Internet Voting in Canada: A Cyber Security Perspective

Aleksander Essex
Department of Electrical and Computer Engineering
Western University, Canada
aessex@uwo.ca

Summary. Secure and verifiable Internet voting remains one of the most challenging open problems in cyber-security. Despite numerous potential social benefits, the technological risks are many, and the democratic stakes, therefore, remain high. We recommend the Special Committee on Electoral Reform (ERRE) not proceed with Internet voting in federal-level elections until (a) research and development efforts can create effective end-to-end election verification technologies, and (b) a national framework for secure Internet voting can be created establishing security standards, software testing requirements, government oversight, and legal accountability.

I. Introduction

You can bank online. You can shop online. You can file your taxes online. You can renew your license online. Why don't you vote online? It seems like a natural use of the technology. The perceived advantages of Internet voting typically center on otherwise reasonable goals like increasing voter turnout, reaching under-represented populations, improving accessibility and decreasing election costs. But one of the main reasons we don't vote online already is because, simply put, Internet voting is a really difficult security challenge that we haven't solved.

As a simplification of a very complex problem, the reason Internet voting is harder than other cyber-security systems comes down to the a fundamental tension between the security goals of ballot secrecy, and election integrity. If we simply did away with the secret ballot, Internet voting security would become much more tractable, and resemble other security systems, like online banking.

The technical challenge of electronic voting comes from requiring security and secrecy at the same time. How do you prove my vote counted, when you don't know what my vote even was? This can be accomplished in a suitably reliable fashion with paper ballots and in-person polling through a combination of physical and procedural security measures, along with the immediately observable nature of the physical word. There is, however, no direct software analogue to the physical guarantee that paper ballots going into an empty box are the same as what comes out at the end of the day.

II. Threat Overview

In its most basic form, contemporary commercial Internet voting systems consist of a standard web-application framework; a voting program (typically Javascript) is sent from the election server across the Internet to your browser. When you cast a ballot, the information about your selections is returned to the server and stored in a database to be tabulated later. Security is required at all points in this chain: at your device, in transit, and at the election server.

From a security perspective, this architecture introduces a host of potential threats not found in Canada's current in-person hand-counted paper ballot method.

Vote Selling and Coercion. Because of the inherent unsupervised nature of Internet voting, individuals can be observed by others while voting, and thus could be unduly influenced in their voting intentions.

Phishing. Numerous online avenues exist to misdirect voters into visiting misleading or

malicious websites, or visiting legitimate URLs that deliver, for example, cross-site scripting payloads.

Automation bias. Habituation and lack of comprehension about the goals and purpose of common web security technologies can lead users to place an undue reliance on technological protections, as well as underestimate the significance of warnings or errors. Examples include not noticing when the green padlock icon is missing, or clicking through browser security warnings. This is further complicated by the fact that many websites (see e.g., https://elections.on.ca) generate errors due to simple misconfigurations.

Denial of Service. The distributed nature of the Internet makes it possible for a server to be flooded with connection requests from numerous distributed machines. Although technological mitigations exist for attacks of this kind, they do occasionally cause significant disruptions. For example, a denial of service attack in 2015 caused Canadian federal government websites to be inaccessible for several hours.

Client-side Malware/Spyware. Owing to our connected lifestyle, the computational device we would use to cast a ballot would likely have previously been used in many other contexts. Numerous opportunities thus exist to inject malicious software onto a voter's computer with the intention of altering and/or surveilling ballot selections. Any acceptable Internet voting system must be robust, even in the presence of malware.

Network attacks. Numerous possibilities exist for an internet attacker located in between the network connection of a voter and the election server to attempt to view or modify ballot data. A fundamental and necessary security protection is Transport Layer Security (TLS), which is commonly denoted in your browser as a green padlock. User errors, server-side misconfigurations, and novel cryptographic attacks can all be leveraged in a "man-in-the-middle" attack to access or alter voter preferences. Despite this being a core internet security technology, we found that of the 14 federal, provincial, and territorial election agency websites, only Elections Nova Scotia supported TLS. Further, we found TLS misconfigurations in the Elections Ontario and Elections PEI websites. See Table 1.

Agency	TLS Support	Server Location[1]
Elections Canada	Unsupported	Canada
Elections Alberta	Unsupported	U.S.
Elections BC	Unsupported	Canada
Elections Manitoba	Unsupported	Canada
Elections New Brunswick	Unsupported	Canada
Elections Newfoundland	Unsupported	Canada
Elections NWT	Unsupported	Canada
Elections Nova Scotia	Supported	Canada
Elections Nunavut	Unsupported	Unknown
Elections Ontario	Misconfigured	U.S.
Elections PEI	Misconfigured	Canada
Elections Quebec	Unsupported	Canada
Elections Saskatchewan	Unsupported	U.S.
Elections Yukon	Unsupported	Canada

Table 1. Current TLS Support Across Canadian Election Agency Websites

Server penetrations. A Canadian federal election today technically consists of 338 separate elections held in thousands of separate polling places spread across the country. An Internet-based system consolidates all of these on to one internet-facing server, reachable by any computer in the world. Any combination of undisclosed software vulnerabilities, misconfigurations, or human error could allow a remote attacker to gain access to voter registration information or ballot data. Instances of server penetrations (e.g., ransomware, email and password dumps, IP theft, etc.) are becoming increasingly common, and examples can be found across all organizational sectors.

Insider Influence. There is a risk of insiders (e.g., election officials, vendors, technicians, etc.) viewing or modifying ballot selections on the

[1] Based on iplocation.net consensus.

server, making it vital for there to be strong mechanisms to prevent undetected changes to votes.

