MELEPE

Geste de savoir

Vote électronique ou vote papier : seulement la confiance ?

31 mai 2022

Table des matières

Introduction 1
1. Le vote, c'est quoi? 1
2. Le vote électronique, pourquoi? 2
3. Le vote électronique, comment? 2
Conclusion 5

Introduction

Suite à la tribune de @Gawaboumga, je réagis et plutôt que de pondre un roman en commentaires, je préfère organiser ma réponse dans ce billet.

Tout d'abord, je suis globalement d'accord avec sa conclusion: la confiance des gens dans un tel système est un frein réel à l'adoption. Cependant, je dirais que l'aspect technologique reste également un frein majeur pour l'adoption d'une telle solution et que ces deux inconvénients semblent indissociables du vote en ligne, qui donc selon moi est éternellement condamné au rang de fausse bonne idée.

Je développe ma pensée plus avant dans ce billet.

1. Le vote, c'est quoi ?

Un système de vote est généralement muni des propriétés suivantes:

- **éligibilité, justice** : ne peuvent voter que les électeurs inscrits, chaque vote a un poids égal
- **confidentialité du vote**: personne d'autre que moi ne sait pour qui j'ai voté
- **pas de coupon de reçu (receipt freeness)** : je ne peux pas prouver à quelqu'un pour qui j'ai voté
- **résistance à la coercion** : on ne peut pas me forcer à voter pour quelqu'un
- **vérifiabilité individuelle** : je peux vérifier que mon vote a été pris en compte
- **vérifiabilité collective** : je peux vérifier que tous les votes ont été pris en compte
- etc.

Le vote papier en France garantit plus ou moins ces propriétés, à l'exception notable de la procuration qui peut être forcée[1]. Les résultats peuvent être estimés en une heure, mais les chiffres définitifs prennent quelques jours, ce qui est le principal inconvénient (en plus de devoir se déplacer).

2. Le vote électronique, pourquoi ?

On donne, en général, 3 grands avantages au vote électronique:

— Facilité d'utilisation, qui pourrait mener à une participation accrue
— Rapidité du dépouillement
— Fiabilité du décompte

Sur le papier (huhu), ça semble bien. Le problème, c'est tout ce qui vient ensuite.

3. Le vote électronique, comment ?

Il existe pléthore de systèmes de vote électronique et en ligne, des conférences de cryptographie y sont intégralement dédiées. Je ne vais donc pas en faire la liste, ce n'est pas très intéressant.

Un point essentiel est que si le protocole en question diffère d'un simple +1 dans une base de données (ce qui est le fonctionnement des machines de vote les plus simples), alors de la cryptographie est utilisée.

Il "suffit" ensuite d'implémenter ces protocoles cryptographiques sur vos machines, d'auditer le code et de s'assurer qu'il n'y a pas d'erreur, pour ensuite avoir une solution de vote électronique. Simple, non?

Première étape : la cryptographie

Quand on regarde en détails les articles de vote cryptographique, on se rend compte de plusieurs choses:

— La sécurité prouvable, c'est quelque chose d'extrêmement difficile à obtenir, et beaucoup de chercheurs s'y sont mordu les doigts .
— Certains articles reposent sur des hypothèses exotiques voire jamais étudiées, qui peuvent être cassées par la suite. C'est notamment le cas des signatures aveugles de Schnorr, dont l'hypothèse de difficulté au doux nom de "Random inhomogeneities in a Overdetermined Solvable system of linear equations" a été cassée en 2020 .

Alors, vous me direz, ce que je dis est vrai pour absolument toute la cryptographie utilisée de nos jours, et ça ne nous empêche pas de faire des achats en ligne. C'est vrai, mais j'y reviendrai. Pour l'instant, supposons que notre crypto est sécurisée, et passons à l'étape suivante.

Seconde étape : l'implémentation

Nous passons maintenant à la seconde étape, celle de l'implémentation. Et bien sûr, un programme sans bug, c'est un peu comme le dahut, personne n'en a vu à part peut-être le cousin de la voisine d'un ami, une fois, enfin il paraît.

À l'heure actuelle la quasi-totalité des implémentations de vote en ligne comportent ou ont comporté des bugs sévères ou critiques: Russie 2020 , Estonie 2021 , 2014 , Suisse 2019 , Australie 2015 ...

De plus, implémenter un protocole cryptographique est notoirement difficile et complexe. Non seulement un simple bug peut ruiner toute la sécurité, mais en plus, il faut rester à la pointe de l'actualité. Par exemple, vous souhaitez implémenter quelque chose reposant sur le logarithme discret, vous suivez les recommandations de l'ANSSI de 2014 , et vous utilisez le corps $GF(2^n)$ parce qu'il est bien pratique à implémenter. Vous n'avez cependant pas bien lu les recommandations (comme moi au moment d'écrire cet article), et ne vous rendez pas compte que l'ANSSI ne préconise l'emploi de $GF(2^n)$ que pour un logarithme discret à base de courbes elliptiques définies sur ce corps, et pas directement sur ledit corps. C'est dommage, parce que dans ce corps, le logarithme discret est cassé depuis 2013 .

Tout cela est encore bien abstrait, alors donnons un exemple simple, qui en plus ne repose pas sur de la cryptographie. En 2016, à la conférence Black Hat, des chercheurs ont montré (avec une vraie machine de vote officielle) comment voter plusieurs fois . L'attaque nécessitait environ 20$ de matériel et prenait quelques secondes.

Mais bon, après tout, on est bien arrivés à envoyer des fusées dans l'espace, donc on devrait bien arriver à correctement implémenter un +1 dans une base de données un jour ou l'autre. Alors continuons.

Troisième étape : la sécurisation

C'est ici qu'arrive le cauchemar. Le monde de la cybersécurité est une jungle, où il n'existe qu'une seule certitude: tout le monde cherche à vous attaquer.

