

Security considerations for remote internet voting

By Janita R. Stuart and Val Hooper

The 2004 Local Government elections didn't go smoothly for some electorates as computer complications created nightmares. The elections were a challenge for every territorial authority as they educated the public regarding new STV processes. In the near future we will be facing the challenge of Internet voting (I-voting) and hope to do so without the nightmares. Making the voting systems secure from the start will help keep the election process off the front page of the newspaper.

One of the main drivers for considering I-voting is government's policy of encouraging more of the services the government provides to be available via the Internet. Therefore both central and local government include the possibility of I-voting in their strategic e-government directions (New Zealand. Ministry of Justice. Chief Electoral Office, & Abbott McCaw Richter & Associates, 2003; E-Local Government Project Team, 2003).

A decision regarding I-voting cannot be taken lightly. Some Scandinavian countries have fully embraced I-voting and many people have experienced I-voting in private elections or polls, but it has received the thumbs-down for public elections in most countries. Officials in those countries believe the authentication complications and security vulnerabilities are impossible to overcome as they are fundamental to the architecture of the Internet (Yang and Sneiderman, 2004).

A participant in a Brookings Institute and Cisco Systems, Inc. symposium, expressed the inevitability in its implementation well by saying:

“About the Internet, whether we're going to adopt Internet voting, it seems clear to me that it's another Mount Everest, and we're going to climb it whether it's good for us or not, and because that's the way we people are. And I'm certain that there are people like me who want to be sure that the climbers have all the oxygen and all the clamp-ons and everything they need to get there and to come back safely. So the issues of integrity and security are certainly very important” (Armacost et al. 2000, p. 31).

Are the security vulnerabilities impossible to overcome? Can I-voting work and gain the public trust? It is not the purpose of this paper to compare the security of I-voting with the postal voting system. This study will only indicate the technological capabilities that can be implemented to make I-voting work successfully.

This article will explore the security vulnerabilities in three broad areas:

- Those associated with the client's personal computer,

- Those associated with the Internet lines of communication between the client and server computers, and
- Those associated with the server computers which store and count the votes.

Authentication is a very important aspect of security and is covered in another publication (Stuart, 2004).

As security is only as strong as its weakest link, this article will touch on as many security aspects as is currently known. To leave an area vulnerable to attack will cause the weak link to break, and the election event will be considered unsuccessful.

The client computer

In an effort to ensure that the voter's vote has not suffered from any interference (Barry et al., 2001, p. 13) the environment of the client computer from which votes will be cast is a major weak link in the security chain (California Internet Voting Taskforce, 2000B, p. 21, 22; Salkever, 2000) and one over which the Electoral Officer (EO) has no control (California Internet Voting Taskforce, 2000B, p. 15, 21; Internet Policy Institute, 2001, p. 20).

Without official control of the client voting platform, there are many possible ways for the voter's intent to be fraudulently altered before it arrives to the vote server to be counted which can affect the election results and seriously so in a close election. Technologies have yet to be developed to address these risks, however ways to mitigate against them will follow.

Malicious software

The sophistication and automation of malicious software is advancing significantly. Attacks are doing increasingly more damage, and are more successful at disguising themselves (Rubin, 2002, p. 40). The widespread damage done by the Love Bug illustrates this (Waskell, 2000, p. 2). Malicious software are programs developed by mischievous computer programmers that are capable of performing a wide range of functions on 'infected' computers, from the benign to the malign. They either hide the harmful action or perform it so quickly that it cannot be stopped. Viruses can be executable files (with a '.exe' filename extension) or files in other formats, such as word processing files containing macros. Running these executable files or opening files containing infected macros can cause a computer virus program to run (California Internet Voting Taskforce, 2000B, p. 12, 21).

This section focuses on the malicious software affecting the vote client.

Literally, hundreds of attack programs can be discussed. The Web sites of the security software vendors provide long lists of exploits affecting clients (Rubin,

2002, p. 40). Some of the software programs used by hackers/virus code writers, to create malicious actions are listed below. It is a shame that software which is generally developed for legitimate business purposes is used for malevolent purposes (Internet Policy Institute, 2001, p. 15).

Some of the software programs used by hackers/virus code writers, to create malicious actions are:

- ActiveX controls, JavaScript scripts, Java Applets, etc.
- “Back Orifice 2000 (BO2K) is software packaged and distributed as a legitimate network administration toolkit. It is very useful as a way to enhance security and is freely available, fully open source, extensible, and stealthy (see www.bo2k.de). Moreover, it contains a remote control server that, when installed on a machine, enables a remote administrator (or attacker) to view and control every aspect of that machine as though the person were sitting at the console. BO2K's open source nature means an attacker could modify the code and recompile such that the program evaded detection by security defense software (virus and intrusion detection software looking for known signatures of programs). There can be no expectation that average Internet users participating in online elections from home will have any hope of detecting BO2K on their computers. At the same time, the program enables an attacker to view every aspect of the voting procedure, intercept any action performed by the legitimate user with the potential of modifying it without the user's knowledge, and further install any other program of the attackers desire on the voter's machine” (California Internet Voting Taskforce, 2000B, p. 27; Rubin, 2002, p. 40-41; Internet Policy Institute, 2001, p. 15).
- A proprietary product called PCAnywhere has much the same functionality as BO2K (Alexander & Jefferson, 2000, p. 1; Internet Policy Institute, 2001, p. 15; Rubin, 2002, p. 40).
- LapLink (Alexander & Jefferson, 2000, p. 1; Internet Policy Institute, 2001, p. 15)
- Timbuktú (Alexander & Jefferson, 2000, p. 1; Internet Policy Institute, 2001, p. 15)
- Bubbleboy triggers as soon as an email message is previewed in Outlook (Rubin, 2002, p. 41)

Some of the capabilities of these programs are:

- Prevent access to the ballot website (California Internet Voting Taskforce, 2000A, p. 12; California Internet Voting Taskforce, 2000B, p. 21; Internet Policy Institute, 2001, p. 14)
- Prevent voting by causing the computer to crash (California Internet Voting Taskforce, 2000A, p. 1, 20; KPMG & Sussex Circle, 1998, p. 21)
- Take over or lock the keyboard and mouse (Carey, 2000; Rubin, 2002, p. 41)
- Render the personal computer (PC) unable to function (Carey, 2000; KPMG & Sussex Circle, 1998, p. 21)

- Prevent the voter from voting while the voter is left with the impression that s/he has voted (California Internet Voting Taskforce, 2000B, p. 21; Sullivan, 2000)
- Change the vote before it is encrypted (Alexander & Jefferson, 2000, p. 1; Barry et al., 2001, p. 9; Borenstein, 2000; California Internet Voting Taskforce, 2000A, p. 1, 20; California Internet Voting Taskforce, 2000B, p. 21, 22; Francisco, 2000; Gibson, 2001-2002, p. 570; Internet Policy Institute, 2001, p. 14, 15; KPMG & Sussex Circle, 1998, p. 20, 21; Rubin, 2002, p. 40, 42; Sullivan, 2000; Weinstein, 2000A, p. 1; Yang & Sneiderman, 2004). However, the hacker has to detect where it is stored which requires a very highly sophisticated, targeted attack. S/he has to change the input to an HTML form on the computer in real time at the time the voter is voting. The probability of this happening is extremely slim placing it in the acceptable risk bracket.
- Vote for electors who have not voted (Sullivan, 2000)
- Prevent the vote from being transported to the vote server (KPMG & Sussex Circle, 1998, p. 20)
- Modify the software base and behaviour of any other programme on the computer (California Internet Voting Taskforce, 2000B, p. 22)
- Download onto the client PC and complete its actions totally undetected even by expert systems administrators (California Internet Voting Taskforce, 2000A, p. 20; California Internet Voting Taskforce, 2000B, p. 21, 22; Gibson, 2001-2002, p. 570; Internet Policy Institute, 2001, p. 14; Rubin, 2002, p. 40, 42; Weinstein, 2000A, p. 1; Weinstein, 2000B; Yang & Sneiderman, 2004). There is no way anyone can guarantee that one of these programmes is not running.
- Erase themselves so no evidence is left behind (Rubin, 2002, p. 40; Yang & Sneiderman, 2004)
- Target systems below the level of abstraction at which those security protocols operate. Security mechanisms such as encryption and authentication (e.g., secure socket layer (SSL) and secure hypertext transport protocol (https)) are impotent against this kind of attack (Internet Policy Institute, 2001, p. 14).
- Originate from anywhere in the world, beyond the reach of N.Z. law enforcement (Internet Policy Institute, 2001)
- Be activated at any time, either by remote control, or by a timer mechanism, or through detecting certain events on the host (or a combination of all three) (California Internet Voting Taskforce, 2000B, p. 22; Internet Policy Institute, 2001, p. 14, 37; Rubin, 2002, p. 41)
- Target specific demographic groups. Attacks are not always random (Internet Policy Institute, 2001, p. 14-15).
- Disable virus protection software (Internet Policy Institute, 2001, p. 14).

Some of the ways client PCs get these malicious codes are:

- Directly loading them from diskette or CD-ROM (Internet Policy Institute, 2001, p. 14)

- Hiding in purchased proprietary software (Neumann et al., 2000, p. 2; Salkever, 2000). Possibly in AOL, Microsoft products, Adobe Acrobat, RealPlayer, WinZip, Solitaire, and lots more as well as any computer hardware such as Dell, Acer, or Toshiba (Rubin, 2002, p. 42) that includes minimal software.
- Receiving an email, viewing it in the preview screen, or opening it (Gibson, 2001-2002, p. 570; Internet Policy Institute, 2001, p. 14)
- Receiving an attachment in an email and opening it (Internet Policy Institute, 2001, p. 15; Rubin, 2002, p. 41; Weinstein, 2000A, p. 2; Weinstein, 2000B)
- Accessing files or downloading software from an Internet website (either purposefully downloading software such as device drivers, browser plug-ins, and applications or unknowingly downloading programs such as ActiveX controls just by visiting a web page) (California Internet Voting Taskforce, 2000B, p. 22; Gibson, 2001-2002, p. 570; Internet Policy Institute, 2001, p. 14, 15; Rubin, 2002, p. 42; Weinstein, 2000A, p. 2; Weinstein, 2000B)
- Accessing files or downloading software from another computer on the same network (California Internet Voting Taskforce, 2000B, p. 22)
- Accessing files or downloading software from another computer networked by cable modem connections in which the last link is a coaxial cable (California Internet Voting Taskforce, 2000B, p. 22)
- Exploiting existing bugs and security flaws in such programs as Internet browsers (Internet Policy Institute, 2001, p. 14).