State-level Actors. Perhaps the greatest threat to an Internet election is a sophisticated attack by a state-level actor who undetectably changes an election result. Examples of such potential state-level intervention in elections have surfaced in the United States in the context of voter registry data. In a worst-case scenario the ensuing political turmoil of a stolen election could precipitate an economic collapse, or worse, a war. Further, it is not certain whether a sophisticated attack would ever even be detected. From that perspective, any federal-level Internet voting system is a critical infrastructure, and its safeguard could reasonably be viewed as a matter of national security.

III. Recommendations.

A. End-to-end Verifiability.

Recent research into Internet voting implementations has shown weak procedural security (Springall et al., 2014; Wolchok et al., 2010), and weak, vulnerable, or ad-hoc security implementations and configurations (Wolchok et al., 2012; Clark & Essex, 2014; Teague & Halderman, 2015). One promising approach is cryptographic end-to-end verifiable Internet voting (E2E-VIV), which allows voters to create privacy-preserving receipts of their ballot, which can later be used as part of a public, universally-verifiable cryptographic proof of correctness. Two notable projects include Helios (Adida, 2008) and Scantegrity/Remotegrity (Carback et al., 2010; Zagorski et. al, 2013), the latter of which was deployed in the first governmental E2E verifiable election in the city of Takoma Park, MD in 2009 and 2011.

A recent report by the U.S. Vote Foundation (Dzieduszycka-Suinat et al., 2015) has gone as far as to suggest *all* Internet elections be E2E-VIV. Owing to its extensive use of cryptography, however, many research challenges remain to make such schemes practical in terms of functional requirements (i.e., usability, accessibility, etc.) and conceptual requirements (understandability, verifiability, etc.). Giving these risks and potential avenues for developing mitigations, we recommend, therefore, ERRE *not* proceed with Internet voting at this time, and instead prioritize research into Internet voting verification technologies, and promote interdisciplinary opportunities for research collaborations to explore issues at the intersection of elections and cyber-security.

B. National Framework for Internet Voting

Before Canada can proceeded with Internet voting, it would be vital to establish a national framework to lay out security standards, software requirements, testing methodologies, government oversight, and legal accountability.

Regarding testing and government oversight, an advisory panel to the state of Utah (Cox et al., 2015) recently recommended that any candidate system be made available in an open trail in which the public is invited to conduct penetration testing through a series of mock elections over the Internet. As demonstrated by Wolchok et al. (2012), this can be an effective means of discovering critical vulnerabilities in a realistic, but non-live election scenario.

Regarding standards and requirements, the government does not necessarily have the in-house expertise to adequately evaluate and verify Internet voting systems. Similar to the recommendations of the Internet voting advisory panel to the Legislative Assembly of British Columbia (Independent Panel, 2014), we recommend the formation of an independent technical committee consisting of election administrators and Internet voting security experts. This committee would be responsible for rigorously evaluating the security of candidate systems.

Conclusion. ERRE should be aware that considerable concern about the safety of Internet voting exists among international technology and cyber-security experts. Echoing a statement by prominent U.S. computer technologists (Computer Technologists), we urge Internet voting only be adopted after the numerous technical threats outlined above can be suitably mitigated, and strong

mechanisms put in place to prevent undetected changes. The entire system must be reliable and verifiable in a way that is convincing to the voting public.

REFERENCES

[1] B. Adida. Helios: web-based open-audit voting. In USENIX Security Symposium, pages 335–348, 2008.

[2] R. T. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P. S. Hernson, T. Mayberry, S. Popoveniuc, R. L. Rivest, E. Shen, A. T. Sherman, and P. L. Vora. Scantegrity II election at Takoma Park. In USENIX Security Symposium, 2010.

[3] J. Clark and A. Essex. Security Assessment of Vendor Proposals, Final Report. City of Toronto RFP #3405-13-3197, 2014. https://www.verifiedvoting.org/wp-content/uploads/2014/09/Canada-2014-01543-security-report.pdf

[4] Computer Technologists Statement on Internet Voting. https://www.verifiedvoting.org/projects/internet-voting-statement/

[5] S. J. Cox, A. Lawrence, C. Bramble, R. Chavez-Houck, R. Cowley and others. iVote Advisory Committee Final Report for the State Utah, 2015. https://elections.utah.gov/Media/Default/Documents/Report/iVote%20Report%20Final.pdf

[6] S. Dzieduszycka-Suinat, J. Murray, J. Kiniry, D. Zimmerman, D. Wagner, P. Robinson, A. Foltzer, and S. Morina. The Future of Voting: End-to-End Verifiable Internet Voting - Specification and Feasibility Study. https://www.usvotefoundation.org/E2E-VIV, 2015.

[7] Independent Panel on Internet Voting. Recommendations Report to the Legislative Assembly of British Columbia, 2014. https://www.verifiedvoting.org/wp-content/uploads/2014/10/CA-BC-2014-recommendations-final-report.pdf

[8] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman. Security analysis of the Estonian Internet voting system. In Proceedings of the 21st ACM Conference on Computer and Communications Security. ACM, Nov. 2014.

[9] V. Teague and J. A. Halderman. The new south wales ivote system: Security failures and verification flaws in a live online election. In VoteID, 2015.

[10] S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati, S. K. Sakhamuri, V. Yagati, and R. Gonggrijp. Security analysis of india's electronic voting machines. In Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS), 2010.

[11] S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman. Financial Cryptography, chapter Attacking the Washington, D.C. Internet Voting System, pages 114–128. 2012.

[12] F. Zagorski, R. T. Carback, D. Chaum, J. Clark, A. Essex, and P. L. Vora. Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System. 2