Les organisations de vote sont régulièrement la cible d'attaques . Pour autant que je sache, il n'existe pas de preuve directe d'une altération d'une élection suite à un piratage. Cependant, il reste compliqué d'expliquer la présence du fichier `-.mp3` sur certaines machines de vote de Virginie .

Les machines de vote ne sont pas les seules cibles, en particulier pour un vote en ligne où n'importe qui peut voter depuis n'importe quel appareil. Si votre ordinateur est vérolé (et vous savez comme moi que l'ordinateur de votre tonton contient plus de virus qu'une réunion d'antivax lors d'un pic de contamination Covid), il n'y a aucune garantie que vous votiez réellement pour qui vous pensez voter. C'est notamment une des mises en garde du Loria sur le vote des législatives 2022 .

Ainsi, un système de vote doit faire face à des attaquants étatiques, qui n'hésiteront pas à allègrement hacker toutes vos plateformes ou celles de vos citoyens s'ils y trouvent un intérêt. Le retour sur investissement est rapide. Coût d'une 0-day: quelques dizaines de milliers de dollars, monter une attaque: quelques dizaines/centaines de millions, faire tomber une démocratie ennemie: priceless.

Selon moi, c'est le désavantage majeur du vote en ligne par rapport au vote papier. Pour un vote papier, le périmètre de sécurité à défendre est assez petit: quelques dizaines de milliers de bureaux de vote (environ 70 000 en France), que l'on peut sécuriser avec une ou deux caméras et quelques assesseurs. Pour le vote en ligne, le périmètre s'étend au monde entier, vu qu'un hacker peut sévir depuis littéralement n'importe où, et à l'intégralité des protocoles internet.

Si nous revenons aux faiblesses cryptographiques, c'est la raison pour laquelle votre transaction en ligne court moins de risques qu'une élection: tout simplement parce qu'il est plus intéressant de hacker une élection que votre compte en banque. De plus, une transaction frauduleuse peut

être annulée par la banque, tandis que pour une élection, le gouvernement est à la fois juge et partie, c'est plus compliqué. De même, pour les fusées, un bug est moins critique car moins de gens vont chercher à l'exploiter (exception faite des satellites), et tant que la fusée arrive à destination, ce n'est pas très gênant. Alors que pour une élection, toute modification du scrutin est susceptible d'annuler la procédure.

À noter qu'en 2020, les autorités américaines reconnaissaient le vote en ligne comme à haut risque , et en 2018 l'académie des sciences américaine disait même que "aucune technologie connue ne permet la confidentialité, la sécurité, et la vérifiabilité d'un bulletin transmis par internet" . Ce qui nous mène au dernier point.

Quatrième étape : la confiance dans le système

Pour qu'un système soit bénéfique, il faut que les gens y fassent confiance. Et… c'est loin d'être gagné pour le vote en ligne.

Vous vous souvenez quand je disais que des faiblesses cryptographiques ou d'implémentation, ce n'était pas gênant quand on s'en servait quand même pour acheter en ligne? Eh bien le pour le vote en ligne, c'est une autre paire de manches. Pour un utilisateur lambda, **tout**, dans un vote en ligne, est obscur et difficile à faire confiance. D'autant que les complots cryptographiques, ça existe .

Tous ces points d'ombre sont autant de sources de défiance possible. Et quand on n'est pas content du résultats, ces points d'ombre peuvent servir de bouc émissaire bien pratique, qu'on ait des preuves ou non. Il n'y a qu'à voir les accusations de Fox News sur les machines de vote lors de l'élection américaine de 2020 pour s'en convaincre.

D'autant qu'un second point vient en la défaveur des votes en ligne: souvent, de tels protocoles reposent sur le fait que les votes (chiffrés) sont à disposition du public. Or, la cryptographie ne garantit pas une confidentialité perpétuelle, les clefs RSA de 1990 sont cassées en quelques heures sur un ordinateur moderne. Il en sera sûrement de même dans 30 ans pour les clefs privées actuelles, en particulier si l'ordinateur quantique fait son apparition. Ainsi, un protocole de vote en ligne doit prévoir que les clefs privées seront cassées dans un futur plus ou moins lointain, ce qui est… compliqué.

Le point bonus

On vient de voir que la fiabilité du décompte n'est pas assurée par le vote électronique, du fait de toutes les attaques possibles. En ce qui concerne la participation, si l'on observe effectivement un gain de participation sur les voteurs occasionnels, on n'observe pas de gain significatif sur la population entière . Autrement dit, beaucoup de troubles pour pas grand-chose.

D'autres arguments, déjà mentionnés dans les commentaires du billet originel, entrent aussi en compte comme la quasi impossibilité de résister à la coercion sur un vote en ligne (j'ai lu des protocoles qui tentaient de s'en affranchir mais ce n'est pas la majorité).

1. Petit jeu: trouvez une méthode permettant à un électeur français de prouver, en sortie du bureau de vote, pour qui il a voté, sans même utiliser de caméra.

Conclusion

Des trois arguments en faveur du vote électronique, seul un seul subsiste réellement: celui de la rapidité du décompte. Mais la lenteur de notre système est-elle réellement un problème insupportable? Par ailleurs, le vote papier possède un avantage incontestable: il est quasi impossible d'y faire germer de théorie du complot sans arguments un minimum fondés du fait de l'absence de boîte noire (ce n'est pas pour rien que les urnes sont transparentes), ce qui est non négligeable en ces temps de désinformation.

À titre personnel, je trouve que le vote en ligne est une solution à un problème qui n'existe pas, et qui de plus amène avec lui toute une série de complications bien plus dramatiques que les problèmes qu'il prétend résoudre.