Why home PC's are extremely vulnerable:

- Although anti-virus software is normally loaded on when the PC is purchased, the owner is often remiss in keeping it updated, even though there is no monetary costs in doing so
- Although firewalls for non-profit computer use are free, many home computer owners do not load them
- Home PCs typically have numerous operating systems and browser extensions from a wide variety of sources (California Internet Voting Taskforce, 2000B, p. 22)
- There is no test on extensions to ascertain whether they carried malicious code (California Internet Voting Taskforce, 2000B, p. 22)
- Home PCs are generally not professionally managed (California Internet Voting Taskforce, 2000B, p. 16)
- The home users are not aware of security hazards (Barry et al., 2001, p. 13; California Internet Voting Taskforce, 2000B, p. 16)
- The home users do not know how to use the security tools available (California Internet Voting Taskforce, 2000B, p. 16)
- It is very easy for a rogue programmer to write a malicious program in the form of an ActiveX control or plug-in or virus, then lure thousands of users to download that code (California Internet Voting Taskforce, 2000B, p. 22).

However, there are mitigating strategies to address all these vulnerabilities.

1. Some malicious software attaches itself to the PC's operation system and does its damage while there (California Internet Voting Taskforce, 2000a, p. 12). To help ensure voting integrity, a single-use clean operation system could be supplied (California Internet Voting Taskforce, 2000a, p. 3, 11, 20; KPMG & Sussex Circle, 1998, p. 21; Neumann et al., 2000, p. 2; NZ. Ministry of Justice, 2003, p. 36; Salkever, 2000; Weinstein, 2000b). Combined with sophisticated scans for an infected BIOS (or equivalent on other computers), this step could virtually eliminate the possibility of malicious software during voting (California Internet Voting Taskforce, 2000b, p. 23). This would need to be specially booted on voters' systems.
2. Using standard web browsers for I-voting also creates vulnerabilities (Weinstein, 2000b; California Internet Voting Taskforce, 2000b, p. 22). However, if the user has installed the software themselves, set the browser from day one to not allow the execution of code (or set the permissions very high), and made sure the machine is patched up to date at all times, there should be no concerns regarding the browser. For voters not meeting those conditions, a clean browser application program can be installed for the election event (California Internet Voting Taskforce, 2000a, p. 3, 11; California Internet Voting Taskforce, 2000b, p. 23).
3. Using updated anti-virus software. This can only detect and neutralise/prevent *known* viruses and other malicious programs that have already come to the attention of the security experts after the fact. They can do very little about unknown malicious programs, such as those that would have been quietly lying in wait for a specific event (e.g. voting) and then take invisible action (e.g. changing a vote) (California Internet Voting Taskforce, 2000b, p. 22).
4. Home computers can also have firewalls installed. A firewall is set to only allowing certain types of code through to the server, disallowing any other uses to be made (California Internet Voting Taskforce, 2000b, p. 29). However the firewall should not be so very tightly set as to disallow the voter from initiating the SSL session with the vote server that enables the encryption (California Internet Voting Taskforce, 2000a, p. 19, 20, 21; California Internet Voting Taskforce, 2000b, p. 16, 17).

To enable the home PC to be used for I-voting with integrity, the Electoral Officer (EO) could issue a diskette or CD-ROM or downloadable off the Internet, software which includes the following functionality:

- voting software that would make the computer immuned to malicious software attacks (California Internet Voting Taskforce, 2000a, p. 19)
- diagnostic checking of the hard drives for the presence of name brand anti-virus software and firewall software (one that looks for the code instead of software name)
- diagnostic checking if the computer is networked to any other computer capable of monitoring or remote controlling its actions
- download encryption software to enable the SSL session. This would include a unique symmetric public key.

- if the diskette, etc is personally handed to the voter, it can include the security codes such as PINs, passwords, and other shared secrets.

If the diagnosis results indicate an absence of security precautions, then the EO can either deny the voter the right to vote via the Internet using that PC or only permit it with the voter accepting all responsibility should their vote be attacked.

There are other options for addressing the vulnerabilities

- Special security PC hardware: A special, software-closed security device might be developed to be attached to the voter's computer, e.g. through a USB port. Its purpose would be to display the ballot to the user, accept the voter's choices as input, and perform the cryptographic operations. In effect the voting is done on the security device, and the PC it is attached to is used only as a conduit to the Internet. Since the device is software-closed, it is not subject to infection by malicious code (California Internet Voting Taskforce, 2000b, p. 23; Internet Policy Institute, 2001, p. 37).
- Closed, secure devices: It is possible that special, software-closed, Internet-capable devices may be developed for commerce and may be secure enough for voting as well (California Internet Voting Taskforce, 2000b, p. 23).
- Obscurity/complexity: While not sufficient for real security, this approach raises the cost to potential attackers. Digital ballot formats may be kept secret prior to the election and possibly randomly changed during the election, or made complex in other ways. In order to successfully carry out an attack and escape detection, malicious software code writers must have a great deal of information about the internal format of the ballot. If these details are not available in advance, and/or if that information is complex or frequently changed, the potential authors of attack software may not have enough time to develop and distribute it during the election window (California Internet Voting Taskforce, 2000b, p. 24).
- Individual checks: Set up a service wherein a computer technician visits the homes and offices to check the computers for vulnerabilities. The responsibility for the risk then is placed on the computer technician who may or may not be acting under the EO's delegation. It is possible that at the time of the personal visit, the technician can exchange the shared secrets and security codes.

Privacy

One of the principles of fair elections is that the elector is assured that no one knows how he or she has voted. Beyond the possibility of malicious software, the home or office PC may compromise the voter's right to privacy. There may be no visual barriers to prevent others from looking over the shoulder (California Internet Voting Taskforce, 2000a, p. 25) or employers may protect their investment by having security cameras around their staff (California Internet Voting Taskforce, 2000a, p. 25).

Privacy can also be violated when the voting software causes a record of the vote to be stored on the client's PC, leaving a footprint or when the next user of the PC can click on the "back" key and therefore see the previous voting screen.

Amongst the solutions to this problem are making the voting page "expire" with a few seconds and thereby preventing the voting screen from appearing when clicking on the "back" key. Also running diagnostic software mentioned above that can detect whether the client PC is networked. This can check for LAN, open PPP, SLIP connections, wireless connections, etc. It can then inform the voter with a warning not to use that PC if she or he is concerned about privacy (California Internet Voting Taskforce, 2000b, p. 27).

Social Engineering

One means by which votes are stolen is when the attacker contacts the voter (by a Java dialog box, email, or any other means) claiming to be an official representing the EO asking the voter for their password and other security codes so that the "technician" can fix a problem. Or to tell the voter that he or she has been disconnected and must re-enter his or her security codes to continue. When the voter trustingly follows the instructions, this information is sent to the attacker (Panko, n.d., p. 31). This type of attack is enabled by the recommendation in this study of making the voting web page time out after a few minutes and requiring the voter to re-enter the security code again to regain entrance. The difference is that upon re-entering the voting web page, the legitimate voter would get the message saying s/he had already voted with the message to contact the EO if s/he disagrees with that statement.

The remedy for this attack is to educate the voter that once the security codes are established/agreed, never to divulge them to anyone, not even the EO.

The internet communication lines

The focus will now turn to the vulnerabilities that may occur through the Internet Service Provider (ISP) and Domain Name Service providers for the journey from the client PC through the communication lines to the vote server (California Internet Voting Taskforce, 2000A, p. 11; California Internet Voting Taskforce, 2000B, p. 12, 21; Internet Policy Institute, 2001, p. 12, 15, 18, 37; KPMG & Sussex Circle, 1998, p. 45; Neumann et al., 2000, p. 2).

In the recent mass releases of credit-card numbers and other customer information, it was typically the security at the servers themselves at fault, not communications security (Weinstein, 2000A, p. 1; Weinstein, 2000B). In general, this is not a high risk area. Many of the vulnerabilities of voter privacy and vote changing are resolved with encryption as discussed below as anyone who looks into the packets sees unintelligible scramble and is unable to make any intelligent alterations to their content. It is also obvious at the vote server end if any

tampering has occurred (California Internet Voting Taskforce, 2000B, p. 21; NZ. Ministry of Justice, 2003, p. 32, 34, 36, 54).

Through the communication lines, there needs to be a guarantee that no ballot is either created or destroyed (lost) anywhere on this journey without detection (California Internet Voting Taskforce, 2000B, p. 21).

One main vulnerability is the fact that ISPs are private enterprises and may have no interest in election integrity (California Internet Voting Taskforce, 2000B, p. 21). Understandings need to be formed with multiple ISPs to set in place a plan for switching between them should an attack affect one of them (NZ. Ministry of Justice, 2003, p. 36).

A more serious attack involves targeting the Internet's Domain Name Service (DNS). The DNS is known to be vulnerable to such attacks as cache poisoning, which changes the information available to hosts about computers' IP addresses (Internet Policy Institute, 2001, p. 18; Rubin, 2002, p. 43).

Another problem is spoofing by diversion of Domain Name which is covered below.

As a part of the systems acceptance procedures, communications verification, testing and maintenance should be carried out. Communications should be tested both on its own and in conjunction with associated hardware and software. Communications verification tests (otherwise known as qualification tests) with the testing measures are listed in Appendix B.

Solutions

- Special contracts need to be formed with ISPs to ensure they remained up and running without overloading as outages are also not in their best interest. A broken fiber is more a problem than computer grunt and bandwidth which are not as much of a problem as they once were. This agreement should include the ability to divert the traffic off somewhere else should a broken fiber or a denial of service attack occur (Internet Policy Institute, 2001, p. 19).
- The IP number that connects the system to the Internet should be rotated frequently (Neumann et al., 2000, p. 2). This protects the system from flooding and makes hacking very difficult, if not impossible (Barry et al., 2001, p. 10).
- The system should be set up to force switch between ISPs. This will make hacking very difficult as the time window a hacker has to strive to break into the system will be significantly limited.
- The system should be engineered with redundant communication with smooth failover procedures so that if one resource goes down, the others remaining can automatically take up its slack with no loss of votes and minimal disruption. This should include redundant connections to the Internet through multiple ISP's (California Internet Voting Taskforce, 2000B, p. 29).

Encryption

One of the most effective, reputable and widely accepted methods of providing security and privacy for transporting transactions over the Internet is through the U.S. Department of Defense's encryption system (Armacost et al., 2000, p. 27; California Internet Voting Taskforce, 2000A, p. 4, 12, 13; California Internet Voting Taskforce, 2000B, p. 3, 21, 23, 27; Green, 2001b, p. 2; Green & Kunze-Hamel, 2001I, p. 4-5; Internet Policy Institute, 2001, p. 15-16; National Science Foundation. Office of Legislative and Public Affairs, 2001, p. 3; NZ. Ministry of Justice, 2003, p. 35; Panko, n.d.; Rubin, 2002, p. 42).

