Security Disclosure: New South Wales iVote System is Vulnerable to MiTM Vote Stealing Attacks

J. Alex Halderman
University of Michigan
jhalderm@eecs.umich.edu

Vanessa Teague
University of Melbourne
vjteague@unimelb.edu.au

March 19, 2015

Confidential report. Please do not distribute.

The iVote Internet voting system, currently in use for the 2015 State Election in New South Wales, is among the largest deployments of Internet voting anywhere in the world, with around 250,000 votes predicted to be cast online over 13 days. It is described to voters as private, secure and verifiable. With the election underway, we have completed a partial security analysis of the iVote system and uncovered a severe vulnerability that can be leveraged to manipulate votes and violate ballot privacy. This does not seem to have been detected by the authorities at the time of writing, despite a pre-election security review and despite the system having run in a live state election for five days.

1 Background on iVote

The iVote system allows voters to register and cast their votes using websites managed by the New South Wales Electoral Commission (NSWEC). The system was implemented by Scytl (a multinational electronic voting vendor) to NSWEC specifications using a combination of custom and off-the-shelf code.

Upon registration, voters are given an 8-digit iVote ID number and asked to choose a 6-digit PIN. Then they visit a website operated by NSWEC which serves an online voting application implemented with JavaScript and HTML. When they submit their vote, they receive a 12-digit “Receipt Number”. There is also a verification service which may be accessed only by telephone. Voters enter their iVote ID, PIN and Receipt Number on their touchtone keypad and hear an automated system read their vote

We performed a limited-scope security analysis of the iVote system based on publicly available documents and hands-on testing. We tested using a practise version of the system made available by NSWEC at https://practise.ivote.nsw.gov.au. The practise site allows members of the public to log in using published credentials and vote a mock ballot. The client-side code used in the live election is substantially the same as the code of the practise system and the vulnerabilities described below apply to the live election.

2 MiTM Vulnerability

The iVote voting website, cvs.ivote.nsw.gov.au, is served over HTTPS. While this server appears to use a safe TLS configuration, the website includes additional JavaScript from an external server, https://ivote.piwikpro.com/piwik.js. As can be seen using the SSLLabs SSL Server Test site, the ivote.piwikpro.com server is vulnerable to a range of TLS attacks, including the recently disclosed FREAK attack.

We have confirmed that if a voter uses the iVote system from a malicious network, a man-in-the-middle attacker can manipulate the data returned by piwikpro.com to inject malicious JavaScript code. This code can arbitrarily change the function of the iVote web application without triggering any browser security warnings.

FREAK affects major desktop and mobile browsers, including Internet Explorer, Chrome, and Safari. While these browsers have been patched over the last two weeks to fix the problem, many users have not yet updated. The authors are also aware of a similar, as yet unpatched, TLS vulnerability recently disclosed to browser vendors but not to the public. This additional vulnerability also impacts ivote.piwikpro.com and can be used to attack up-to-date versions of most browsers.

3 Proof of Concept

We have developed a proof-of-concept demonstration that illustrates how this vulnerability could be exploited to steal votes. Our proof-of-concept injects
JavaScript that hooks the iVote client-side code to subvert the voting session, expose the vote that voter intended to cast, and substitute a different vote. We tested our proof-of-concept against the practise election server at https://practise.ivote.nsw.gov.au and the attack succeeds as expected.

Although the iVote system provides a kind of verification mechanism, there are a number of ways that a network-based MiTM could attempt to subvert it. In addition, the security of the verification mechanism itself has not been well established, as it has had no public peer review, and only limited design specifications and no source code are available for inspection.

4 Recommendations

We recommend that NSWEC immediately modify the iVote system to remove the external dependency on ivote.piwikpro.com.

This incident highlights the challenges of conducting secure elections online, and it supports the view held by most security researchers worldwide that Internet voting cannot be adequately secured with current technology. If Internet voting must proceed, future versions should have a genuine peer-reviewed verification mechanism, publicly available source code and documentation, a firm eligibility restriction to voters unable to vote via a more secure channel, and a clear public statement of the risks.