EXTRAORDINARY MEETING

OF

WELLINGTON CITY COUNCIL

MINUTE ITEM ATTACHMENTS

Time: **9.15am**
Date: **Wednesday, 16 September 2015**
Venue: **Committee Room 1**
Ground Floor, Council Offices
101 Wakefield Street
Wellington

Business **Page No.**

Evidence to the Extraordinary Council meeting called to discuss the e-voting trial

Jan Rivers 0221261839, www.publicgood.org.nz

022 – 1261839 jrivers@paradise.net.nz

Summary: Second interim report into the 2013 federal election

Published Nov 2014

An assessment of electronic voting options

Joint standing committee on electoral matters (MPs and senators)

Chaired by Tony Smith MP

Report addressed e-voting bit.ly/catastrophictodemocracy

Concluded: Australia is not in a position to introduce any large-scale system of electronic voting in the near future without catastrophically compromising our electoral integrity.

Why is voting different.

"My answer to that is that voting once every three years to determine our democratic destiny is not an everyday transaction.

Not only do we have the right to a ballot; we have rightly enshrined within our system the right to a secret vote. Voting at a booth in a polling place guarantees this; voting over the internet threatens this."

Tony Smith Chair of the electoral review committee.

Separation of confidentiality aspect – login and vote are key and not well handled.

Estonia Remote internet voting 25% of pop since 2011 election

Highly tech literate but increasing criticism.

Vote data exposed to lapses allowing data manipulation, inadvertently released security and Pin no.

E-voting remains but an independent 2014 review identified serious security and data integrity flaws and recommended discontinuation of the system - security out of date and subject to cyber- attacks or hacking; system relies on voters computer and security;

Brazil: since 2000 OK initially and increasingly concerns about transparency and verifiability concerns of civil society. Isolated static devices ie go to a polling station.

Problems: Verifiability of source code, No democratic mandate – like NZ a technical committee.

Ireland – heavy investment from 1999 abandoned in May 2004 1 month before election –technicians showed vulnerabilities, increasing costs

The assurance of public confidence is of paramount importance.

Subsequent report - Ill conceived, poorly planned $50M 70K scrap

Subsequent legislation has banned electronic voting.

Netherlands - Early adopters since 1960s of electronic intervention

2006 99% councils were using, expats cd use popular but computer scientists demonstrated that machines could be hacked.

Dependant on third party actors. High costs of keeping up to date

Government had not (initially) reacted so signs that should have raised concern,

2008 Netherlands implemented legislation to ban future use of electronic voting

USA

Mixed experience, high spend on tech, failure between elections 25% malfunction

Rapid advance followed by needing to re-engineer a paper trail.

North Carolina and Maryland observed vote flipping D-R and vice versa

The move back to paper voting seen as a positive

UK level of security risk unacceptable, security and transparency issues

2007. UK trials have not continued but reasons are not documented

India hardwired, static systems but nonetheless attempts to hack

Item 1.5.2 Attachment B

Objectives

To change the outcome of a close election
To determine how given people voted
To see or change the vote of a specific voter

Strategies

Delay the vote to an advantageous time
Prevent or discourage critical voters from voting
Change a number of critical votes

Ways to achieve this

Target: Voter

Manipulation
Trick voter into compromising their computer or believing they've already voted - "Click this link to vote!"

Target: Personal or public computer

Keyboard sniffing
A device or software that records what keys have been pressed on a computer

Viruses, Trojans
Malicious software that can manipulate almost any aspect of the computer, presenting false information to the user, changing or recording information sent

Browser extensions/plugins
Additions like browser toolbars that can modify web pages displayed or change or record information sent

Browser bugs
Browsers contain security bugs that can be exploited to install viruses or trojans, or modify the way information is shown or sent in various ways.

Browser caching
Browsers store information about requests for performance reasons. Without care this information can reveal websites visited and sometimes actions taken.

Backups
Information on a computer which would normally be temporary or secure in the computer can be retrieved at later times and other locations from backups. Particularly relevant for cloud backups.

Operating system and application updates
Most operating systems and many applications automatically update. These updates could be used to deliver viruses or trojans. Many services do this - Microsoft, Apple, Adobe, Oracle (Java), Google/Mozilla, Spotify, Steam, all Anti-virus software

Target: Smart Phones

Viruses, Trojans
While less common than their computer counterparts, Smartphones can get viruses or be compromised by trojans. Unlike modern computers, many smartphones are not automatically updated to patch security holes.

Target: Home networks

Appliances
Many in-home smart devices now have some form of network connectivity. These devices are rarely updated and often easily compromised. They can then be used to sniff network traffic or attack computers or phones. Smart TVs, printers, even some refrigerators.

Wireless access point
Wireless access points can be compromised allowing the attacker to record or change any traffic on the network.

