Threats to Electronic Voting Systems in Canada
Date: September 16, 2018

Disclaimer: this briefing note contains summaries of open sources and does not represent the views of the Canadian Association for Security and Intelligence Studies.

Key events

Electoral voting systems have been the subject of several cybersecurity reviews, and speculation about them being vulnerable. In 2017, Communications Security Establishment noted that electronic voting tabulation may be vulnerable to third party cyberattacks (CSE, 2017). In March 2018, a report from Brazil demonstrated it was possible to attack the voting machine (Aranha et. al., 2018). Moreover, a 2018 report by Elections BC includes reference to the requirement that voting machines must maintain an internet connection, thus creating a vulnerability for a potential cyber-attack (Archer, 2018).

Nature of Discussion

This report is organized into the following points: a) what is the specific electronic voting vulnerability being considered (SQL Injection)?; b) how are these attacks carried out against the electoral system?; and c) what is the impact of a cyberattack on the integrity of voting process (e.g. balloting, voter confidence, and electoral outcome)?

Background

Traditional electoral systems consist of a number of physical checks and balances between identification of a voter, validation of their vote, and the counting of the final vote. Electronic voting introduces one more level of accountability, but also increases levels of vulnerability. One

such vulnerability is the potential compromising of the electoral database, which records the electronic vote. For example, during the Ontario election in June 2018, the province made extensive use of optical scan tabulators for vote counting (The Canadian Press, 2018). These tabulating machines may be one such system which could potentially be exploited in Canada.

Online voting is not a novel concept. In Estonia, it has been used federally since 2005 with mixed results (Springall et al, 2014). However, some of the key vulnerabilities in online voting may have been demonstrated by Russia, who allegedly attacked the Ukrainian electoral system in 2014, which resulted in delayed election reporting (Clayton, 2014). Moreover, a 2018 paper by Aranha et. al., suggests that a SQL attack could be utilized against voting machines to violate the secrecy of the ballot by attacking the computer network that the machines are connected to. One potential attack vector could be achieved through exploiting the communication network transmitting information from voting places to headquarters and back. This potential exploit may enable the cyber attacker to gain access to the voters' data set while potentially bypassing any security systems that are built directly into the voting machines.

To protect electoral systems, Ontario required municipalities to pass a by-law allowing online voting by May, 2017 for the 2018 elections (Butler, 2018). However, there appears to be no set of standards for online voting or security standards that the municipalities are required to adhere to (Porup, 2018). One possible model for delivering electronic voting is being considered by Keith Archer, Chief Electoral Officer in British Columbia. Archer is proposing:

> "[…] a communication network that transmits information from voting places to headquarters and back, resulting in an almost instantaneous sharing of voter participation information across voting places. This allows real-time strike-off of voter participation across voting places, protecting the system from multiple votes, while removing the need for

> the 'provisional' absentee ballots of the current model" (Archer, 2018: 26).

In New Brunswick,

> "the 2014 election saw malfunctioning software cause issues tallying votes - ultimately delaying the release of the election's final results by two hours. Officials say there was never a problem with the tabulation machines themselves but that it was a program processing the initial results that had a glitch. The program failed to properly transfer polling data from a computer server in Fredericton to a website where media outlets were gathering results. The software was used to get the results to the media as quickly as possible" (Quon, 2018).

Since the 2014 election New Brunswick has since changed systems and data validation processes, prior to their election in September 2018. The article notes "some votes disappeared from the website during the delay, which prompted speculation about the validity of the election. Despite the glitches, the final vote counts were accurate" (Quon, 2018).

Key Points of Discussion and West Coast Perspectives

Currently, BC Gaming uses the TGS1 standard for testing their electronic gaming machines. This is a global standard to protect the integrity of the gambling environment, gamblers identity, and financial data (Gaming Policy and Enforcement Branch, 2016). Could or should provincial and federal electoral agencies, and associated electoral voting vendors explore this standard as a comparable testing model?

What can British Columbia learn from Canadian specific examples of voting issues related to specific computer software and hardware events which interfered with election processes? For example, how did New Brunswick select their current systems and validation processes?

Does British Columbia face the same potential threats as Ontario and other electoral regions? Should the province begin to expand the accessibility of convenience voting (advanced polls and absentee

ballots) to include electronic voting machines and/or remote voting systems that would allow electors to cast a ballot from potentially insecure places and networks?

References

Aranha, D. F., Barbosa, P. Y. S., Cardoso, T. N. C., de Araújo, C. L., & Matias, P. The Return of Software Vulnerabilities in the Brazilian Voting Machine.Aranha, D. F., Barbosa, P. Y. S., Cardoso, T. N. C., de Araújo, C. L., & Matias, P. The Return of Software Vulnerabilities in the Brazilian Voting Machine.

Archer, K. (2018). *Report of the Chief Electoral Officer on Recommendations for Legislative Change* (Canada, Elections BC). (May, 2018) Retrieved from https://elections.bc.ca/docs/rpt/2018-CEO-Recommendations.pdf

Butler, C. (2018). Ontario civic elections: the problem with online voting. (April 4, 2018) Retrieved from https://www.cbc.ca/news/canada/london/london-ontario-online-voting-1.4598787

Communications Security Establishment (2017). Cyber Threats To Canada's Democratic Process. Retrieved from https://cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process

Clayton, M. (2014). Ukraine election narrowly avoided 'wanton destruction' from hackers. (June 17, 2014) Retrieved from https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers

Gaming Policy and Enforcement Branch (2016). TGS5 Technical Gambling Standards for Internet Gambling Systems (IGSs) Technical Standards Document (TSD) Version 2.2. Retrieved from https://www2.gov.bc.ca/assets/gov/sports-recreation-arts-and-culture/gambling/gambling-in-bc/stds-tech-gaming-tgs5.pdf

Porup, J.M. (2018). Online voting is impossible to secure. So why are some governments using it? (May 2, 2018) Retrieved from https://www.csoonline.com/article/3269297/security/online-voting-is-impossible-to-secure-so-why-are-some-governments-using-it.html?page=2

Quon, A. (2018). Elections New Brunswick says there will be no technical glitches on election night. (August 27, 2018) Retrieved from https://globalnews.ca/news/4405070/elections-new-brunswick/

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014, November). Security analysis of the Estonian internet voting system. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 703-715). ACM.

The Canadian Press. (2018). Voting in Ontario's spring election? It's going to be a bit different this time. CBC News. (May 9, 2018) Retrieved from https://www.cbc.ca/news/canada/toronto/ontario-election-electronic-voting-machines-1.4655427

Published by the Journal of Intelligence, Conflict and Warfare and Simon Fraser University, Volume 1, Issue 3.

Available from: https://jicw.org/