“Encryption involves encoding data that is being transmitted via a computer network or disk so that only the sender and the recipient can read the data. Any kind of computerised data can, in theory, be encrypted. Data are encrypted by the sender using a software program to ‘scramble’ or encipher data using a code ‘locking key.’ The recipient ‘unscrambles’ or deciphers the data by using the matching ‘unlocking key,’ which is unique to the recipient. Anyone who intercepts the message will simply see scrambled data that makes no sense without the necessary key” (Green & Kunze-Hamel, 2001D, p. 1).

When should encryption begin? Most authorities recommended that encryption begin just before the voter submits the completed ballot page. However, encryption when used as soon as the voter logs on to the ballot page, can be used to maintain the voter's privacy as hackers or systems administrators can only see online the encrypted scramble. Therefore following the pattern used by Internet banking transaction, it seems good to begin the SSL (secure sockets layer) session at the point when the voter logs on to the ballot page that will cause the public key to be downloaded on to the client's PC. The firewall on the client's PC needs to be set low enough to allow this download to occur. At the end of the voting, the system should cause the public key to be deleted from the client's PC.

As with any code, encryption can be broken given sufficient time and resources (Barry, et al., 2001, p. 13). The more sophisticated levels of encryption now available have made it very difficult to unscramble encrypted data. This is a continuously moving target however and as encryption technology and strength increases, so in general do the countermeasures. Given the voting process only takes approximately five minutes, if the highest level of encryption is applied (currently 268 bits), it would likely take longer to crack the code than the time the voting transaction takes. It is so difficult for the hacker to break the encryption, many do not bother because other portions of the election process provide greater vulnerabilities and are easier to hack.

New Zealand Internet security authorities such as Chris Budge of eCrime (NZ) Ltd and Tony Krzyzewski of Kaon Technologies Ltd believe PKI (Public Key

Infrastructure) encryption is mature enough to place confidence in whereas Barry et al. (2001, p. 13) does not.

A common form of encryption is the public key - private key system (Internet Policy Institute, 2001, p. 40; Perera et al., 2000). This asymmetric system uses two different keys to lock and unlock messages and files. The two keys are mathematically linked together. The EO distributes the public key to all potential I-voters who uses it to encrypt the completed ballot and send it to the EO. The EO keeps the private key secret and uses it to decrypt the ballot sent with the public key (Green & Kunze-Hamel, 2001D, p. 1). However there are alternatives around the symmetric and asymmetric systems that can be explored for greater processing efficiencies.

Ultimately this process of encryption prevents hackers from knowing how a voter voted or stealing the vote packet electronically as it indicates whether a vote has been tampered with, and provides an audit trail (Armacost et al., 2000, p. 25; California Internet Voting Taskforce, 2000A, p. 13; California Internet Voting Taskforce, 2000B, p. 34; Coughlin & Ward, 2000; Sullivan, 2000). Encryption does not stop a hacker getting in, but if it occurs, it is blatantly obvious (California Internet Voting Taskforce, 2000B, p. 21; NZ. Ministry of Justice, 2003, p. 32, 34, 36, 54).

The EO will need to upgrade the public key infrastructure before each election event (Internet Policy Institute, 2001, p. 40).

Alternative to encryption: Code sheets: As voters from many workplace computers can not download the data encipher software program through the employer's firewall and therefore can not encrypt their votes, voters can be mailed code sheets that map their vote choices to entry codes on their ballot. While voting, the voter uses the code sheet to know what to enter in order to vote for a particular candidate. In effect, the voter does the vote encryption, and since any malicious software on the PC would have no access to the code sheet, it would not be able to change a voter's intentions without invalidating the ballot (California Internet Voting Taskforce, 2000B, p. 23-24). As valid an option this may be, it is too complicated for some voters who find it difficult to follow the simplest of instructions. The instructions would have to be so clear that voter intent cannot be challenged in court.

Spoofing

One means by which votes are prevented or stolen is called "spoofing" or "site-jacking" (Internet Policy Institute, 2001, p. 17, 37; Rubin, 2002, p. 41) whereby a copy of the election site is created, and voters are directed to the imposter site by search engines or hyperlinks. As it appears to be the official site, the voter logs on with his/her PIN and personal details. S/he votes and leaves unaware that the site is a fake and that the votes will not count. The site owner then can do nothing having successfully prevented the voter from voting or can take the

authentication information collected from the fake site logs, log onto the real voting site, and use the voter's PIN and personal details to vote (Gibson, 2001-2002, p. 570; Internet Policy Institute, 2001, p. 17; Rubin, 2002, p. 43).

This can be prevented if the elector's PC has SSL and digital certificates as they are capable of distinguishing legitimate servers from malicious ones (Internet Policy Institute, 2001, p. 17). The likelihood of home PC's having digital certificates is slim (Rubin, 2002, p. 41, 43).

Another preventative measure is for the voter to have another shared secret with the EO. After the voter has authenticated him/herself and advanced to the voting page, a shared secret code can appear on the screen. The voter can be instructed not to vote unless that code from the EO appears on the page correctly. Its absence is a sign that the voter is not on the official voting website (NZ. Ministry of Justice, 2003, p. 35). This introduces a non-repudiation element to the voting process and complies with the e-government authentication principle of providing the assurance that the person is connected to the official government site (State Services Commission. E-Government Unit, 2003, p. 3).

Voters can be directed to the spoof site by being given the wrong URL address. A preventative measure is to forbid links to the ballot page being placed in emails, or any other website (Rubin, 2002, p. 43). This view is in opposition to the e-Government Unit's wishes to make voting available via the Government Online portal (NZ. Ministry of Justice, 2003, p. 18). However unless there is a way to ensure against spoofing, voters should be required to manually enter the URL. They would therefore be more likely to enter the URL provided on the documents posted out by the EO. The EO must not send the URL in an email to any elector.

Another means by which spoofing can occur is when the domain name service provider that is controlling the voting web site redirects the whole domain en masse to a different IP address (Rubin, 2002, p. 43). An administrator at the domain name provider can easily do this in 2 minutes and it is very tricky to detect. With the whole site redirected elsewhere, there will be no votes arriving to the vote server. The lack of votes arriving is a sign of this spoofing. The way to prevent this attack from occurring is to (1) have a management system running in the background that pings the voting address and also pings the IP address¹ and (2) employ people to continuously observe whether there is a couple of minutes of down-time while the WWW address disappears and the IP address changes. Both of these features should be implemented because it is unlikely the voting site will be continuously used especially in the middle of the night when having no activity is normal. It is reasonable for a mission-critical activity such as voting to have a continuous manager system in place.

1: Pinging the vote server and IP addresses can be actioned by setting up a macro that takes the security codes of an elector who has already voted and continually entering the voting address. The system will continually send back "already voted" messages.

Denial of Service Attack (DOS)

Some hackers do not aim to take control of the server or adulterate its data; they just aim to keep the server from getting its work done, thereby "denying service" to all users as if there was a massive system failure (California Internet Voting Taskforce, 2000B, p. 30). It is often very difficult to break into a server by password cracking. Therefore attackers use other means (Pando, n.d., p. 21). Denial of service attacks cause disenfranchisement and are relatively easy to do (Green, 2000, p. 3; Panko, n.d.; Rubin, 2002, p. 42), even at times done by children without a great deal of technical knowledge. Though not very sophisticated, these attacks foster inconvenience and anger and demonstrated power over the Internet as they prevent people from voting at the last minute (Panko, n.d.; Weinstein, 2000A, p. 2). A few high profile attacks are fresh in mind such as Yahoo, eBay, CNN and E*Trade (Alexander & Jefferson, 2000, p. 2; Internet Policy Institute, 2001).

In general, there are three categories of denial of service attacks for which defenses need to be designed (California Internet Voting Taskforce, 2000A, p. 12; Gibson, 2001-2002, p. 569; Green, 2000, p. 3; Internet Policy Institute, 2001, p. 37; Perera et al., 2000).

One denial of service attack occurs when the hacker sets up a "macro" that continually tries other people's authentication codes knowing they are not correct. As the system denies access after a specified number of mis-matched attempts, the hacker has successfully denied access to genuine voters who have not yet voted (KPMG & Sussex Circle, 1998, p. 46, 47, 53; NZ. Ministry of Justice, 2003, p. 34-35). Access to the system should be reinstated after a specified number of minutes (e.g. 30 minutes) and the voter (although frustrated) can make another attempt to gain access to the ballot page and cast his/her vote. However reinstatement should not occur within the last couple of hours of voting.

A second type of attack occurs on the ISP which interrupt the communication links (Internet Policy Institute, 2001, p. 15). These deliberate attacks are intended to control, crash, or overload the communication networks or routers the vote servers are attached to (California Internet Voting Taskforce, 2000B, p. 21; Rubin, 2002, p. 43).

A number of actions can be taken to prevent or minimise the harm done. They are:

- (1) The voting system can be set up with multiple redundant network pathways to the system with no single points of failure and sufficient performance capacity to cope with expected peak demands (NZ. Ministry of Justice, 2003, p. 36, 54).
- (2) Network concentration points on which an attack can be focused can be avoided (Neumann et al., 2000, p. 2).
- (3) Extra staff can be hired for the day.
- (4) Router software can be upgraded (Panko, n.d.).

The third category of denial of service attack occurs on the vote server. These delay or prevent a voter from voting by either clogging the communications channels leading to the server so that requests to it and responses from it cannot get through, or by crashing the server repeatedly so it gets no work done, or by overloading the server with fraudulent requests that force it to take all of its time checking and rejecting them instead of dealing with legitimate requests (Bowman, 2000; California Internet Voting Taskforce, 2000B, p. 12, 21, 30; Panko, n.d.).

One such attack is known as the single-message attack. Standards specify the structure of TCP, IP, PPP, and other types of messages that flowed over the network. In some cases, either because the standard is deficient or because it is implemented in a particular way, a single malformed message can bring down a server. When the server attempts to process the message, it crashes because it does not know what to do with the message (Panko, n.d., p. 21).

Another such attack is known as the message stream attack. Its strategy is to send the target host a stream of messages that overwhelms its processing power. For instance, when one host wishes to open a connection to another host, it sends a TCP "SYN" message. When the receiver gets the SYN message, it prepares to open the connection. It sets aside RAM and other system resources and does considerable amounts of processing to prepare for the connection. A long stream of SYN messages, called a SYN flood, overwhelms a server. The server slows down or even crashes if its system resources are exceeded in the attempt to open thousands of connections. Refusing further SYN messages keeps the system running, but also keeps legitimate users from using the system. SYN floods and many other message stream attacks are able to be remedied with patches (Panko, n.d., p. 21-22).

