to examine the electoral process and identify a problem—it would be better if all the details, code and system documentation were available for open, independent analysis so that problems could be found and fixed.

We conducted a security analysis of the external parts of the iVote system used in WA. The most important risk was the introduction of a third party as a TLS proxy for all regsitration and voting sessions. The implications are detailed in our paper [1] and summarized here.

Impact of TLS Proxy on Trust

In a departure from the setup that was used in NSW in 2015, the WA variant of iVote was hosted through a TLS Proxy. A TLS Proxy acts as an intermediary in secure connections to provide additional networking services, primarily protection against Denial of Service attacks. In order to understand the impact that such a setup has on the trust and security of iVote, we must first provide some background as to what TLS is and what a TLS proxy does.

What is TLS?

TLS stands for Transport Layer Security. It provides encryption and authenticity of communication over an untrusted network, namely the Internet. TLS is at the heart of the modern internet, with e-commerce dependent on it to provide the necessary security and authentication to allow online transactions. TLS is intended as an end-to-end encryption technique, namely that the client connects to the server in a way that only the client and server can view the communication. Additionally, the client, and optionally the server, can authenticate that the other party they are talking to really is who they say they are. In this case, the client is the voter, who would normally expect a secure connection directly to the electoral commission. The iVote service looked like a direct, secure, connection to WAEC, but actually passed through an intermediary.

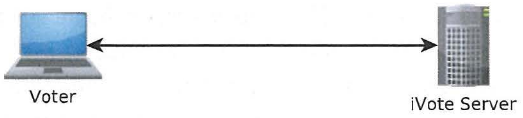

Figure 1: Example of direct TLS connection

What is a TLS Proxy?

A TLS Proxy is exactly what it sounds like, it is a proxy for TLS connections. TLS Proxies are used to protect against security threats and Denial of Service attacks. They operate by inspecting the incoming traffic and blocking malicious connections. The TLS Proxy is run on a high speed redundant network so that it can shield the end point from the onslaught of a distributed denial of service attack. Conceptually it is clearly a useful tool for protecting against such attacks, however, it comes with a significant trade-off, namely that the TLS Proxy becomes the end-point for the connecting user, and as such is able to view all communication between the user and the server. In the case of e-commerce this is a reasonable trade-off, because there is no presumption of secrecy for online shopping. However, in the context of voting this constitutes a significant departure from what would be expected. The voter must trust the TLS Proxy in addition to the Electoral Commission. Furthermore, due to the nature of the connection, the voter may not even be aware that their connection is being proxied through a third party entity. As we shall discuss in the next section, the TLS Proxy possesses a certificate that allows it to pretend to be the electoral commission.

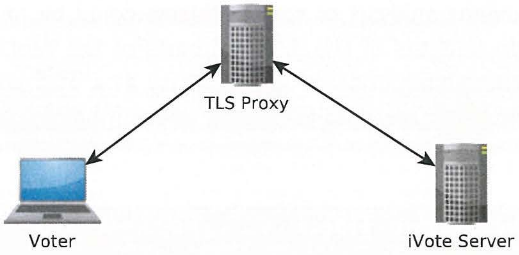

Figure 2: Example of TLS Proxy connection

iVote and TLS Proxies

WAEC deployed TLS Proxies across both the registration and voting portions of the iVote system. Part of the design of iVote is to separate the registration service from the voting service so that citizens can vote anonymously. That separation is removed when both connections are sent through the same TLS proxy service.

Importantly, the registration process involves the voter selecting and sending to the iVote server a 6 digit PIN. This PIN will be visible to the TLS Proxy during its transmission to the iVote Server. The 8 digit Voter ID is sent to the voter through a second channel, for example, by post or SMS.

The Voter ID and PIN are used to provide access to the iVote system, and to access the voting credentials. The design of the iVote voting portion of the system is such that Voter ID and PIN are never transmitted to the server - with all the necessary processing taking place in the voter's web browser. However, the deployment of the same TLS proxy service for both registration and voting nullifies this protection, since the TLS Proxy service has seen the PIN. Furthermore, due to the way in which the TLS Proxy service worked, in that it set a persistent cookie on the voters machine, it would have been possible to identify the same voter between registration and voting, if they used the same computer. As discussed in our paper, it would have been possible for a malicious TLS Proxy to recover a voter's Voter ID by performing an exhaustive search of all possible Voter IDs. Possession of both the Voter ID and PIN would have allowed a malicious entity to learn the Receipt Number then discover how a voter had voted by calling the verification service.

WAEC used Incapsula, a US based company, to provide TLS proxy services. Incapsula have a global network of servers to perform proxying and inspection of connections. It is this global network that provides resilience to attacks. Without getting into too many technical details, the way their network works is that any connection could go to almost any of their servers worldwide. This is a process known as Anycast, in which the optimal route is selected at the time of the connection. As such, if the connection to the Australian proxy becomes congested or unavailable the connection could be routed via a number of other global servers. This setup is evidenced by our analysis of TLS certificates that authenticate the WAEC domain. Such certificates allow the holder to act as the WAEC. We found them served from 153 IP addresses, consistent with Incapsula points of presence in Australia and also China, Poland, Spain and numerous other countries. Furthermore, the dynamic nature of the routing means that it is not possible to guarantee that the communications remained within Australia. They could have been routed via foreign nation states, who could impose data interception requirements on those connections.

