Commentaire sur le vote par internet

Marc-André Miron

Université de Montréal - Novembre 2019

Ce document se veut un court commentaire sur une part du risque encouru des élections par internet. Celui-ci ne discute pas de toutes les propriétés du vote par internet ni même de l'entièreté des risques possibles, mais d'un seul aspect particulier.

Sur son site dédié à la consultation sur le vote par internet, Élection Québec note les principaux avantages et inconvénients les plus fréquemment mentionnés dans la documentation sur le sujet [8]. Si Élection Québec remarque à juste titre le « Risque qu'un vote ou que les résultats de l'élection soient modifiés par un acte malveillant », il faut ajouter que cela ne souligne pas la différence principale en ce qui a trait aux risques encourus par des élections par internet par rapport aux élections par papier. Dans les deux cas, en permettant une forme de vote à distance, on tolère un certain risque. Cependant, comme le remarquent Barbara Simons et Douglas W. Jones , dans le cas du vote par internet, on permet des attaques massives sur un grand nombre d'électeurs à partir de n'importe où dans le monde, alors que le vote postal contraint les fraudeurs à une action physique sur place et sur une quantité limitée de bulletins de vote [9].

Plusieurs possibilités sont ouvertes à un adversaire : s'attaquer aux serveurs d'Élection Québec ou aux clients utilisés par les électeurs ainsi qu'en ciblant les communications entre les deux par une attaque de l'homme du milieu (man-in-the-middle).

En ce qui a trait aux attaques de clients, la solution la plus simple pour l'adversaire est la location de réseaux de machines préinfectées, ou la création

d'un tel réseau grâce à l'utilisation de vulnérabilités. On doit d'abord savoir à ce sujet qu'un vif marché existe où se monnaient des chaînes de vulnérabilités inconnues, dites « zero-day », n'ayant fait l'objet d'aucune publication ou de correctif [3, 7]. Hormis les marchés noirs qui proposent de tels services, citons que des compagnies agissant dans des zones grises de légalité achètent et revendent des exploits complets aux plus offrants, par exemple Zerodium [1]. Les exploits les plus sérieux permettent des infections sans intervention de la part de l'utilisateur (vulnérabilités « zéro-clic ») et peuvent être acquis pour 2 M $ US pour des appareils iOS ou 1 M $ US pour Windows, à tout exemple. Notons qu'à ce point, rien ne peut garantir à l'utilisateur d'un appareil électronique que ce qu'il voit est bien authentique lorsque l'appareil est compromis, empêchant par conséquent de bien savoir si ou pour qui cette personne a voté.

Il ne s'agit donc pas d'être à risque de voir un adversaire trouver un tel exploit mais bien qu'un tel tiers parti existe et soit intéressé à financer l'élaboration d'une telle attaque. Vu ce contexte, il est difficile d'envisager qu'un critère de risque acceptable puisse essentiellement reposer sur la simple volonté ainsi qu'un budget minimal de la part d'un adversaire éventuel.

À la vue du contexte très différent dans lequel évolue le vote par internet qu'une élection par papier, il convient de rechercher des garanties fortes permettant de vérifier après coup la justesse de l'élection ou si des adversaires sont intervenus entre-temps puisque, comme nous l'avons vu, il leur est plus facile d'agir sur les votes et à plus grande échelle. Depuis des années, des chercheurs et chercheuses à la recherche d'une solution ont élaboré des protocoles électoraux vérifiables de bout-en-bout avec trace papier (« end-to-end auditable voting system », voir [5]). Cette solution comporte néanmoins des limitations importantes, notamment du fait qu'elle n'empêche pas nécessairement que les votes soient dévoilés et de grandes précautions doivent être prises lors de son élaboration, pour éviter par exemple qu'un groupe malhonnête puisse prétendre à des résultats faux sans que ce soit le cas [4]. De même, la vérification des élections par internet de bout en bout n'empêche pas que les élections soient facilement perturbées ou annulées par un adversaire.

