

Simply Voting submission to the Special Committee on Electoral Reform

Submitted by Brian Lack
on September 20, 2016


Background

1. Simply Voting Inc. is a full-service provider of secure, internet voting based in Montreal. It serves over 1000 customers from varied sectors including universities, associations, unions, political parties, and First Nations. On any given day of the year it is running approximately 100 concurrent voting events and has never suffered a security incident.
2. Of particular relevance to this committee, Simply Voting has delivered internet and telephone voting to several municipalities during the 2014 Ontario municipal elections and will be running the upcoming PEI Plebiscite on Democratic Renewal on our platform, the latter being the first province-wide internet vote in North America.
3. Brian Lack, President and founder of Simply Voting Inc. first developed Simply Voting's online voting system in 2003 and holds a B.Sc. From McGill University in Computer Science.

An Elevated Threat

4. Currently internet voting is being used in Canada for municipal elections in Ontario and Nova Scotia. This application of voting technology has been a success, more municipalities are coming on board each election cycle and it is anticipated that more provinces will allow municipal internet voting in the future.
5. However, as the significance of the voting event increases, so does the danger of an attack. Economic and political powers wielded by federal governments are far greater than those wielded by municipal governments. Campaign budgets for federal elections run in the tens of millions of dollars¹, dwarfing municipal campaigns. With much higher stakes, the candidates, parties, supporters, interest groups and even organized crime direct far more resources towards influencing the outcome and may be tempted to target the voting system.

[1] https://en.wikipedia.org/wiki/Federal_political_financing_in_Canada



6. At the federal level, external actors become interested in the outcome as well. International organized crime, hacker groups such as Anonymous, Russia, China, and even the U.S. National Security Agency all have powerful cyberwarfare capabilities. The Arizona and Illinois online voter registration systems were recently hacked, allegedly by foreign actors, which is a clear example of this threat².

7. With a significant amount of technological resources applied, an actor may take advantage of the following vulnerabilities of internet voting. These vulnerabilities exist due to the limitations of web technology in general, irrespective of the particular internet voting system being used.

Targeted Malware


8. Malware is a malicious program that does something on the infected computer against the computer owner's wishes and without their knowledge. Some malware, such as the Stuxnet worm which destroyed centrifuges of Iran's nuclear program³, is engineered with a specific target and purpose in mind. Malware can be engineered specifically to hijack a particular vote on a particular internet voting system. When the voter signs on to the internet voting system from an infected computer and clicks on Candidate A, the malware would silently submit a vote for candidate B. The voter would never know the difference.

9. To be successful in affecting the outcome of the vote, enough eligible voters' computers must be infected with the malware. The malware could either be a self-propagating virus or the attacker could make use of a "Botnet". A "Botnet" is a number of personal computers infected with a type of computer virus that allows a single hacker to take control of all the computers. Large Botnets comprised of hundreds of thousands of computers are known to exist⁴. They are often used for spamming, denial-of-service attacks, and fraudulent activity. The operator of a Botnet could easily install the malware of his choosing across the computers.

[2] <http://www.theverge.com/2016/8/29/12692756/voter-registration-hack-arizona-illinois-election-security>

[3] <https://en.wikipedia.org/wiki/Stuxnet>

[4] <https://en.wikipedia.org/wiki/Botnet>



10. No matter how advanced the internet voting system's security may be, the computers on which the voting occurs are not secure. This type of attack is very difficult to detect let alone stop, unless personalized voting codes are used which undermine the convenience and accessibility that internet voting promises.

Zero-Day Vulnerabilities

11. Leading internet voting systems follow best practices in internet security and are generally protected against known hacking techniques. The true danger is from unknown hacking techniques, known as "zero-day". Cybercriminals and intelligence agencies discover, collect and exploit zero-day vulnerabilities, which could be used to gain access to servers or decrypt encrypted data⁵. For example, the Stuxnet worm mentioned above made use of several zero-day vulnerabilities to effectively attack its target.

12. It is extremely difficult for any online service to protect itself against unknown vulnerabilities, and no server on the internet is truly 100% secure. When a zero-day vulnerability is exploited it risks becoming known to the security community and therefore becoming less potent. Actors would not "waste" a zero-day hack on a low-value target. Yet a federal election is undoubtedly a high value target.

Conclusion

13. Despite the fact that Simply Voting is a major Canadian internet voting vendor, its recommendation is **against the use of internet voting for federal elections**. The heightened threat level of a federal election pushes the security of internet voting past its limits and poses too much of a risk.

14. However, it should be noted that plebiscites, territory elections, municipal elections and First Nations elections are all **excellent applications for internet voting** where existing security measures are extremely high compared to the level of threat. If this committee were to conclude that internet voting is not safe enough for federal elections, it would be important to qualify that recommendation and not characterize the technology as flawed or unusable in general.

[5] [https://en.wikipedia.org/wiki/Zero-day_\(computing\)](https://en.wikipedia.org/wiki/Zero-day_(computing))