A single attacking computer may be limited in the amount of denial of service damage it can inflict. As it is at times possible to track the perpetrators of denial of service attacks, the attackers disguised themselves by distributing the attack by planting a "zombie" or "daemon" program in a number of programs by hacking into the computer or by tricking users into installing the zombie themselves. The latter is done by sending the user a Trojan horse program that masquerades as something else, such as a game, but that installs the zombie as well. Later, when it is time for an attack, the attacker sends each zombie program an instruction to attack a particular target host. All of the zombies then begin sending a stream of denial of service messages at the target host. They access the bandwidth of many computers that flood and overwhelm the intended target. The server cannot communicate until the attack stops (Internet Policy Institute, 2001, p. 16; Panko, n.d.). No matter how high the vote server processing specifications may be, if the whole world is trying to take it out, the attack can't be prevented (Internet Policy Institute, 2001, p. 16). Nor can an attack be stopped in progress without shutting down unrelated and legitimate communications - and even then it

takes several hours of diagnosis and network administration time (Internet Policy Institute, 2001, p. 16; Panko, n.d.).

A number of actions can be taken in the lead up to the election to protect the servers:

- (1) The broadest bandwidth possible can be provided (California Internet Voting Taskforce, 2000B, p. 30).
- (2) Systems staff can work 24/7 to vigilantly monitor the server(s) and networks and to be prepared to quickly cut communications with the network(s) from which the attack originated (although that would also cut off voters originating from that network) (California Internet Voting Taskforce, 2000B, p. 30).
- (3) There are software programmes such as NZ designed ESPHION to prevent such attacks.
- (4) Firewall software can be upgraded to prevent the opening (California Internet Voting Taskforce, 2000B, p. 29, 30; Panko, n.d.). The firewall can block all incoming packets on all ports except those involved in voting, and can be configured to filter malformed packets and any other suspicious traffic (California Internet Voting Taskforce, 2000B, p. 30).
- (5) Multiple, redundant systems can be used (California Internet Voting Taskforce, 2000B, p. 30; Neumann et al., 2000, p. 2) including renting another server for the duration of the election.
- (6) As with any risk assessment and management, implement a threat analysis plan, such as an appreciation process, being:
 - a. Be aware that it is a possibility, with “what if” scenarios
 - b. Complete a realistic threat assessment of all the different ways an attack could occur
 - c. Analyse how to defend the systems against all the possible attacks
 - d. Implement systems that appear to be the best defence
 - e. Install hardware and software that can take the worst case scenario
 - f. Have a back up system that can switch the data flow straight away to another machine. This re-route system would also be good in peak demand situations.

Implement all the second best defense systems as contingencies because they are possibilities.

The vote server

Security for the vote server has two main aspects: ensuring the technology is physically secure and ensuring data and software are secure (Green, 2001a, p. 1).

The security of the vote server is critical as any compromises will affect a large number of votes, such as a whole file. This is in contrast to tampering with the client PC wherein a hacker will have to expend a great deal of effort to significantly affect an election result.

Physical environment

The physical environment in which the ISP servers, the vote servers and the data storage equipment reside should be secure and protected against physical attack (California Internet Voting Taskforce, 2000A, p. 28; Green & Kunze-Hamel, 2001C, p. 1). As the law requires the paper voting documents to be securely contained, the equivalent should be true for the electronic ones.

Physical security measures can be divided into two broad categories: security against environmental factors, such as fire, moisture, flood, heat & cold and power failure; and security against human interference, either deliberate or accidental, from internal or external people (Green, 2001b, p. 1; Green & Kunze-Hamel, 2001J, p. 1).

The first consideration is the physical security against environmental factors.

Computerised electoral system require a continuous power supply. Backup power supplies should be an integral part of the technology system (Green & Kunze-Hamel, 2001J, p. 1-2; Green & Kunze-Hamel, 2001I, p. 1; Internet Policy Institute, 2001, p. 18). This will prevent loss of vote data or data corruption through power failure, by allowing a controlled close down of a system, rather than ensuring that work can proceed on backup power (Green & Kunze-Hamel, 2001J, p. 1-2; California Internet Voting Taskforce, 2000B, p. 29; Cranor, 1998, p. 3).

The other function of UPS systems is to smooth out surges in power supplies. Power surges can be dangerous to computer equipment and can cause fuses to blow or components to burn out. A UPS system will intercept a surge and prevent it from reaching sensitive equipment (Green & Kunze-Hamel, 2001J, p. 2).

“Another important aspect of physical security is ensuring that technology equipment, particularly computer equipment, is appropriately housed. Ideally, computer equipment should be stored in sealed buildings with climate control, so that temperature and humidity are kept at constant, optimal levels, and dirt, dust, smoke and other contaminants are excluded. In many cases normal building air conditioning systems that control cooling and heating are employed for this purpose” (Green & Kunze-Hamel, 2001J, p. 2).

“Another form of technology with special physical security needs is communication equipment. In particular, cables connecting computer networks need to be kept safe from harm. Cables are at risk of being gnawed by rodents and being tripped over by humans. Ways of safeguarding cables include shielding the cables inside ducts or strong sheaths, placing them inside walls, below floors and

above ceilings, building false floors to enable cables to travel underneath them, burying cables underground or mounting them on poles. Where cables are at risk, alternatives such as microwave links could be considered” (Green & Kunze-Hamel, 2001J, p. 3).

In New Zealand many of the buildings meet the standards required to withstand an earthquake which are the same as for fireproofing.

The second consideration is physical security against human factors.

Many of the measures taken to secure technology against environmental factors can also be used to prevent accidental or deliberate human intervention with technology. One way to steal votes is to physically steal the computer on which they are stored. While it may be too cumbersome, expensive or impractical to keep all computers under high security, it is usually highly desirable and more practical to do so with at least the servers (Green & Kunze-Hamel, 2001C, p. 3). Physical isolation, such as placing key items of technology like network servers, inside locked dedicated rooms, can help to reduce the chance of human intervention and insider fraud (Green & Kunze-Hamel, 2001J, p. 3).

Another means of security is to geographically distribute portions of the electoral process. With postal vote scanning and I-vote servers located in a number of places, a person desiring to commit a crime against the election’s integrity would have had to plan his/her crime for a number of locations simultaneously.

“Surveillance is another form of security. Security guards can be used to verify entry to a facility. Security cameras can be used by security guards to monitor a range of access areas” (Green & Kunze-Hamel, 2001J, p. 4; California Internet Voting Taskforce, 2000B, p. 28).

“If physical security to electoral technology is of high importance, it may be worth employing a security expert to conduct a security audit on the premises to ensure that all appropriate steps are taken” (Green & Kunze-Hamel, 2001J, p. 4).

“The final form of security against human intervention in technology is to make it difficult or impossible for an unauthorised user to access or change the data held in computer systems. This can be achieved by restricting access to data through use of passwords and encryption” (Green & Kunze-Hamel, 2001J, p. 4).

Testing

In order to build and maintain the public trust there should be extensive on-going tests. Some tests have been discussed above under communication and in Appendix B. There are a large number of tests required but the one the public most want to see are the Logic and Accuracy Tests (L&A) which verifies that 'what goes in' is 'what comes out' (Green, 2001B, p. 1; Green and Kunze-Hamel,

2001E, p. 1-2; Green and Kunze-Hamel, 2001G, p. 1; Green and Kunze-Hamel, 2001H, p. 2-3).

There are two categories of L&A tests. Firstly, before the voting period begins, test ballots can be transmitted from all types of vote clients (home, office, library PC, etc.). Secondly, during the I-voting window, test ballots are again transmitted from all types of vote clients. These ballots would be indistinguishable from real ballots for all purposes except that the vote is always informal or blank. If a hacker changed the vote, their motive would be to change it to a vote for a candidate. This fraud would be detected. These test ballots would also detect any lost ballots or extra ballots and enable appropriate corrective action to be taken. The locations of infected machines can be determined, the approximate time of the attack estimated, and the total number of votes affected bounded. Note that this technique does *not prevent* malicious code attacks; it only *detects* them after the fact. Hence it must be combined with other preventative techniques. Still, it is a very powerful technique because it provides a quantitative measure of the size of any problem it detects (California Internet Voting Taskforce, 2000b, p. 24, 28) and it can be performed with members of the public (such as scrutineers) watching to help gain public confidence in the entire end to end process.

In addition to the communication tests, the hardware and software should be tested for functionality, meeting standards and performance measures, being fit for purpose, consistency, and capacity loadings. In essence, the tests are to ensure that every component of a system is operating as it should, and that the system is performing exactly in accordance with the specific local requirements. The tests need to cover all the known vulnerabilities and result in identifying weaknesses that are to receive remedial attention (California Internet Voting Taskforce, 2000b, p. 26). Essential tests that should be performed by an independent authority are:

- a. default installation of web servers, implemented without removing default applications, files, folders, scripts, etc.
- b. the altered script applications in the web server to make sure they don't contain vulnerabilities
- c. the linkages between the front end web server and back end database so that the information can't be either injected into or extracted from the database
- d. cookies are correctly authenticated
- e. every single link is tested to make sure it is a valid link which does not allow the passing of false information

As software is constantly being changed to implement desirable functionality, fix faulty code, address new threats, support new platforms or devices, and respond to evolution in the security protocols and related technologies, it is important to continuously retest the systems (Internet Policy Institute, 2001, p. 19-20, 38).

Software audit measures can include:

- verifying that the code is logically correct
- ensuring the code is of modular design (that is, that the code is made up of discreet modules that can be separately tested and evaluated)
- verifying there is no 'hidden' code intended to perform unauthorised functions
- checking that the code is straightforward and relatively easy to understand
- ensuring the code is designed for easy testing - that is, that it includes features to allow testing of flow of data within and between modules
- verifying that the code is robust, so that it includes error trapping and error correction features that will allow immediate detection of errors and prevent loss of data through error
- ensuring the code incorporates security features that will prevent unauthorised access and/or detect and control any attempts at unauthorised access
- ensuring that the system is useable without the need for complex or obscure procedures
- ensuring that the software can be easily installed in the live environment
- verifying that the software can be easily maintained, and that errors or defects can be easily identified, corrected and validated after installation
- checking whether the software can be easily modified to add new features (Green and Kunze-Hamel, 2001H, p. 2).

Publishing the source code

As an aspect of providing transparency to gain public acceptance, the merits of whether the source code should be published or not is debated. For the most part, the public is disinterested as they have interests that do not include getting behind the user interface and poking about in the workings of computer systems (Russell & Cunningham, 2000, p. 3). EOs are interested to the degree in which they are satisfied that the systems are fit for purpose and they can defend themselves when challenged in court (Green & Kunze-Hamel, 2001A, p. 1; Green & Kunze-Hamel, 2001K, p. 2).

Publishing source code for most computerised functions is not routinely done, and is normally only contemplated where a system being used is particularly sensitive, such as an electronic voting or counting program (Green & Kunze-Hamel, 2001K, p. 2). Some software vendors published their code.

Looking at the debate whether to publish or not, whether to use open source code or proprietary code, the table below outlines the advantages and disadvantages of choosing the transparent option.

