TITLE: Threats to Electronic Voting Systems in Canada
Date: Sept 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 that the electoral voting systems is vulnerable. In 2017 CSE noted electronic voting tabulation may be vulnerable to third party cyberattacks. In March 2018 a report from Brazil demonstrated it was possible to attack the voting machine. The final key event is the published report in 2018 by Elections BC which includes reference to the requirement voting machines must maintain an internet connection thus creating a vulnerability for a potential cyber attack.

NATURE OF DISCUSSION

This report is organized into the following points; What is the specific electronic voting vulnerability being considered (SQL Injection), How are these attacks carried out against the electoral system, and finally, 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. 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. 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. More specifying a 2018 paper by Aranha et al, demonstrates how 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. However, there appears to be no set of standards for online voting or security standards that the municipalities are required to adhere to. One possible model for delivering electronic voting is being considered by BC's Chief Electoral Office Keith Archer. 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."

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." 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".

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. Could or should provincial and federal electoral agencies, and associated electoral voting vendors explore this standard as a comparable testing model?

What can BC 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 BC 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?