Le vote par Internet au Canada : optique de cybersécurité

Aleksander Essex
Département de génie électrique et de génie informatique
Western University, Canada

Sommaire. Le vote par Internet sécurisé et vérifiable est encore l'un des problèmes non résolus les plus complexes de la cybersécurité. Malgré les nombreux avantages sociaux potentiels qui s'y rattachent, les risques technologiques sont importants, et les enjeux démocratiques demeurent donc élevés. Nous recommandons au Comité spécial sur la réforme électorale (ERRE) de ne pas aller de l'avant avec le vote par Internet dans le cadre d'élections fédérales tant et aussi longtemps a) que les efforts en matière de recherche-développement n'auront pas entraîné des technologies efficaces de vérification de bout en bout des élections, et b) qu'un cadre national de vote par Internet sécurisé n'aura pas été créé en vue de l'établissement de normes de sécurité, d'exigences liées à l'essai de logiciels, d'une surveillance gouvernementale et d'une responsabilité légale.

I. Introduction

Nous pouvons faire nos transactions bancaires en ligne. Nous pouvons faire des achats en ligne. Nous pouvons produire notre déclaration de revenus en ligne. Nous pouvons renouveler notre permis de conduire en ligne. Pourquoi alors ne pouvons-nous pas voter en ligne? Cela semble pourtant une façon toute naturelle d'utiliser la technologie. Les avantages perçus du vote par Internet sont généralement axés sur des objectifs autrement raisonnables, notamment faire augmenter le taux de participation au scrutin, joindre les populations sous-représentées, améliorer l'accessibilité et réduire les coûts des élections. Cependant, l'une des raisons principales pour lesquelles nous ne votons pas déjà en ligne est que le vote par Internet est simplement un problème de sécurité vraiment difficile que nous n'avons pas réussi à régler.

Pour résumer un problème très complexe, disons que la raison pour laquelle le vote par Internet est plus difficile qu'au moyen d'autres systèmes de cybersécurité s'explique par la tension fondamentale qui existe entre les objectifs en matière de sécurité du secret du vote et l'intégrité des élections. Si nous éliminions simplement le secret du vote, le problème de sécurité du vote par Internet deviendrait beaucoup plus facile à régler, et la situation ressemblerait à celle des autres systèmes de sécurité, comme dans le cas des transactions bancaires en ligne.

Le défi technique du vote électronique découle de la nécessité d'assurer la sécurité et le secret en même temps. Comment peut-on prouver que mon vote a vraiment compté alors qu'on ne le connaît même pas? C'est une situation à laquelle on peut faire face de manière assez fiable avec le scrutin secret et le vote en personne grâce à une combinaison de mesures de sécurité matérielle et administrative ainsi qu'à la nature immédiatement observable du monde réel. Cependant, il n'y a aucun analogue logiciel direct à la garantie matérielle que les bulletins de vote en papier qui se retrouvent dans une boîte vide seront les mêmes que ce qui en ressortira à la fin de la journée.

II. Vue d'ensemble des menaces

Dans leur forme la plus fondamentale, les systèmes commerciaux contemporains de vote par Internet désignent un cadre d'application Web standard; un programme de votation (généralement JavaScript) est envoyé par Internet à votre navigateur à partir du serveur des élections. Lorsque vous déposez votre bulletin de vote, l'information au sujet de vos choix sera retournée au serveur et stockée dans une base dont les données seront calculées plus tard. La

sécurité s'impose à tous les échelons de cette chaîne, à savoir dans votre ordinateur, tout au long de l'envoi et dans le serveur des élections.

Dans une optique de sécurité, cette architecture présente de nombreuses menaces potentielles qu'on ne retrouve pas dans la méthode actuelle de dépouillement des votes à la main du Canada.

Vente de vote et coercition. Vu l'absence de supervision inhérente au vote par Internet, quiconque peut observer un électeur en train d'exprimer sa voix et être alors indûment influencé dans son intention de vote.

Hameçonnage. Il existe de nombreuses voies électroniques par lesquelles des électeurs pourraient se retrouver malgré eux dans des sites Web trompeurs ou malveillants, ou bien à des adresses URL légitimes qui leur fourniraient, par exemple, des données utiles sur le scriptage entre sites.

Partialité de l'automatisation. L'accoutumance et le manque de compréhension à l'égard des buts et de l'objet des technologies courantes de sécurité sur le Web peuvent inciter les utilisateurs à se fier outre mesure aux mesures de protection technologiques et à sous-estimer l'importance des avertissements ou des erreurs. Citons notamment les cas où des personnes ne remarquent pas l'absence de l'icône du cadenas vert ou cliquent sur des avis de sécurité dans le navigateur. Ajoutons le fait que de nombreux sites Web (par exemple https://elections.on.ca) génèrent des erreurs en raison d'une simple mauvaise configuration.