Pros	Cons
<ul style="list-style-type: none">• Public confidence is increased by the level of transparency provided	<ul style="list-style-type: none">• Software developers may not be motivated to be innovative and develop enhancements if their work is published

<p>(Internet Policy Institute, 2001, p. 3, 21, 38; Sommer, 2003).</p> <ul style="list-style-type: none"> • Proprietary software can (and sometimes will) include code that permits stealth observation. This is unacceptable for elections wherein privacy is legislated. • The bugs and problems in software can be found and fixed quickly (Green & Kunze-Hamel, 2001A, p. 1; Weinstein, 2000A, p. 1). • Source code is made more secure the more it is scrutinized by others (Internet Policy Institute, 2001, p. 21). • Accountability and independent analysis are able to occur as required of all other aspects of a public election (Green, 2001b, p. 1; Internet Policy Institute, 2001, p. 21). 	<p>(Internet Policy Institute, 2001, p. 3, 38).</p> <ul style="list-style-type: none"> • Vendors argue that they need to maintain their technology secrets in order to maintain competitiveness, profitability and protect their investment (Internet Policy Institute, 2001, p. 3, 21). • Vendors claim that secrecy is a necessary requirement to keep their systems secure (Kohno et al., 2003, p. 1). When code is published, its public availability expose weaknesses that can be exploited by anyone able to gain access to the code used in a "live" system (Green & Kunze-Hamel, 2001K, p. 2; Internet Policy Institute, 2001, p. 21). • While the intended goal of encouraging experts to evaluate the code is sound, such a process can result in many false or erroneous reports of software error, needlessly undermining confidence in the electoral process and diverting the attention of EOs (Internet Policy Institute, 2001, p. 21-22). • Publishing the code does not guarantee that its serious faults will be found (Internet Policy Institute, 2001, p. 22).
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

In general, "what can go wrong will go wrong, security by obscurity doesn't work" (Russell & Cunningham, 2000, p. 2). People have a right to know, in as much detail as they are capable of understanding, exactly how their elections are conducted (Internet Policy Institute, 2001, p. 21). Elections by nature are required to withstand a great level of scrutiny and analysis.

Secrecy does not, in any event, prevent copying the technology. Foreign governments and other interested parties can acquire access to the source code for these systems - either through direct purchase of the source code (and foreign governments are unlikely to purchase election systems without access to source code since *their* national security is at stake) or through reverse engineering. Vendors' intellectual property can be protected with copyrights and patents (Internet Policy Institute, 2001, p. 21). On balance, the advantages of making source code available for public review significantly outweighed the disadvantages (Internet Policy Institute, 2001, p. 22).

The only acceptable exceptions to publishing the source code are:
(1) Do not publish the security code.

- (2) Consideration can be made to exempt the source code of universally-verifiable, protocol-based applications from public disclosure if such certification is available (Internet Policy Institute, 2001, p. 22).

An alternative to publishing the source code would be for independent professional experts and trusted members of the public selected for their expertise to perform rigorous evaluation and scrutinise the code. They should provide certification of the software around two important aspects of voting systems: (1) the system is performing the intended functions and (2) the system has no security vulnerabilities (Green & Kunze-Hamel, 2001A, p. 1; Internet Policy Institute, 2001, p. 22; Neumann et al., 2000, p. 2; Weinstein, 2000B).

Repudiation

At some point after the vote is cast (maybe next day), the voter should receive an email that verifies that the vote has been received. It can be automatically generated but should use an external email system that validates the transaction for both parties.

Vote server/Election results

When security weaknesses in the vote server are discovered, vendors usually are fairly prompt about creating patches to fix them. Whenever server administrators neglect to download and install the patches, the resultant vulnerability raises the risk level significantly (Panko, n.d.).

Anti-Virus and firewalls

The vote server is equally vulnerable to virus attacks as the home PC, therefore everything covered under malicious software above applies to the vote server (California Internet Voting Taskforce, 2000A, p. 12; Green, 2001b, p. 1; Internet Policy Institute, 2001, p. 18; NZ. Ministry of Justice, 2003, p. 32, 54). The vote server's anti-virus software should also be regularly upgraded. If the preventative measures are not put in place, security experts would surely criticize publicly any election system having such vulnerabilities, and that could influence the public to have no confidence in the system (California Internet Voting Taskforce, 2000B, p. 22). Many viruses infecting systems are not found even though millions of dollars are spent finding, removing, and developing patches to negate them.

Also, as with home PCs discussed above, firewalls are required to control access to the vote servers and should be updated periodically (Green & Kunze-Hamel, 2001C, p. 4; KPMG & Sussex Circle, 1998, p. 53; NZ. Ministry of Justice, 2003, p. 32, 36, 54). The firewall is programmed to only allow certain types of code through to the server, disallowing any other uses to be made of the web site. For the vote server, it should be programmed to only receive HTML (or XML or EML) code which would sufficiently protect the site. If the vote server is a separate computer from the count server as shown in Figure 2 below, there should be a

firewall place between them, and communication lines between them should not go out through the Internet exposing the data to those vulnerabilities again (California Internet Voting Taskforce, 2000B, p. 21). Both the web server and database should each have a very high level certified firewall which currently is either an EAL4 or EAL4+ firewall. This is a Commonwealth government security standard and is used by all the Defense systems.

Fraudulent or accidental change of votes, creation or loss

Altering the intent of the voter's vote by accidental or intentional fraud by changing, forging, creating or losing votes needs to be prevented with adequate defenses (California Internet Voting Taskforce, 2000A, p. 11, 28; California Internet Voting Taskforce, 2000B, p. 2, 21; Gibson, 2001-2002, p. 570; Green & Kunze-Hamel, 2001A, p. 1; Green & Kunze-Hamel, 2001C, p. 1; Green & Kunze-Hamel, 2001I, p. 5; Internet Policy Institute, 2001, p. 3, 12; Salkever, 2000).

Some vulnerabilities are:

- Tampering by election personnel who the EO has delegated responsibilities to (California Internet Voting Taskforce, 2000B, p. 12, 21; Internet Policy Institute, 2001, p. 37)
- Computer memory failure (Internet Policy Institute, 2001, p. 18)
- System crashes (Bowman, 2000).
- Server attacks (California Internet Voting Taskforce, 2000A, p. 12)
- System overload (Barry et al., 2001, p. 6)
- Server manager mistakes (Internet Policy Institute, 2001, p. 18).

System maintenance

Maintenance regimes need to be seen to be operational (Green, 2001B, p. 1) beginning with the schedules and programmes recommended by the manufacturer or supplier. Systems should be maintained to ensure that they continued to perform to the level demonstrated during the testing stage (Green and Kunze-Hamel, 2001E, p. 2-3).

Redundancies and duplication of systems

It is wise to have alternative equipment available on stand-by that can be brought on-line at short notice as a part of the contingency against risks (Internet Policy Institute, 2001, p. 3). Contingency systems are most effective if they are not implemented as an afterthought, but included in the overall technology strategy from the beginning. The level of resources committed to contingency systems will depend on the level of risk involved which is also dependent on the election's time-critical nature. It is hoped that they will not be needed, but their expense is preferred over the public embarrassment of a failed election (Green and Kunze-Hamel, 2001F, p. 1-2; Internet Policy Institute, 2001, p. 18).

Therefore multiple redundant back-up servers are required (California Internet Voting Taskforce, 2000b, p. 29; Internet Policy Institute, 2001, p. 19; NZ. Ministry of Justice, 2003, p. 32) to manage the following risks:

- to provide a back up in case of malfunction or failure (California Internet Voting Taskforce, 2000a, p. 12; Internet Policy Institute, 2001, p. 19).
- to assist with meeting excess demand and maintain acceptable response times (Internet Policy Institute, 2001, p. 18, 19; NZ. Ministry of Justice, 2003, p. 32, 54). As stated under DOS attacks above, this server duplication can kick in under moments of excess demand. If voters leave voting to the last minute, a deluge may occur (Green, 1999, p.105; Green, 2000, p. 6).
- to provide a means of detecting and isolating fraudulent vote changes. When running a dual channel system the votes duplicate themselves and go off to two vote servers for storage. This is not a backup after the fact. If the main system goes down, every record is mirrored at the other location. If a hacker has successfully penetrated the system and changed the software code or vote data, s/he would have penetrated only one of the channels. Each day of the voting period, the EO will cause the 'escrowed' copy of the software to be compared with the two 'live' copies to detect whether any changes have been made. If a change is detected, the escrow copy will be copied back to the vote server and the voting carry on. An analysis of the effect of the corrupted data or software will also occur to ascertain which and how votes were affected by the corruption. The votes recorded via the un-corrupted channel will be the record that proceeds to the counting program (Green and Kunze-Hamel, 2001a, p. 1; Green and Kunze-Hamel, 2001G, p. 2; Internet Policy Institute, 2001, p. 38; Weinstein, 2000a, p. 1).

Data Storage

Another way to help keep data secure from unauthorised access is to limit the places in which data are stored. In networked computer systems, it is good practice to keep all data, particularly all sensitive data, on centralised servers rather than on local personal computers' hard drives. These centralised servers should also be another step away from the Internet world with a firewall in between. This practice means that any unauthorised intruder trying to access data has to pass two levels of security to reach them - both the local computer's and the network server's. It is generally more difficult to gain unauthorised access to data on a server than it is on a personal computer. Another advantage of keeping sensitive data on centralised servers is that it limits the number of computers that need a very high level of security (Green & Kunze-Hamel, 2001C, p. 3).

Vote counting process and integrity

During the voting period, I-votes are arriving electronically from all over the world (Green, 1999, p.105) and stored in the database, and postal and special votes are being scanned into a database with the progressive processing procedures. The EO is frequently checking that the electronic votes have not been tampered

with (as described above) but by law no calculating is attempted until mid-day polling day when no more voting documents (paper or electronic) are received (California Internet Voting Taskforce, 2000A, p. 12; California Internet Voting Taskforce, 2000B, p. 37; NZ. Ministry of Justice, 2003, p. 35).

Only with the command enabled by the EO's official password (Internet Policy Institute, 2001, p. 28; Salkever, 2000) can the functions of the database holding the I-votes applying the decryption code, combine these votes with the database holding the scanned paper votes, and the system electronically calculating the results (Barry et al., 2001, p. 13; California Internet Voting Taskforce, 2000A, p. 13; California Internet Voting Taskforce, 2000B, p. 37). It certainly adds to the security for the decryption not to occur before end of polling and the Internet connection disabled.

Occasions have occurred when the accuracy of the vote count was questionable, such as in Florida in the 2000 Presidential election (Internet Policy Institute, 2001, p. 27; KPMG & Sussex Circle, 1998, p. 17). It is important that votes are accurately recorded and counted (Internet Policy Institute, 2001, p. 12) and that the public has confidence in the accuracy of the system (Internet Policy Institute, 2001, p. 27) as it determines the winners of elections (Internet Policy Institute, 2001, p. 28). Accuracy depends upon a variety of factors, such as the integrity of the system, the vulnerability of the hardware, software, and networking medium, and skilled personnel to operate and troubleshoot the system, none of which is transparent to monitoring officials (Internet Policy Institute, 2001, p. 28).