Les expériences récentes de vote par internet se sont avérés des désastres à plusieurs égards : codes source fermés, utilisations de logiciels propriétaires, démonstrations de vulnérabilités pour des systèmes réellement utilisés (Mos-

cou, Australie) ou en test (Suisse, Washington D.C. [9]) alors qu'en parallèle, des attaques à grande échelle contre des systèmes électoraux ont été dévoilées pour l'entièreté des états américains aux dernières élections [6]. Remarquons que lors des tests de Washington D.C., les chercheurs ayant piraté le système informatique de l'autorité électorale ont pu constater les tentatives de deux groupes iraniens et chinois de pénétrer également dans le réseau. Il s'avère aussi que, malgré ces menaces, beaucoup d'états et de pays se sont montrés réticents à dévoiler leurs protocoles de vote internet en code source ouvert, ce qui ne les rend pas plus sécuritaires et rend impossible la vérification du code par les citoyens et experts (c'est une méthode largement rejetée par les experts de sécurité depuis longtemps [2]), sans compter qu'aucun de ces systèmes de vote à distance n'ait conservé l'utilisation du vote de bout en bout.

Entre ces dangers connus du vote par internet et la robustesse du vote par papier avec audit manuel, j'aimerais suggérer d'abord la prise en compte d'avis d'experts en sécurité avant tout, puisqu'un système électoral vulnérable aux intérêts étrangers à la population rend inutile toute autre considération. J'aimerais également suggérer que si le vote par internet devait être retenu (ce que je ne propose pas), que des critères rigoureux soient retenus pour la sélection du protocole dont la vérifiabilité universelle de bout-en-bout et la confidentialité du vote, que l'entièreté du protocole proposé et de sa mise en oeuvre soit disponible en code source ouvert et que des tests publics soient mis en place et répétés jusqu'à nécessité. Malgré tout, si nous devions passer par toutes ces étapes, des acteurs avec des moyens suffisants seraient en bonne route pour perturber plus facilement nos élections, à distance et à grande échelle. Le jeu en vaudrait-il la chandelle ?

Références

[1] Zerodium. URL : https ://zerodium.com/program.html.

[2] Security through obscurity, Sep 2019. URL : https ://en.wikipedia.org/wiki/Security$_t hrough_o bscurity$.

[3] Sebastian Anthony. The first rule of zero-days is no one talks about zero-days, Oct 2015. URL : https ://arstechnica.com/information-technology/2015/10/the-rise-of-the-zero-day-market/.

[4] Chris Culnane, Aleksander Essex, Sarah Jamie Lewis, Olivier Pereira, and Vanessa Teague. Knights and knaves run elections : Internet voting and undetectable electoral fraud. *IEEE Security & Privacy*, 17(4) :62–70, 2019.

[5] Susan Dzieduszycka-Suinat, Ir. M. Menco B. Ph., Joseph Kiniry, Daniel M. Zimmerman, Daniel Wagner, Philip Robinson, and Ádám. The future of voting end-to-end verifiable internet voting specification and feasibility assessment study internet voting today no guarantees end-to-end verifiability e2e-viv. 2015.

[6] Sean Gallagher. Dhs, fbi say election systems in all 50 states were targeted in 2016, Apr 2019. URL : https ://arstechnica.com/information-technology/2019/04/dhs-fbi-say-election-systems-in-50-states-were-targeted-in-2016/.

[7] Andy Greenberg. Shopping for zero-days : A price list for hackers' secret software exploits, Nov 2012. URL : https ://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/7e80b3b12660.

[8] Élections Québec. Vote par internet. URL : https ://www.electionsquebec.qc.ca/voteparinternet/.

[9] Barbara Simons and Douglas W Jones. Internet voting in the us. *Communications of the ACM*, 55(10) :68–77, 2012.