Algorithmes et systèmes de vote électronique : vices et vertus.

Thomas Abecassis

Résumé 1

Abstract 1

Introduction 1

Les exigences du vote 2

Deux systèmes de vote électroniques différents 2

Signature aveugle 3

Mix network 3

Les problèmes du vote électronique 4

Pour les urnes électroniques : 4

Pour le vote via internet : 5

Sources 6

Résumé

Les algorithmes et les systèmes de vote électronique peuvent offrir de nombreux avantages, tels qu'une plus grande efficacité, une meilleure accessibilité et une plus grande transparence dans le processus de vote. Cependant, ils peuvent également présenter des risques pour la sécurité et la fiabilité des élections.

Un des principaux problèmes liés aux systèmes de vote électronique est la vulnérabilité aux piratages informatiques. Si un système de vote est piraté, il peut être manipulé de manière à changer les résultats des élections. Les algorithmes de vote peuvent également être biaisés, ce qui peut conduire à des résultats injustes.

Il est important de mettre en place des mesures de sécurité robustes pour protéger contre les piratages et de s'assurer que les algorithmes de vote sont justes et équitables. Il est également important de veiller à ce que les citoyens aient confiance dans les systèmes de vote électronique et qu'ils aient la possibilité de vérifier que leurs votes ont été correctement enregistrés et comptabilisés.

Mots-clés :

Vote électronique / Systèmes de vote / Urne électronique / Vote par Internet / Anonymat / Confiance / mix networks / Signature aveugle

Abstract

Electronic voting algorithms and systems can offer many benefits, such as greater efficiency, accessibility and transparency in the voting process. However, they can also pose risks to the security and reliability of elections.

One of the main problems with electronic voting systems is the vulnerability to hacking. If a voting system is hacked, it can be manipulated to change the outcome of the election. Voting algorithms can also be biased, which can lead to unfair results.

It is important to have robust security measures in place to protect against hacks and to ensure that voting algorithms are fair and equitable. It is also important to ensure that citizens have confidence in electronic voting systems and that they have the ability to verify that their votes have been properly recorded and counted.

Keywords

Electronic voting / Voting systems / Electronic voting machine / Internet voting / Anonymity / Trust / Mixed networks / Blind signature

Introduction

Les algorithmes et les systèmes de vote électronique ont été développés dans le but de moderniser et de faciliter le processus électoral. Cependant, l'idée d'automatiser le processus de vote n'est pas récente, des machines de vote auto-mécanique de type machines à levier étaient utilisées aux États-Unis d'Amérique en 1892. Ces machines ont évolué jusqu'à devenir électronique en France à partir de 2002. Néanmoins l'informatisation du vote est contestée par une grande partie de la population. Dans cette fiche de synthèse nous allons faire la part des choses pour apposer une conclusion si l'utilisation de l'informatique pour le vote présidentiel français est envisageable. Pour répondre à cette question nous verrons d'abord les exigences d'un vote, ensuite nous verrons techniquement comment ces exigences sont respectées, puis nous verrons les différents problèmes du vote électronique et pour finir nous conclurons.

Les exigences du vote

Afin de garantir qu'un vote soit démocratique il est nécessaire qu'il respecte plusieurs exigences :

- Droit de vote et unicité : il est important que tous les citoyens admissibles aient le droit de voter et que chaque personne ne puisse voter qu'une seule fois. Cela garantit que chaque vote compte équitablement et que le résultat du vote reflète la volonté de la population de manière juste et équitable.

- Anonymat : il est important que les électeurs puissent voter de manière anonyme pour éviter la pression ou la coercion de la part d'autres personnes. Cela garantit que chaque électeur peut exprimer sa véritable opinion sans crainte de représailles.

- Résistance à la coercition : les systèmes de vote doivent être conçus de manière à résister aux efforts de coercion qui visent à influencer le résultat d'une élection. Cela se traduit en des mesures de sécurité pour empêcher la fraude, la violence, la pression.

- Vérification de son vote : il est important que les électeurs puissent vérifier que leur vote a été enregistré et comptabilisé de manière correcte. Cela peut se faire en utilisant des reçus de vote ou en permettant aux électeurs de vérifier en ligne que leur vote a été pris en compte.

- Transparence et confiance : les systèmes de vote doivent être transparents et fiables pour garantir la confiance des électeurs dans le processus électoral. Cela peut inclure la publication des résultats du vote en temps réel, la diffusion en direct des décomptes et l'accès ouvert aux données de vote.