Certainty of a reliable, indisputable, verifiable outcome is extremely important (California Internet Voting Taskforce, 2000A, p. 29; California Internet Voting Taskforce, 2000B, p. 11; Perera et al., 2000; Weinstein, 2000A, p. 1). The risks with I-voting are:

- outsider tampering (Green & Kunze-Hamel, 2001, p. 5; Weinstein, 2000B) and
- software miscalculations (Gibson, 2001-2002, p. 573).

The risks with counting paper ballots manually is that they are handled by humans and that alone could change the count (Barry et al., 2001, p. 11, 14; Green, 2001a). Many authorities feel that computerising the election process and removing the human touch increased the certainty of outcome (California Internet Voting Taskforce, 2000B, p. 11; Gibson, 2001-2002, p. 573).

Auditability, Recounts, Transparency

At the end of an election, there are times when the validity of the results are in doubt (California Internet Voting Taskforce, 2000B, p. 12, 18; NZ. Ministry of Justice, 2003, p. 35), especially when the election is close (Borenstein, 2000; Carey, 2000).

Therefore there has to be a means of providing transparency of the systems. Not only do all voters have a right to possess a general knowledge and

understanding of the voting process (Internet Policy Institute, 2001, p 12; KPMG & Sussex Circle, 1998, p. 20; Sullivan, 2000) but there should be enough transparency so that the non-computer-geek court judges can make a good decision on the case set before him or her (Armacost et al., 2000, p. 23; Internet Policy Institute, 2001, p 12). Transparency with electronic systems are different from transparency with paper-based systems as paper ballots can be touched, handled, checked and rechecked (Green, 2000, p. 2). Some authorities seem to believe there is no transparency with electronic systems (Ananthaswamy, 2004, p. 7; Barry et al., 2001, p. 13; Borenstein, 2000; Internet Policy Institute, 2001, p. 28; KPMG & Sussex Circle, 1998, p. 20).

As the law provides for recounts, there has to be a verifiable, auditable method for recording votes (California Internet Voting Taskforce, 2000A, p. 12; Neumann et al., 2000, p. 2).

As electronic votes are stored in database tables, these tables can be printed out such as on an Access or Excel spreadsheet, providing a paper copy or "transcript" (KPMG & Sussex Circle, 1998, p. 20; NZ. Ministry of Justice, 2003, p. 32, 54). However there is no way to check it against voters' intentions (Ananthaswamy, 2004, p. 8; Neumann et al., 2000, p. 2) to detect inaccuracies and correct them (although the same is true for paper ballots). This simply guarantees that whatever is in the system (whether fact or error) will be reflected in the printout (Internet Policy Institute, 2001, p. 28).

Audit trails can be created and viewed for (California Internet Voting Taskforce, 2000A, p. 3):

- logging the activities of persons accessing sensitive data. This can show which staff accessed which data (Green & Kunze-Hamel, 2001C, p. 4).
- logging any changes made to the data...what the changes were, when they were made, and who made them (Green & Kunze-Hamel, 2001C, p. 4; NZ. Ministry of Justice, 2003, p. 53).
- checking the encryption has not been tampered or the seal broken.
- matching that each ballot came from a legitimate voter (Ministry of Justice, 2003, p. 35, 53) without identifying who the voter is (Armacost et al., 2000, p. 25; California Internet Voting Taskforce, 2000A, p. 13; California Internet Voting Taskforce, 2000B, p. 18; Internet Policy Institute, 2001, p. 38)
- checking whether tampered votes can from a common IP address as the voter's IP address can be recorded with there vote (NZ. Ministry of Justice, 2003, p. 53). This is a cookie taken as a part of encoding. If a data adulteration has a common IP address, this provides a means for auditors to chase down the problem.
- The duplication/redundancy/backup provisions and certification provisions mentioned above provide evidence (Barry et al., 2001, p. 9; Carey, 2000) computer experts will use when testifying at an election outcome challenge (Carey, 2000; KPMG & Sussex Circle, 1998, p. 20).

These audit trails can be powerful tools for either verifying that security breaches have not occurred, or can identify any breaches that have occurred (Green &

Kunze-Hamel, 2001C, p. 4). For identified breaches, they also identify what needs to be corrected or patched.

With the Internet, there can be more checks, balances and controls than there is on the postal system. "For the people who said that Internet voting was too buggy to be trusted, others who are pushing e-voting can now point to paper voting as being, at least, not much better. And probably, they'll say, a lot worse" (Manjoo, 2000B, p. 2).

Some authorities provide cases wherein electronic calculation of votes contained some inaccuracies when there were no viruses changing the code (Barry et al., 2001, p. 2) and also when viruses changed the code (Carey, 2000; Gibson, 2001-2002, p. 573). Other authorities believe there are no electronic calculation errors and feel there would be other reasons than vote accuracy for requesting a recount of electronic votes (Alexander & Jefferson, 2000, p. 2; Internet Policy Institute, 2001, p. 27). In their view it appears that the only reason for a recount would be to establish the voter's intent. In such cases it is more the design of the ballot on the web site or the difficulty for voters to understand and follow instructions that would cause a recount request.

Conclusion

Although it is believed that the I-voting system only needs systems to be secure enough for the environment in which it operates, and since New Zealand is a society with very low levels of corruption, the I-voting system for N.Z. local government elections will not require the highest level of security available. However, I-voting is not implemented into an environment confined to New Zealand. A lax attitude toward security would open the opportunity for some overseas mensa hacker to take advantage of the trusting nature of New Zealanders and mess up the election just to prove s/he can.

With the systems described in this paper, there are enough redundancy and backups to make it extremely unlikely that any votes will be compromised (California Internet Voting Taskforce, 2000a, p. 12). This will result in a trustworthy voting system that people (both geeks and dummies alike) can feel confident using.

For the future, it will be necessary for EOs or sub-contractors to stay one step ahead of the hackers and continually study the security field (KPMG & Sussex Circle, 1998, p. 45; Russell & Cunningham, 2000, p. 3) because the technological capabilities and what the bad guys are doing with be constantly changing (Internet Policy Institute, 2001, p. 17).

Bibliography

- Alexander, K.I., & Jefferson, D. (2000, May 16). Internet voting: proceed cautiously. [Online] 3 pages. Available: <http://www.sjmercury.com/premium/opinion/columns/e-voting.htm> [2003, December 10].
- Ananthaswamy, A. (2004, February 14). Can we ever trust e-voting? *New Scientist* 181(2434), 7-8.
- Armacost, M. et al. (2000). The Future of Internet voting: a symposium co-sponsored by Brookings Institution and Cisco Systems, Inc. [Online] 34 pages. The Brookings Institute. Available: <http://www.brook.edu/comm/transcripts/20000120.htm> [2003, December 9].
- Barry, C., Dacey, P., Pickering, T., & Byrne, D. (2002). Electronic voting and electronic counting of votes: a status report. [Online]. 17 pages. Canberra: Australian Electoral Commission. Available: <http://www.aec.gov.au/content/Why/committee/subs/sub147/sub147e.htm> [2003, December 9].
- Borenstein, S. (2000, November 14). Better methods of voting debated. [Online] 3 pages. Available: <http://www.bergen.com/morenews/better14200011142.htm> [2004, 10 December].
- Bowman, L.M. (2000, November 3). Is online voting in your e-future? ZDNet News [Online] 3 pages. Available: <http://www.zdnet.com/zdnn/stories/news/0,4586,2650235-1,00.html> [2004, December 10].
- California Internet Voting Taskforce. (2000A). *A Report on the feasibility of Internet voting January, 2000 : Internet voting report*. Sacramento, Calif.: Office of the Secretary of State for California. [Online] 31 pages. Available: http://www.ss.ca.gov/executive/ivote/final_report.htm [2003, December 10].
- California Internet Voting Taskforce. (2000B). *Appendix A : Technical committee recommendations*. Sacramento, Calif.: Office of the Secretary of State for California. [Online] 41 pages. Available: http://www.ss.ca.gov/executive/ivote/appendix_a.htm [2003, December 10].
- Carey, J. (2000). Is There Any Help for the 'Hanging Chad'? : Punch cards are troublesome, but Internet voting could be, too. *Business Week* [Online] 3 pages. Available: http://www.businessweek.com/2000/00_48/b3709017.htm [2004, December 10].
- Coughlin, K., & Ward, J.T. (2000, November 12). Florida mess spurs calls for e-voting : Advocates claim it will be cleaner, faster. [Online]. 3 pages. Available:

<http://www.nj.com/news/ledger/index.ssf?elections/ledger/116f546.html> [2004, 10 December].

Cranor, L.F. (1998). Election automation - types of computerized voting systems. Electoral management. [Online]. 4 pages. Available: <http://www.aceproject.org/main/english/em/emf02/default.htm> [2003, December 15].

E-Local Government Project Team. (2003). *Strategic Plan for E-Local Government*. Wellington: NZ Society of Local Government Managers [and] Association of Local Government Information Managers [and] Local Government on-line [and] Local Government New Zealand.

Francisco, B. (2000, November 16). Online Voting. CBS Market Watch [Online] 3 pages. Available: <http://www2.marketwatch.com/news/yhoo/story.asp?nu=1&source=blq/yhoo&dist=yhoo&guid=%7BB16A29DC%2DB97D%2D11D4%2DB601%2D00A0C9EF346A%7D> [2004, 10 December].

Gibson, R. (2001-2002). Election online : assessing Internet voting in light of the Arizona Democratic Primary. *Political Science Quarterly* 116(4), 561-583.

Green, P. (1999). *Elections and technology - implications for the future*. Paper presented at the Conference on Electoral Research: The Core and the Boundaries, Adelaide, Australia p. 97-105. Available: http://www.eca.gov.au/research/conf_papers.pdf [2003, December 1].

Green, P. (2000, October 5). *The Politics of the future: the Internet and democracy in Australia: the Internet and the electoral process*. Presentation to the Australian Political Science Association's Politics of the Future seminar at the Australian National University. [Online]. 6 pages. Available: <http://www.elections.act.gov.au/adobe/PolFut.pdf> [2003, December 9].

Green, P. (2001A). *The Future of elections and technology*. Elections and Technology. Administration and cost of Elections Project. [Online]. 3 pages. Available: <http://www.aceproject.org/main/english/et/etq.htm> [2003, December 15].

Green, P. (2001B). *Minimising the risks in using technology*. Elections and Technology. Administration and cost of Elections Project. [Online]. 2 pages. Available: <http://www.aceproject.org/main/english/et/ete.htm> [2003, December 15].