Potential for attack

Even if the TLS Proxy had not been used across both registration and voting, and had just been deployed to protect the voting system, it would still present an unacceptable risk. The TLS Proxy occupies a privileged position in that it stands as a man-in-the-middle of the connection. It can see and modify both what is sent by the voter, and what is sent by the iVote system. As such, a malicious TLS Proxy could modify the iVote scripts and pages to inject vulnerabilities, or to leak voter data. A proof of concept of just such an attack was presented in [1].

The possibility of modifying the iVote web pages is not theoretical, it happens as part of the standard operation of Incapsula. The Incapsula TLS Proxy injects additional JavaScript that creates a profiling cookie, that records information like the operating system, browser, and available plugins. This cookie is short lived, and is destroyed shortly after the analytics information is sent to Incapsula. It is clearly not appropriate to have a third party altering the contents of the iVote pages in order to acquire analytics information, yet that is exactly what occurred.

Audit Report

With no opportunity for meaningful scrutineering, WAEC engaged an auditor to observe and comment on the electronic electoral process.[5] Both reports explicitly exclude cryptography and system architecture from the scope of the review. However, the long report makes a number of strong claims on both these topics.

1. The auditor claims that the iVote system is verifiable despite our explanation that it is not. A number of flaws in the verification process are clearly explained in Halderman and Teague [3]. The security vulnerability described in that paper has been corrected; the easily-evaded verification process has not been changed. Indeed, the fact that it is flawed is adequately demonstrated by the unnoticed high verification failure rate in NSW.

2. The auditor claims that the double layer of encryption prevents the TLS proxy from exposing or manipulating votes. This demonstrates a misunderstanding of the security mechanisms for serving javascript code. If the code for encrypting the vote is served from an untrustworthy source, then the vote may not be properly encrypted at all.

[5] The final report is at https://www.elections.wa.gov.au/sites/default/files/content/WAEC%20iVote%20Auditor%20Recommendations%202017.pdf

3. The auditor states that the likelihood of anyone compromising Incapsula's servers is small and that, if such a compromise happened, it would be too hard for an attacker to identify iVote data on the server. In fact Incapsula offers the helpful service of careful tracking of traffic to your particular site.[6]

The audit report also mentions a number of concerning occurrences during the voting period.

1. The system lockdown was raised on 24th February, *i.e.* after voting had started, to address an issue that is described only as a "race condition." This again mirrors a similar problem that occurred in the NSW state election, in which the vendor was allowed to make changes to the software after votes had begun to be collected. He insisted that his changes had not altered any votes, but there is no way for external parties to check. In the WA case, there is not even enough detail in the auditor's report describing what was changed.

2. An administrator login, which was thought to have been turned off, apparently persisted throughout the voting period. This illustrates the difficulty of truly observing what a computer is doing. Was it properly turned off in NSW 2015 or was it just that nobody noticed it was left on? The auditor does not say what privileges this account had.

3. Logging in the IVR system, *i.e.* the system that records telephone votes, seems to have been detailed enough to expose how the person voted. The suggestion that "The individual voter cannot be identified based on the log information," is hardly comforting if their log can be easily identified by some other method, such as caller ID or telecommunications metadata (which can be accessed by numerous agencies without a warrant).

The auditor refers to viewing the WA Legislative Council and Legislative Assembly iVote first-preference data but does not say whether they were broadly similar to the paper returns or not. These statistics should have been made available to scrutineers.

The audit report shows both the Core Voting System and the Verification service hosted by NSWEC. This fundamentally undermines what little protection the verification service might have offered. Even in the NSW state election, the verification service was hosted by a third party. To have both systems hosted by NSWEC risks one successful attack or corrupt insider being able to alter both lists of votes, rendering the decryption-reconciliation ceremony completely meaningless.

The auditor does not mention any audit of the paper printouts against the reconciled votes.

Legislation on criminalising false and misleading statements

Western Australian law now specifies: "A person must not make a statement (whether orally, in writing or by means of electronic communication) that the person knows to be false or misleading in a material particular for the purposes of or in connection with: a) Making an application for registration for technology assisted voting; or b) Casting a vote by means of technology assisted voting." The penalties are severe.

Unfortunately the WAEC's official FAQ website continues to state that the iVote system is "Extremely safe and secure." It assures voters that their vote, "cannot be tampered with or changed," and claims, "Your vote is completely secret." Since the WAEC, along with the Australia's other electoral commissions, has been repeatedly and clearly informed that these assurances are false, we recommend that either the law or the FAQ be speedily amended.

[6] https://www.incapsula.com/ddos-protection-services.html

References

[1] Chris Culnane et al. *Trust Implications of DDoS Protection in Online Elections*. https://arxiv.org/abs/1708.00991; to appear in E-Vote-ID 2017.

[2] Chris Culnane et al. "vVote: a verifiable voting system". In: *ACM Transactions on Information and System Security (TISSEC)* 18.1 (2015). https://arxiv.org/abs/1404.6822, p. 3.

[3] J Alex Halderman and Vanessa Teague. "The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election". In: *Proceedings of the 5th International Conference on E-Voting and Identity-Volume 9269*. https://arxiv.org/abs/1504.05646. Springer-Verlag New York, Inc. 2015, pp. 35–53.

[4] Tadayoshi Kohno et al. "Analysis of an electronic voting system". In: *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on*. IEEE. 2004, pp. 27–40.