Deux systèmes de vote électroniques différents

Il existe deux systèmes de vote électronique principaux : les urnes électroniques et le vote par internet

Les systèmes de vote par urne électronique utilisent des machines sur lesquelles les électeurs peuvent sélectionner leurs choix en utilisant un écran tactile ou un clavier. Les votes sont enregistrés dans la machine et peuvent être comptabilisés de manière automatique une fois la période de vote terminée. Ces systèmes ont l'avantage d'offrir une expérience de vote similaire à celle du vote papier, mais ils peuvent être coûteux à mettre en place et à entretenir en raison de la nécessité de maintenir et de remplacer les machines de vote. Il est à noter que seules 64 communes utilisent encore ces système en France et que ce nombre descend d'élection en élection.

Modèles agréés par le ministère de l'Intérieur :

- ESF1 (HW 1.06/2.01 – FW 4.02) » – Nedap (Hollande)
- iVotronic – ES&S Datamatique (USA)
- Point & Vote plus – Indra Sistemas SA (Espagne)

Les systèmes de vote par Internet permettent aux électeurs de voter en ligne à partir de leur ordinateur ou de leur appareil mobile. Ils peuvent être utilisés pour des élections locales, régionales ou nationales et offrent une grande souplesse en termes de temps et de lieu de vote. Cependant, ils sont également exposés à des risques tels que la fraude en ligne et les attaques informatiques, et ils peuvent exclure les électeurs qui ne disposent pas d'un accès fiable à Internet.

Architecture technique utilisées

De nombreuses techniques sont utilisées pour respecter les exigences d'un vote démocratique de manière informatique. Dans cette partie nous allons nous intéresser à deux de ces techniques : la signature aveugle et les mix networks.

Signature aveugle

La signature aveugle est une technique de cryptographie utilisée pour garantir l'anonymat et la confidentialité dans les communications en ligne. Elle permet à un utilisateur de signer un document de manière à ce que la signature ne puisse pas être associée à l'utilisateur. Le principe de la signature aveugle repose sur l'utilisation de deux clés, une clé publique et une clé privée. L'utilisateur souhaitant signer un document de manière aveugle effectue les étapes suivantes :

1. L'utilisateur génère une paire de clés publique et privée.
2. L'utilisateur envoie sa clé publique à un tiers de confiance, appelé tiers de garantie, mais garde sa clé privée secrète.
3. L'utilisateur rédige le document qu'il souhaite signer et le transmet au tiers de garantie, qui lui fournit une version "aveugle" du document en masquant l'identité de l'utilisateur.
4. L'utilisateur utilise sa clé privée pour signer la version aveugle du document et envoie la signature au tiers de garantie.
5. Le tiers de garantie utilise la clé publique de l'utilisateur pour vérifier la signature et transmet le document signé et la signature au destinataire du document.

La signature aveugle permet à l'utilisateur de signer un document de manière à ce que seul le tiers de garantie connaisse l'identité de l'utilisateur. Le destinataire du document ne peut pas savoir qui a signé le document, ce qui garantit l'anonymat de l'utilisateur.

Mix network

Les mix networks sont une technique utilisée pour améliorer l'anonymat et la confidentialité dans les communications en ligne. Ils fonctionnent en mélangeant les messages de différents utilisateurs de manière à ce qu'il soit difficile de déterminer l'origine d'un message spécifique.

Le principe de fonctionnement d'un mix network est le suivant :

1. Un utilisateur souhaitant envoyer un message à un destinataire envoie d'abord le message à un nœud de mélange (ou mix).
2. Le mix ajoute son propre message au "paquet" de messages qu'il reçoit, de manière à ce que tous les messages soient mélangés ensemble.
3. Le mix envoie le paquet de messages mélangés à un autre mix, qui répète le processus de mélange.
4. Ce processus de mélange est répété plusieurs fois, de sorte que les messages sont mélangés et envoyés à travers plusieurs mixes avant d'atteindre leur destination finale.

L'objectif des mix networks est de rendre difficile pour un observateur extérieur de déterminer l'origine d'un message spécifique en raison du mélange des messages de différents utilisateurs. Cela peut être utile pour protéger l'anonymat des utilisateurs et

assurer la confidentialité de leurs communications. Les mix networks sont souvent utilisés dans les systèmes de vote en ligne pour protéger l'identité des électeurs et assurer la confidentialité de leur vote.

Les problèmes du vote électronique

Dans cette partie nous allons discuter des problèmes qui peuvent survenir en théorie avec le vote électronique, nous verrons aussi les différents problèmes qui sont survenus en pratique lors d'élections.

