Grand Est

Vulnérabilité du vote électronique à distance : des solutions made in Lorraine

Deux chercheurs lorrains ont découvert des failles et des vulnérabilités dans le vote électronique à distance des Français de l'étranger à l'occasion des législatives 2022. Ils ont proposé des solutions pour y remédier.

Lucca Hirschi et Alexandre Debant, chercheurs de l'Institut national de recherche en sciences et technologies du numérique au Laboratoire lorrain de recherche en informatique et ses applications. Photo Patrice Saucourt

Le vote électronique à distance lors d'élections politiques agite la société depuis des années. Les pour, les contre, les méfiants… En 2022, lors des élections législatives, les Français résidant à l'étranger ont eu la possibilité d'utiliser ce moyen pour choisir leur député. L'occasion pour Alexandre Debant et Lucca Hirschi, chercheurs de l'Institut national de recherche en sciences et technologies du numérique au Laboratoire lorrain de recherche en informatique et ses applications à l'Université de Lorraine de procéder à des tests pour savoir si le vote, par ce système, garantissait le secret et l'intégrité des résultats conformément à la loi.

Ce sont « nos collègues, Véronique Cortier, Pierrick Gaudry et Stéphane Glondu (NDLR : qui développe la plate-forme de vote Belenios) qui ont été mandatés pour la mise en place d'un outil « tiers de confiance » », confient-ils. Quelques semaines avant le début des votes, « une description partielle du protocole a été publiée. On est curieux, on est allé voir ! » Les deux chercheurs s'en sont donc saisis « pour comprendre comment ça fonctionnait ».

Attaque sans laisser de traces

Alexandre Debant et Lucca Hirschi ont travaillé pour tester leurs hypothèses. Là, ils ont constaté des failles et des vulnérabilités dans le système de vote.

D'abord, « personne ne doit savoir pour qui j'ai voté », c'est le secret du vote. En ce cas, le chiffrement se fait via une clef « donnée à plusieurs personnes qui ont des bouts de cette clef », soulignent-ils. « Il y a onze élections dans onze circonscriptions. Un attaquant pourrait mettre, par exemple, un bulletin prévu pour Sidney à Minsk ou dans une circonscription consulaire où il y a très peu de votants. Il va savoir, avec une bonne probabilité, pour qui j'ai voté ».

Bien sûr, ces attaques ne pourraient émaner de néophyte en la matière, « ce n'est pas donné à tout le monde, mais ça ne demande pas un très haut niveau de technicité ». De plus, « si un attaquant existe, il attaque sans laisser de traces ». D'ailleurs, ils ne peuvent pas dire, si ces élections de 2022 ont subi ou non des attaques qui auraient exploité ces failles de sécurité.

« Le gros du danger est inexistant en 2023 »

Quant à la vérifiabilité du vote, il s'agit de savoir s'il n'y a pas eu de « modification du bulletin car, une fois que j'ai cliqué sur « voter », je ne sais plus ce qui se passe ». Un reçu Pdf est envoyé au votant avec « un code de associé à mon intention de vote. À la fin de l'élection, je peux me connecter sur le site » pour vérifier que le bon bulletin est dans la bonne urne. « On a analysé le pdf » et les chercheurs se sont aperçus que le vote pouvait être modifié mais que le reçu envoyé au votant portait bien les bonnes informations. Un problème dû « à un bug ».

En tout, deux failles majeures… qui ont été réparées. En effet, les chercheurs, qui ont signalé ces failles et ont participé à deux réunions « avec le ministère des Affaires Étrangères, l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et le prestataire » chargé de mettre en place le système de vote. En 2023, des législatives partielles ont été organisées pour les Français de l'étranger dans les circonscriptions où le scrutin avait été annulé par le Conseil constitutionnel. Différentes options avaient été proposées par Alexandre Debant et Lucca Hirschi qui sont retournés voir… Les failles avaient été réparées : « Ils ont choisi des options raisonnables. Le gros du danger était inexistant en 2023 ».

● **Frédéric Plancard**

« Il faut penser comme un attaquant ! »

Bien sûr, la sécurisation des votes électroniques « peut toujours être améliorée », expliquent Alexandre Debant et Lucca Hirschi. Par exemple, en faisant qu'un vote électronique soit conforme pour la confidentialité et l'intégrité du résultat, même si la machine du votant est corrompue. Il faut quand même que l'expérience utilisateur soit satisfaisante, que le « système soit utilisable par tous et qu'il ne soit pas trop long et trop compliqué ».

On le voit, « le problème du vote électronique est complexe et il n'y a pas de solutions satisfaisantes », poursuivent-ils. Pour le vote électronique, « détecter une fraude est plus difficile que pour une banque en ligne » et le risque « est souvent mal perçu ». Pour tester ces systèmes, « il faut penser comme un attaquant ! », poursuivent-ils.

Rappelons qu'en France, le vote électronique à distance est interdit pour les votes politiques quand le corps électoral inclut la métropole.

Et le vote pour les primaires ?

Concernant le vote sur des machines à vote, « le reçu est imprimé sur la machine et c'est la même problématique qui se pose ». Les machines à voter sont en outre, placées sous moratoire depuis 2008 ce qui altère d'autant plus la sécurisation.

Pour les chercheurs, le problème du vote électronique est complexe et il n'y a pas de solutions satisfaisantes. Photo d'archives Lionel Vadam

« Un autre enjeu, ce sont les primaires », confient les deux chercheurs. Ce vote est utilisé par les partis politiques pour désigner, par exemple, un candidat à la présidentielle. « C'est une zone grise », évoquent Alexandre Debant et Lucca Hirschi. Il a déjà été constaté qu'il y a eu « des systèmes qui étaient des passoires ».

Les deux chercheurs qui travaillent sur la conception et la vérification de protocoles cryptographiques, le vote électronique en étant un, ont présenté leurs travaux dans ce domaine dans de prestigieuses manifestations. Cet été, c'est au colloque Usenix Security de Los Angeles que leurs résultats ont été évoqués. En mars, c'était au Real world crypto symposium de Tokyo.

● **F.P.**