Déni de service. La nature peu centralisée d'Internet fait en sorte qu'il est possible qu'un serveur soit inondé de demandes de connexion de la part de nombreux systèmes répartis. Bien qu'il existe des mesures d'atténuation technologiques pour les attaques de ce genre, elles entraînent parfois des interruptions importantes. À titre d'exemple, une attaque par déni de service qui s'est produite en 2015 a rendu les sites Web du gouvernement du Canada inaccessibles pendant plusieurs heures.

Logiciels malveillants ou espions chez le client. En raison de notre mode de vie branché, l'appareil informatique dont nous nous servirions pour déposer un bulletin de vote serait susceptible d'avoir été utilisé antérieurement dans bien d'autres contextes. Par conséquent, il existe de nombreuses possibilités d'injecter un logiciel malveillant dans l'ordinateur d'un électeur dans le but de modifier ou de surveiller ses choix sur le bulletin de vote. N'importe quel système acceptable de vote par Internet doit être solide, même en présence d'un logiciel malveillant.

Attaques contre un réseau informatique. Il existe de nombreuses possibilités pour un pirate informatique qui se trouve entre l'emplacement réseau d'un électeur et le serveur des élections de tenter de voir les résultats du scrutin ou de les modifier. Une mesure fondamentale et nécessaire de protection et de sécurité se traduit par le recours au protocole de sécurité de la couche transport (TLS), qui est couramment désigné dans votre navigateur par un cadenas vert. Les erreurs commises par l'utilisateur, la mauvaise configuration du serveur et les nouvelles attaques cryptographiques peuvent toutes être exploitées dans le cadre d'une attaque d'interception visant à accéder aux préférences de l'électeur ou à les modifier. Même s'il s'agit d'une technologie de sécurité Internet de base, nous avons constaté que sur les 14 sites Web d'organismes responsables de l'administration électorale à l'échelle fédérale, provinciale et territoriale, un seul, soit celui d'Elections Nova Scotia, prenait en charge le protocole TLS. De plus, nous avons détecté des cas de mauvaise configuration du protocole TLS dans les sites Web d'Élections Ontario et d'Elections PEI (voir le tableau 1).

Organisme	Prise en charge du protocole TLS	Emplacement du serveur[1]
Élections Canada	Non	Canada
Elections Alberta	Non	États-Unis
Elections BC	Non	Canada
Élections Manitoba	Non	Canada
Élections Nouveau-Brunswick	Non	Canada
Elections Newfoundland and Labrador	Non	Canada
Élections Territoires du Nord-Ouest	Non	Canada
Elections Nova Scotia	Oui	Canada
Élections Nunavut	Non	Inconnu
Élections Ontario	Mal configuré	États-Unis
Elections PEI	Mal configuré	Canada
Élections Québec	Non	Canada
Elections Saskatchewan	Non	États-Unis
Élections Yukon	Non	Canada

Tableau 1. Prise en charge actuelle du protocole TLS dans les sites Web des organismes canadiens responsables de l'administration électorale

Pénétration de serveur. Aujourd'hui, une élection fédérale canadienne se traduit sur le plan technique par la tenue de 338 élections distinctes dans des milliers de bureaux de vote différents à l'échelle du pays. Un système Internet regroupe les renseignements sur toutes ces élections dans un seul serveur Internet, auquel il est possible d'accéder au moyen de n'importe quel ordinateur sur la planète. Cependant, toute combinaison de vulnérabilités logicielles non divulguées, de mauvaises configurations ou d'erreurs humaines pourrait permettre à un pirate à distance d'avoir accès à l'information sur l'inscription électorale ou aux données des bulletins de vote. Les cas de pénétration de serveur (p. ex. logiciel rançonneur, clichage de courriels et de mots de passe, et vol de la propriété intellectuelle) sont de plus en plus courants, et il est possible d'en trouver des exemples dans tous les secteurs organisationnels.

[1] Selon le consensus sur iplocation.net.

Influence de l'intérieur. Il y a un risque que des personnes de l'intérieur (p. ex. personnel électoral, fournisseurs et techniciens) aperçoivent ou modifient les choix faits sur le bulletin de vote dans le serveur; c'est pourquoi il est primordial de mettre en place des mécanismes solides en vue de prévenir les changements de vote non détectés.

Intervenants de l'État. La menace la plus importante pour une élection sur Internet est sans doute une attaque sophistiquée de la part d'un intervenant de l'État qui changerait le résultat d'une élection sans qu'on le détecte. Des exemples d'interventions potentielles de l'État de ce genre dans le cadre d'élections se sont produits aux États-Unis au chapitre des données du registre des électeurs. Dans le pire des scénarios, les troubles politiques subséquents à une élection frauduleuse pourraient provoquer un effondrement économique ou, pire encore, une guerre. De plus, on ne sait pas avec précision si une attaque sophistiquée serait même détectée un jour. Dans cette optique, un système de vote par Internet à l'échelle fédérale, quel qu'il soit, est une infrastructure essentielle, et sa protection pourrait raisonnablement être considérée comme une question de sécurité nationale.