Modem/Router compromise
Broadband connections are often supplied with a modem or router which is subsequently ignored by the user. Rarely patched, these devices often have security bugs which can be exploited to manipulate or record traffic coming to or from the home or business.

Target: Public wireless

Wireless access points
The devices that provide public wireless can be compromised, allowing the attacker to record or change any traffic on the network.

Interception
Some public wireless services are not encrypted, exposing all traffic by users. Others only have very weak encryption.

Trojan APs
Attackers can set up access points with the same name as valid ones. They can then record or redirect traffic as they see fit.

Target: Corporate networks

Firewall/Proxy/Switch compromise
Corporate networks can have their border or network systems compromised, allowing interception, recording or manipulation of traffic on that network.

Deep packet inspection / HTTPS
Some corporate networks deliberately subvert encryption security in order to monitor the traffic, revealing private voter information to compromised hosts or IT staff.

Target: Cellphone towers and networks

Interception
Much like wireless, cellphone signals can be intercepted and decrypted. This is far harder but within reach of governments.

Trojan towers
Fake cellphone towers can be set up to provide unwitting phones with service that can then be recorded or manipulated.

Network infrastructure
Cellphone networks have standard network infrastructure which can be compromised to manipulate or record traffic.

Target: Major ISPs, Peering exchanges

Compromise of key equipment
Traffic from the voter to the voting system will pass through upwards of 10 different devices on the way. These devices, or the cabling between them, can be compromised or spliced to gain visibility of or manipulate traffic.

Routing manipulation
Internet providers often have multiple ways to get data from A to B, some of which go via other countries. Targeted attacks could result in voter traffic being sent via other countries, where compromised devices may wait.

Compromise of key equipment
Routers, switches, load balancers are all potential points of compromise allowing recording or manipulation of data.

Denial of service attacks
Service providers are vulnerable to attacks designed to clog up network connections or force equipment or software to fail, preventing voters from communicating with the voting service.

Target: Voting service data centres

Compromise of key equipment
Much like other networks, the data centres within which the voting servers are kept have routers, switches, load balancers and control systems which can be compromised to record or manipulate traffic.

Physical compromise of hardware
Physical security of the data centre can be compromised, or staff could be bought or coerced to install software or hardware on or in front of the voting servers. Backups could be stolen post-election to reconstruct voting data.

Target: Voting service systems

Compromise of key equipment
As with the data centre itself, the voting platform has its own equipment which can be compromised to record or manipulate traffic.

Platform or application compromise
Similar to the vulnerabilities of a personal computer, the voting platform could be compromised via security updates, installed software, security holes in the platform or underlying operating system, allowing traffic to be recorded, manipulated, or even votes to be changed

Denial of service
Targeted attacks on the voting software or platform could prevent specific demographics of voter from voting by overloading individual aspects or at specific times or locations.

Target: Voting service offices

Physical compromise of keys, software
Important passwords, security keys or software could be compromised by someone entering an office, or at a distance using something as simple as a telescope through a window to watch a staff member type.

Compromise of key equipment
The network, or staff devices themselves, could be compromised in much the same way as the voters own computer, allowing the attacker to act as the staff member or manipulate or steal information.

Interception or theft of backups, uncleaned devices
Lost devices or devices decommissioned without careful cleaning, or backups of current systems could be intercepted and analysed to obtain passwords, security keys or sensitive data.

Compromise of personal devices
Staff smartphones could be compromised to enabled video or audio recording to obtain security keys, passwords or other intelligence, or impersonate them to obtain other information via trusted networks.

Tabled Item C - Janita Stuart 16 September 2015

Good Morning. I am Janita Stuart.

I did thorough research on Internet Voting for Local Government at Masters degree level at Victoria University of Wellington.

I was sponsored by Local Government New Zealand. I interviewed a number of SOLGM Electoral Working Party members.

My research covered the aspects of social, technical, legal and financial. I looked at examples of other elections that used internet voting. I looked at all the objects people raise and proposed a way to address them.

As you all know, you can't learn how to have a successful election by trial and error. Elections must be done right the first time. Errors find their way to the front page of the DomPost.

This research is about having a successful election the first time.

To boil down my 300 pages of research into a sound bite:

- Internet voting can be done successfully
- However it won't be successful if you cut corners. If you feel you have to cut corners, then don't do internet elections.
- It is very expensive when you aren't cutting corners. The initial set up is extremely expensive, however the ongoing costs are much less.

I see you are using Electionz.com. My concern with them is they are too willing to cut corners. I'm not saying don't use them. I am saying to negotiate a very tight contract with them.

DIA were involved. I interviewed Gavin Beattie and send him a copy of the research.

In the first instance, seek a copy of my research from Local Government New Zealand. If that isn't successful, I am happy to accommodate. I can be reached at Janita@clear.net.nz