Pour les urnes électroniques :

Un des problèmes majeurs des urnes électroniques est que chacun des votants doit faire confiance à l'algorithme s'exécutant sur la machine. Néanmoins il est impossible d'avoir confiance en ce dernier étant donné qu'il n'est pas open-source et donc que personne ne peut le vérifier. Nous sommes contraints de faire confiance aux entités de vérification mais nous faisons que déplacer le problème, il faut maintenant faire confiance aux entités de vérification. Ensuite même dans le cas où le programme est open-source et parfait il faudrait pouvoir vérifier que ce dernier est bien celui qui est exécuté sur la machine, techniquement on pourrait le mettre en place en utilisant un checksum du programme et vérifier ce dernier mais nous retombons sur le problème précédent, il faut maintenant faire confiance au programme qui vérifie le checksum.
Pour ces deux points il est donc très difficile de faire confiance aux urnes électroniques.

Ensuite il faut faire remonter les résultats individuels des différentes machines pour les compter, cela peut se faire de différentes manières. Certaines machines utilisent une clé usb qu'on doit transporter, brancher dans une autre machine qui va faire le comptage, néanmoins cette technique est sujette aux attaques par social engineering, une personne peut modifier le résultat de milliers de votes en interchangeant deux clés usb, là où une personne seule en échangeant deux enveloppe aura un impact sur un seul vote.
Certaines machines communiquent directement via réseau privé ou internet, ici sujet aux attaques de type “man in the middle”

Pour finir, dans le cas où un serveur centralisé est utilisé pour compter les votes, ce dernier comporte tous les risques précédents.

Dans la pratiques des problèmes avec les urnes sont apparus, notamment en 2003, en Belgique où un candidat a reçu 4096 voix supplémentaires dû à la valeur d'un bit qui a changé à la suite d'énergie obtenue via des rayons cosmiques.

Les élections allemandes de 2007, 2012 et 2017 ont toutes constaté des différences entre vote et émargement 10 fois supérieur à la par rapport aux votes papier.

En 2019 à la Def Con (convention de hack aux états-unis) des hackers réussissent à faire tourner Doom sur une des machines (et bien d'autres hacks)

Pour le vote via internet :

Le vote via internet comprend les problèmes de l'urnes auxquels s'ajoutent de nouveaux. D'abord, le plus grand problème, la vulnérabilité des systèmes clients, si le vote via internet se démocratise, ce serait toute la population qui l'utiliserait, de l'ingénieur informatique à Polytech aux personnes âgées de 85 ans utilisant leur ordinateur 3 fois par an. De ce fait, cela deviendrait facile de modifier le résultat des votes par l'utilisation de botnet en ayant infectés machines de personnes pas au point sur la cybersécurité.

De plus même si la personne n'a pas de virus elle peut se faire usurper ses identifiants, en utilisant, par exemple une attaque par dictionnaire, ou en utilisant des identifiants leaks qui ont été réutilisés. Même sans cela nous pouvons imaginer une personne oubliant de se déconnecter d'un pc public sur un des services de France Connect.

Un des autres problèmes que peut engendrer le vote via internet est la simplification de la vente de vote, en effet dans ce cas nous ne somme pas contraint de voter dans l'isoloire ce qui rend facile la vérification d'un tier que nous votons bien pour tel candidat, donc permettant de mettre en place la vente de vote. Nous pouvons aussi imaginer une automatisation de ce processus, en entrant nos identifiants dans une plateforme tierce qui fera à notre place le vote et fera le virement à la suite.

En pratique nous pouvons facilement modifier le code des applications clientes, cela à été fait par Mr Laurent Grégoire (démonstration)

Conclusion

Le vote électronique se montre intéressant pour les votes sans sources de menace néanmoins les failles rendent son utilisation trop risquée pour des élections comportant des sources de menaces sérieuses comme les élections présidentielles.

Sources

Wikipédia, Vote électronique : https://fr.wikipedia.org/wiki/Vote_%C3%A9lectronique
Wikipédia, Electronic voting : https://en.wikipedia.org/wiki/Electronic_voting
CNIL Délibération n° 2019-053 : lien
Firmin de Barros, Thomas Gergouil, Rémy Grelard, Samuel Thibault. Analyse de systèmes de vote électronique. Cryptographie et sécurité [cs.CR]. 2022. hal-03580506 : lien
Tom Scott, Why Electronic Voting Is Still A Bad Idea : https://www.youtube.com/watch?v=LkH2r-sNjQs&t=318s
Laurent grégoire, Comment mon ordinateur a voté à ma place : http://tnerual.eriogerg.free.fr/autovote.pdf