Green, P. & Kunze-Hamel, G. (2001A). *Code security*. Elections and Technology. Administration and cost of Elections Project. [Online]. 2 pages. Available: <http://www.aceproject.org/main/english/et/et01c.htm> [2003, December 15].

Green, P. & Kunze-Hamel, G. (2001B). *Communications verification, testing and maintenance*. Elections and Technology. Administration and cost of Elections Project. [Online]. 3 pages. Available: <http://www.aceproject.org/main/english/et/ete05b.htm> [2003, December 15].

Green, P. & Kunze-Hamel, G. (2001C). *Data access security*. Elections and Technology. Administration and cost of Elections Project. [Online]. 4 pages. Available: <http://www.aceproject.org/main/english/et/ete01b.htm> [2003, December 15].

Green, P. & Kunze-Hamel, G. (2001D). *Encryption*. Elections and Technology. Administration and cost of Elections Project. [Online]. 2 pages. Available: <http://www.aceproject.org/main/english/et/ete08.htm> [2003, December 15].

Green, P. & Kunze-Hamel, G. (2001E). *Ensuring availability of data*. Elections and Technology. Administration and cost of Elections Project. [Online]. 2 pages. Available: <http://www.aceproject.org/main/english/et/ete03.htm> [2003, December 15].

Green, P. & Kunze-Hamel, G. (2001F). *Insurance*. Elections and Technology. Administration and cost of Elections Project. [Online]. 1 page. Available: <http://www.aceproject.org/main/english/et/ete06.htm> [2003, December 15].

Green, P. & Kunze-Hamel, G. (2001G). *The Internet*. Elections and Technology. Administration and cost of Elections Project. [Online]. 5 pages. Available: <http://www.aceproject.org/main/english/et/etf04.htm> [2003, December 15].

Green, P. & Kunze-Hamel, G. (2001H). *Manual/alternative contingency systems*. Elections and Technology. Administration and cost of Elections Project. [Online]. 2 pages. Available: <http://www.aceproject.org/main/english/et/ete04.htm> [2003, December 15].

Green, P. & Kunze-Hamel, G. (2001I). *Performance safeguards*. Elections and Technology. Administration and cost of Elections Project. [Online]. 2 pages. Available: <http://www.aceproject.org/main/english/et/ete07.htm> [2003, December 15].

Green, P. & Kunze-Hamel, G. (2001J). *Public information and privacy policies*. Elections and Technology. Administration and cost of Elections Project. [Online]. 3 pages. Available: <http://www.aceproject.org/main/english/et/ete10.htm> [2003, December 15].

Green, P. & Kunze-Hamel, G. (2001K). *Software verification, testing and maintenance*. Elections and Technology. Administration and cost of Elections

Project. [Online]. 4 pages. Available:
<http://www.aceproject.org/main/english/et/ete05c.htm> [2003, December 15].

Green, P. & Kunze-Hamel, G. (2001L). *Virus protection*. Elections and Technology. Administration and cost of Elections Project. [Online]. 3 pages. Available: <http://www.aceproject.org/main/english/et/ete01d.htm> [2003, December 15].

Internet Policy Institute. (2001). *Report of the National Workshop on Internet voting : issues and research agenda*. Sponsored by the National Science Foundation. Conducted in cooperation with the University of Maryland and hosted by the Freedom Forum. [Online] 63 pages. Available: http://www.digitalgovernment.org/archive/library/doc/ipi_onlinevoting.doc [2003, December 10].

Kohno, T., Stubblefield, A., Rubin, A.D., & Wallach, D.S. (2003). *Analysis of an Electronic voting system*. Johns Hopkins Information Security Institute Technical Report TR-2003-19, July 23, 2003 [Online] 2 pages. Available: <http://avirubin.com/vote/response.html> [2004, February 5].

KPMG & Sussex Circle. (1998). *Technology and the voting process: final report*. Montreal: Elections Canada. [Online]. 93 pages. Available: www.elections.ca/loi/vot/votingprocess_e.pdf [2003, December 15].

Manjoo, F. (2000B, November 10). *Ballots need an upgrade - Duh!* [Online]. 4 pages. Available: <http://www.wired.com/news/politics/0,1283,40078,00.html> [2003, December 1].

National Science Foundation. Office of Legislative and Public Affairs (2001, March 6). *Internet voting is no "magic ballot," distinguished committee reports*. [Online] 3 pages. Available: <http://www.nsf.gov/od/lpa/news/press/01/pr0118.htm> [2003, December 15].

Neumann, P.G., Mercuri, R., & Weinstein, L. (2000). IP: Internet and electronic voting. *The Risks digest* [Online] 21(14), 1-3. Available: <http://catless.ncl.ac.uk/Risks/21.14.html> [2004, January 11].

New Zealand. Ministry of Justice. Chief Electoral Office, & Abbott McCaw Richter & Associates. (2003). *On-line voting strategy and business*. Wellington: Ministry of Justice.

Panko, R.R. (n.d., in press). *Security: the snake in the e-commerce garden*. In S. Dasgupta (Ed), *Managing internet and intranet technologies in organizations: challenges and opportunities*. Hershey, Penn.: Idea Group Publishing.

Perera, R., Fonseca, B., Williams, M., & Uimonen, T. (2000, November 13). *E-voting could have prevented election confusion*. [Online] 4 pages. Available:

<http://www.infoworld.com/articles/hn/xml/00/11/08/001108hnevot.xml> [2004, December 10].

Rubin, A.D. (2002). Security considerations for remote electronic voting. *Association for Computing Machinery. Communications of the ACM* 45(12), 39-44.

Russell, R., & Cunningham, S. (2000). Hack proof your network : Internet tradecraft. Rockland : Syngress Media, Inc.

Salkever, A. (2000, November 15). A Vote for Online Ballots. [Online] 3 pages. Available: <http://www.securepoll.com/Archives/Archive11.htm> [2004, December 10].

Sommer, L. (2003). Great expectations : supply and demand in the economy of e-government. Presentation given to GOVIS 2003 Conference. Wellington: State Services Commission.

State Services Commission. E-Government Unit. (2003). *Blueprint : Authentication for e-government*. [Online] 15 pages. Available: <http://www.e.govt.nz/docs/authent-blueprint-200307/authent-blueprint.pdf> [2004, January 29].

Stuart, J. (2004). Authentication on the Internet. *Future Times* 4:10-11.

Sullivan, T.J. (2000, November 11). Casting votes via Internet coming, but still years off. Ventura County Star [Online] 3 pages. Available: <http://www.securepoll.com/Archives/Archive11.htm> [2004, December 10].

Waskell, E. (2000). From the editor. *The Bell* [Online] 1(2), 2. Available: <http://www.thebell.net> [2003, 1 December].

Weinstein, L. (2000A). *PFIR statement on Internet voting* [Online] 2 pages. Available: <http://www.pfir.org/statements/voting> [2004, January 11].

Weinstein, L. (2000B). Risks of Internet voting. *Association for Computing Machinery. Communications of the ACM* 43(6), 128.

Yang, S., & Sneiderman, P. (2004, January 21). Internet voting system set up for upcoming elections not secure, Computer experts say. *Science Daily News Release* University of California, Berkeley. [Online] <http://www.sciencedaily.com/releases/2004/01/040123005148.htm> 2004, January 26].

APPENDIX A: GLOSSARY

This Glossary was compiled from several sources: California Internet Voting Taskforce (2000B); Galston (1999, p. 7); Internet Policy Institute (2001); Local Electoral Act 2001; Local Electoral Regulation 2001, reg 48; NZ. Ministry of Justice (2003, p. 57-58); State Services Commission. E-Government Unit, (2003); and the Author.

ActiveX control: A program packaged in a format designed by Microsoft that is downloaded from a web server to a client browser and run within the browser, all as a mere side effect of visiting a web page.

Applet: A program in Sun Microsystems' Java programming language that is downloaded from a web server to a browser and run in the browser as a side effect of visiting a web page.

Authentication: The process by which a voter's eligibility to vote is verified. It verifies that an electronic ballot really is from the person it claims to come from, and not just from someone trying to electronically impersonate that person.

Ballot: A ballot is personal to the voter and represents the "voting paper" the voter completes. i.e. it includes the options available to that voter.

Browser: An application program such as Microsoft Internet Explorer or Netscape Navigator that allows the user to navigate the World Wide Web, and interact with pages from it.

Certification: The process the state uses to determine that a voting system meets the requirements of the California Election Code and can be used by any county that decides to select it.

Client: The device with which voters cast their ballot. In a common two-computer interaction pattern, one of them, the *client*, initiates a request, and the other, the server, acts on that request and replies back to the client. In the case of i-voting, "client" refers to the voter's computer that initiates the process of voting, and the server is the computer that accepts the ballot and replies to the client that it accepted it.

Counting program: A computer application program used to calculate both FPP and STV votes that must operate within a particular operating environment. (A modification of the definition in LEA 2001 s 5(1) and LEAA 2002 s 4.)

Decryption: Decoding an encrypted message (usually using a secret key).

Denial of Service (DOS) Attack: the use of one or more computers to 'Interrupt communications between a client and a server by flooding the target with more requests that it can handle.

Digital Certificate: An electronic credential, issued by a neutral, trusted third party, used to verify the identity of a user. By generating a digital signatures the authenticity and integrity of a document can be verified.

Distributed Denial of Service (DDOS) Attack: a more powerful denial of service attack that uses the processing power of multiple computers without the knowledge or consent of their owners to flood and overwhelm the intended target.

Election: A process for selecting representatives in a democratic way

Election Event: An event encompassing one or more (concurrent) elections. A New Zealand Local Government Election is an Election Event with approximately four *Elections*: one for mayor, one for City/District Councillors, One for Regional Councillors, and one for Health Board members

Election Integrity: ensuring the privacy of a voted ballot, the ability to audit the election for verifiability, and maintaining the security of the system.

Elector: Any person entitled under any law for the time being in force to vote at an election or poll as opposed to a "voter" who has actually voted.

Email: Electronic mail, i.e. messages and documents sent from one party to other specific, named parties.

Encryption: The transformation of data into a format that cannot be read without the appropriate key. A message is encoded (scrambled) using a secret key so that anyone intercepting the message but not in possession of the key cannot understand it. 512-bit is standard for most e-commerce transactions, but election software generally uses 1024-bit.

e-Voting: Any method of electronic voting which includes telephone voting, machine voting in polling booths, and Internet voting.

Firewall: One or more computers standing between a network ("inside") and the rest of the Internet (outside). It intercepts all traffic in both directions, forwarding only the benign part (where "benignness" may be defined by a complex policy), thereby protecting the inside from attacks from the outside.

Fit for purpose: The outcome of testing the system holistically to measure its compliance with all the principles of an acceptable election.

Hypertext Markup Language (HTML): the notation used for formatting text and multimedia content on web pages.