III. RECOMMANDATIONS

A. Vérifiabilité de bout en bout

Des recherches menées récemment sur la mise en place de systèmes de vote par Internet ont démontré une faible sécurité administrative (Springall et coll., 2014; et Wolchok et coll., 2010) ainsi qu'une mise en œuvre de services de sécurité et des configurations de sécurité faibles, vulnérables ou ponctuelles (Wolchok et coll., 2012; Clark et Essex, 2014; et Teague et Halderman, 2015). Une approche prometteuse est le vote par Internet cryptographique et vérifiable de bout en bout, qui permet aux électeurs de créer un reçu de leur vote qui protégera leur vie privée et qui pourra plus tard être utilisé dans le cadre d'une preuve de correction cryptographique publique et universellement vérifiable. Deux projets d'envergure ont été

réalisés, à savoir les suivants : « Helios » (Adida, 2008) et « Scantegrity/Remotegrity » (Carback et coll., 2010; et Zagorski et coll., 2013). Ce dernier projet a été déployé dans le cadre de la première élection gouvernementale vérifiable de bout en bout qui s'est tenue dans la ville de Takoma Park, dans le Maryland, en 2009 et en 2011.

Un rapport récent de la U.S. Vote Foundation (Dzieduszycka-Suinat et coll., 2015) a même affirmé que *toutes* les élections sur Internet devraient être cryptographiques et vérifiables de bout en bout. La vaste utilisation de la cryptographie fait toutefois en sorte qu'il reste encore de nombreux défis de recherche à relever pour que ce projet soit pratique sur le plan des exigences fonctionnelles (convivialité, accessibilité, etc.) et conceptuelles (compréhensibilité, vérifiabilité, etc.). Étant donné ces risques et les moyens éventuels d'élaboration de mesures d'atténuation, nous recommandons que le Comité spécial sur la réforme électorale n'aille *pas* de l'avant avec le vote par Internet en ce moment, qu'il accorde plutôt la priorité à la recherche sur les technologies de vérification du vote par Internet et qu'il fasse la promotion de possibilités interdisciplinaires de collaboration sur le plan de la recherche afin d'étudier les enjeux à la jonction des élections et de la cybersécurité.

B. Cadre national de vote par Internet

Avant que le Canada puisse procéder au vote par Internet, il serait primordial d'établir un cadre national qui énoncerait les normes de sécurité, les exigences logicielles, les méthodes d'essai, la surveillance gouvernementale et la responsabilité légale.

En ce qui concerne les essais et la surveillance gouvernementale, un comité consultatif de l'État de l'Utah (Cox et coll., 2015) a récemment recommandé que tout système candidat soit mis à la disposition du public dans une tribune ouverte où ce dernier serait invité à effectuer un essai de pénétration au moyen d'un ensemble d'élections simulées sur Internet. Comme l'ont démontré Wolchok et coll. (2012), il peut s'agir d'une façon efficace de détecter des vulnérabilités cruciales dans le cadre d'un scénario électoral simulé, mais réaliste.

En ce qui a trait aux normes et aux exigences, le gouvernement n'a pas forcément l'expertise nécessaire à l'interne pour évaluer et vérifier adéquatement les systèmes de vote par Internet. Dans la même veine que les recommandations du comité consultatif sur le vote par Internet de l'Assemblée législative de la Colombie-Britannique (comité indépendant, 2014), nous recommandons la création d'un comité technique indépendant qui serait composé d'administrateurs de scrutin et de spécialistes en sécurité du vote par Internet. Ce comité serait chargé d'évaluer rigoureusement la sécurité des systèmes de candidats.

Conclusion. Le Comité spécial sur la réforme électorale doit savoir qu'il existe une préoccupation de premier plan au sujet de la sécurité du vote par Internet chez les spécialistes internationaux en technologie et en cybersécurité. Nous faisons écho à une déclaration faite par d'éminents techniciens spécialistes en informatique des États-Unis (Computer Technologists) et nous recommandons l'adoption du vote par Internet seulement une fois que les nombreuses menaces techniques énoncées ci-dessus pourront être atténuées convenablement, ainsi que la mise en place de mécanismes solides de prévention des changements non détectés. Le système au complet doit être fiable et vérifiable de façon à convaincre les électeurs.

RÉFÉRENCES

[1] Adida, B. *Helios: web-based open-audit voting*, « USENIX Security Symposium », 2008, p. 335–348.

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

[3] Clark, J. et A. Essex. *Security Assessment of Vendor Proposals*, rapport final Report, Toronto, DP n° 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] Cox, S.J., A. Lawrence, C. Bramble, R. Chavez-Houck, R. Cowley et autres. *iVote Advisory Committee Final Report for the State Utah*, 2015, https://elections.utah.gov/Media/Default/Documents/Report/iVote%20Report%20Final.pdf.

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

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

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

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

[11] Wolchok, S., E. Wustrow, D. Isabel et J.A. Halderman. *Financial Cryptography*, chapitre « Attacking the Washington, D.C. Internet Voting System », 2012, p. 114–128.

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