Hypertext Transfer Protocol (HTTP): the communication protocol used between web browsers and web servers for transporting web pages through the Internet.

I-voting: Internet voting refers to any method of voting in a public election in which the voter's ballot is retrieved via the Internet from the Local/Territorial Authority's vote server, presented to the voter electronically on a computer screen, marked electronically by the voter, and then transmitted back to the vote server via the Internet. There are several variations of I-voting that should be distinguished in any discussion, because they have markedly different security properties.

Integrity: Protecting data from undetected modification by unauthorized persons, usually through use of a cryptographic hash or digital signature.

Internet: The worldwide system of separately-owned and administered networks that cooperate to allow digital communication among the world's computers.

Internet Protocol (IP): the basic packet-exchange protocol of the Internet. All other Internet protocols, including HTTP (the Web) and SMTP (email) use it.

IP Address: A unique number (address) assigned to every computer on the Internet, including home computers temporarily connected to the Internet.

Internet Service Provider (ISP): A company whose business is to sell access to the Internet, usually through phone lines or CATV cable.

Key: A typically (but not always) secret number that is long enough and random-looking enough to be unguessable; used for encrypting or decrypting messages.

Local Area Network (LAN): a short-range (building-size) network with a common administration and with a only small number of hosts (computers) attached. The hosts are considered to be sufficiently cooperative that only light security precautions are required.

Malicious code: A program with undesirable behavior that operates secretly or invisibly, or is disguised as part of a larger useful program; in this document, the same as "Trojan horse".

Malicious software: programs developed by mischievous computer programmers that are capable of performing a wide range of functions on 'infected' computers, from the benign to the malign. Benign viruses can simply perform harmless (but usually annoying) functions such as displaying a pop-up message. Malign viruses can corrupt or change data or programs, destroy computer files, or cause massive amounts of email to be generated, threatening the stability of networks by swamping them with data. They either hide the harmful action or perform it so quickly that it cannot be stopped. Viruses can be executable files (with a '.exe' filename extension) or files in other formats, such as word processing files containing macros. Running these executable files or opening files containing infected macros can cause a computer virus program to run.

Mirroring: Keeping two or more memory systems or computers identical at all times, so that if one fails the other can continue without any disruption of service.

Online: Generally, a synonym for "on the Internet", or sometimes, more specifically, "on the web".

Open source: Software whose code is published and available for all users to see. Usually the only condition for its use is that should the user modify or extend the code, the result is to also be published.

Packet: The smallest unit of data (along with overhead bytes) transmitted over the Internet in the IP protocol.

Password: A word or phrase that only you know which can be used to gain access to some services. You will be able to get a password only when the authentication agency has established your identity.

Personal Computer (PC): any commercial computers marketed to consumers for home or business use by one person at a time. In 1999, this includes Intel-based computers (and clones) running a Microsoft operating system or a competitor (e.g. Linux, BEOS, etc.), and it also includes Macintoshes.

Platform: the underlying hardware and software of a voting system.

Plug-in: A software module that permanently extends the capability of a web browser.

Polling day: The day on which the voting period for an election or poll ends.

Privacy: Protecting data from being read by unauthorized persons, generally by encrypting it using a secret key.

Private Elections: elections conducted by private organizations (e.g., corporations, unions, political parties).

Private key: A key, or one member of a key pair, that must be kept secret by one or all members of a group of communicating parties.

Protocol: An algorithm or program involving two or more communicating computers.

Public key: One member of a key pair that is made public.

Public Key Infrastructure (PKI): a framework established to issue, maintain, and revoke digital certificates that accommodates a variety of security technologies to ensure authentication, integrity, and confidentiality.

Redundancy: Excess storage, communication capacity, computational capacity, or data, that allows a task to be accomplished even in the event of some failures or data loss.

Remote Voting: the casting of ballots at private sites (e.g., home, school, office) where the voter or a third party controls the voting client, not voting officials as is the case at polling booths or supervised kiosks.

Risk: A measure of both the likelihood and the consequence of an adverse event. The risk of an election might be considered the total of the probability times the consequence of each possible election systems failure mode. The degree of risk depends not only on the election system in place, but also to some extent on the type of election and the political culture of a jurisdiction.

Script: In the context of this document this term refers to a program written in the JavaScript language, embedded in a web page, and executed in browser of the web client machine when it visits the web page.

Scrutineers: Individuals from differing and conflicting interests selected by election candidates to observe behind the scenes the scrutiny of electoral rolls, the decisions regarding possible informal votes or spoiled voting papers, and to observe the processing and possibly the counting of the votes

Secure Socket Layer (SSL): an encryption protocol used to ensure the authenticity and security of a connection, and the privacy and integrity of a transaction.

Security: General term covering issues such as privacy, integrity, authentication, etc.

Server: A computer that manages network resources. Votes are accumulated, tallied and stored at this location. In a two-computer interaction pattern, one of them, called the client, initiates a request, and the other, the *server*, acts on that request and replies to the client.

Source Code: software program instructions in their original form; the only format that is readable by humans.

Special votes: As described in LEA 2001 s 21, local/territorial authorities provide a means for electors to vote who are on the ratepayer roll or will be overseas for the full postal voting period or who for any reason indicate that they failed to receive their voting papers by mail or who for any reasons spoiled their voting papers.

Spoof: To pretend, usually through a network, to be someone or somewhere other than who or where you really are

Transparency: the ability of citizens to understand how elections are conducted.

Trojan Horse: An apparently harmless program containing hidden code that, once installed, allows for the unauthorized collection, falsification, or destruction of information. Disguised as part of a larger useful program, it performs undesirable behaviour. The same as "malicious code".

Uniform Resource Locator (URL): i.e. a name for a web page, such as <http://www.example.com>

Universal Serial Bus (USB) port: a port (connector) on newer computers used for high speed serial communication with attached devices.

Virus: A Trojan Horse program that actively makes, and covertly distributes, copies of itself. See also **Malicious software**.

Vote: A vote represents a voter's choice for a single Contest. i.e. New Zealand local government elections allow voters to make one (valid) vote for Mayor, a varying number of valid votes for City/District Councillors, a varying number of valid votes for Regional Councillors.

Vote client: The computer that voters use to cast their ballots, which are then sent to the vote server.

Vote server: The computer(s) under control of the county that receives and stores votes transmitted by Internet from vote clients.

Voter: Any person who has voted as opposed to an "elector" who is eligible to vote.

Web: The world-wide web, or WWW; the worldwide multimedia and hypertext system that, along with email, is the most familiar service on the Internet.

Web site: A collection of related web pages, generally all located on the same computer and reachable from a single top-level "home page".

Web page: A single "page" of material from a web site.

APPENDIX B: Verification Tests and Test Measures for Communications, Hardware and Software

Communications Tests	Hardware Tests	Software Tests
Verification tests	Verification tests	Verification tests
<ul style="list-style-type: none"> • testing of communications under conditions simulating expected real-life conditions • ensuring the communications system conforms with local environmental requirements, including shelter, space, furnishings and fittings, electrical power supply and relevant extremes of temperature, humidity and pollution • ensuring appropriate documentation is adequate and complete • verifying that the communications system is capable of performing under expected normal conditions and possible abnormal conditions • ensuring appropriate security measures are in place and that they conform to acceptable standards • ensuring that appropriate quality assurance measures are in place (Green & Kunze-Hamel, 2001B, p. 1-2). 	<ul style="list-style-type: none"> • testing hardware for accuracy which is crucial to a well-functioning system • testing hardware under conditions simulating expected real-life conditions, including storage, transportation, operation and maintenance environments • ensuring the hardware conforms with local environmental requirements, including shelter, space, furnishings and fittings, electrical power supply and relevant extremes of temperature, humidity and pollution • ensuring appropriate documentation is adequate and complete • verifying that hardware is capable of performing under expected normal conditions and possible abnormal conditions • ensuring appropriate security measures are in place and that they conform to appropriate standards 	<ul style="list-style-type: none"> • testing of software to ensure that appropriate standards are met and that the software performs its intended functions, including audits of code • ensuring system documentation is adequate and complete • verifying that systems are capable of performing under expected normal conditions and possible abnormal conditions • ensuring that security measures are in place and that they conform to appropriate standards ensuring that appropriate quality assurance measures are in place (Green & Kunze-Hamel, 2001L, p. 1-2).

	<ul style="list-style-type: none"> ensuring that appropriate quality assurance measures are in place (Green & Kunze-Hamel, 2001G, p. 1). 	
Testing measures	Testing Measures	Testing Measures
<ul style="list-style-type: none"> developing a set of test criteria applying functional tests to determine whether the test criteria has been met applying qualitative assessments to determine whether the test criteria has been met conducting tests in both 'laboratory' and 'real life' conditions conducting tests over an extended period of time, to ensure systems can perform consistently conducting 'load tests', simulating as closely as possible a variety of 'real life' conditions using or exceeding the amounts of data that can be expected in an actual situation verifying that 'what goes in' is 'what comes out', by entering known data and checking that the output agrees with the input (Green & Kunze-Hamel, 2001B, p. 2). 	<ul style="list-style-type: none"> developing a set of test criteria applying 'non-operating' tests to ensure that equipment can stand up to expected levels of physical handling, such as transit drop tests examining (if appropriate) any code 'hard wired' in hardware (this code is sometimes known as firmware) to ensure its logical correctness and to ensure that appropriate standards are followed applying functional tests to determine whether test criteria are met applying qualitative assessments to determine whether test criteria are met conducting tests in both 'laboratory' conditions and in a variety of 'real life' conditions conducting tests over an extended period of time, to ensure systems could perform consistently 	<ul style="list-style-type: none"> developing a set of test criteria applying functional tests to determine whether the test criteria have been met applying qualitative assessments to determine whether the test criteria have been met conducting tests in 'laboratory' conditions and conducting tests in a variety of 'real life' conditions conducting tests over an extended period of time, to ensure systems can perform consistently conducting 'load tests', simulating as close as possible a variety of 'real life' conditions using or exceeding the amounts of data that can be expected in a real situation verifying that 'what goes in' is 'what comes out', by performing logic and accuracy tests (Green & Kunze-Hamel, 2001L, p. 2-3).

--	--	--

	<ul style="list-style-type: none">• conducting 'load tests', simulating as closely as possible a variety of 'real life' conditions and using or exceeding the amounts of data that could be expected in an actual situation• conducting logic and accuracy tests (Green & Kunze-Hamel, 2001G, p. 1-2).	
--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Autobiography

Janita Stuart holds BSc and MLIS degrees from the U.S.A. and MIM from Victoria University. She performs strategic planning, business analysis, and computer application implementation for IM centres.

Val Hooper is a lecturer in the School of Information Management at Victoria University of Wellington.

Janita R. Stuart
16 Tremaine Place
Porirua City
233-0146, 029-200-8847, 918-9021