
partipirate

Rapport de la Séance du déchiffrement de l'urne du vote électronique du 23 Septembre 2012

Diego Abelenda, Frédéric Dubouchet, Alexis Roussel et Alexandre Takacs

22 octobre 2012

A propos

Ce rapport a été rédigé par des citoyens exerçant leurs droits politiques dans le canton de Genève. Ils ont tous été sollicités par le Parti Pirate Genevois à participer à cet audit citoyen. Il est le résultat de l'observation de la procédure de déchiffrement de l'urne au sein du Canton de Genève du 23 septembre 2012 telle qu'elle a été conçue par la Chancellerie. Le déroulement de la séance est étudié afin d'y relever les risques potentiels ou avérés. Des recommandations sont proposées à chacun des risques identifiés. L'étude du code source du logiciel du vote électronique fera l'objet d'un second rapport. La description des vulnérabilités ou failles logicielles potentielles ou des attaques informatiques possibles ne seront pas traitées dans ce rapport.

Ce rapport a été soumis avant publication à la Chancellerie qui nous a fait part de certaines corrections qui ont été intégrées dans ce document.

Table des matières

Introduction

Le Canton de Genève a développé à partir de 2001 une solution de vote électronique par Internet utilisé depuis 2004 pour des votations cantonales et fédérales. Si la mise en œuvre du vote électronique par Internet a été progressive, le système genevois est maintenant utilisé par plusieurs cantons, notamment pour le vote de leurs citoyens résidant à l'étranger. Il est devenu avec le temps et l'expérience un des outils important de vote en Suisse.

En proposant un nouveau canal de vote pour le citoyen, le vote électronique se doit de fournir toutes les garanties de son bon fonctionnement afin que le peuple puisse lui accorder sa confiance.

Suite à un manque d'information de la part de la Chancellerie et à la survenance d'un problème de double vote lors d'une votation dans le canton de Lucerne, la communauté informatique suisse s'est montrée très critique face à la mise en œuvre du projet. Si des efforts importants de communication et de divulgation de certaines informations ont depuis été réalisés par la Chancellerie, de nombreuses interrogations et craintes demeurent.

Le Parti Pirate Suisse représente les intérêts de la «génération numérique». Il influence la formation de l'opinion et la politique. Les buts des Pirates comprennent la promotion de l'accès libre à la connaissance et à la culture, le renforcement des droits civiques, la protection de la sphère privée, un État transparent et la lutte contre la censure.

Ayant lui même développé une solution de vote électronique par Internet [1], le Parti Pirate Suisse est particulièrement conscient des difficultés et des défis d'un tel projet. Pour le Parti Pirate Suisse, les recommandations de la Haute École Spécialisée Bernoise sur le vote électronique par Internet doivent être prises en considération : le code source du logiciel doit être disponible en open-source et les votes doivent être vérifiables.

C'est dans le cadre d'une démarche de contrôle citoyen que des membres du Parti Pirate Suisse ont demandé au Conseil d'État genevois la possibilité d'exercer leurs droits politiques en accédant au code source du logiciel de vote électronique. Suite à cette demande, la Chancellerie a aussi invité les membres du Parti Pirate à assister à la séance de déchiffrement de l'urne du 23 Septembre 2012.

Remarques Générales

La séance d'ouverture de l'urne électronique en présence de Madame la Chancelière et de la Commission électorale a été réalisée par le personnel de la Chancellerie, avec l'appui de la DGSI (Direction générale des systèmes d'information) et de la police avec un professionnalisme et une solennité exemplaires. La salle avait été préparée avec soin afin que tous les éléments techniques fonctionnent au moment de l'ouverture de la séance. La procédure décrite en détail dans l'ordre du jour a été scrupuleusement respectée sous la direction de Madame la Chancelière.

Si tant l'aspect humain et matériel nous a semblé sous contrôle, il nous a paru rapidement évident que la majorité des personnes présentes dans la salle n'avaient que peu

1. Pivote http ://projects.piratenpartei.ch/projects/pi-vote

d'attention, et probablement des compétences insuffisantes pour appréhender correctement les informations et les manipulations qui se déroulaient à l'écran.

Si la Commission électorale exerce un contrôle citoyen primordial et effectif des activités et des manipulations physiques, la nécessité d'un contrôle de qualité équivalent dans les aspects logiciels nous est apparu comme capital. Cela nous a conforté dans notre démarche. Ce rapport, ainsi que les recommandations énoncées, se veulent être une contribution au développement d'une solution de vote électronique par Internet à Genève pour l'aider à fournir au peuple toutes les garanties nécessaires à l'établissement d'un niveau de confiance élevé.

Si l'étude du code source du logiciel et des aspects purement techniques fera l'objet d'un second rapport, nous avons tout de même souhaité faire part à la Chancellerie des points suivants concernant la séance et son déroulement.

1 Utilisation du mot "décryptage"

Description

La séance d'ouverture de l'urne est nommée "décryptage de l'urne". La définition de décryptage [1] laisse supposer que la chancellerie ne dispose pas de la clé de chiffrement lui permettant d'obtenir les résultats. Une telle approche ne serait pas conforme avec le but recherché par la session. L'activité réelle qui est réalisée est bien celle d'un déchiffrement au moyen de la clé de chiffrement disponible au moment de l'ouverture de l'urne. Le terme "décryptage de l'urne" est celui utilisé par l'administration fédérale et a été repris par la chancellerie genevoise par soucis de cohérence.

Risque

Le projet de vote électronique est un projet à haute visibilité notamment au sein des communautés informatiques spécialisées dans la sécurité et la cryptographie. Une mauvaise utilisation du vocabulaire peut créer une confusion non souhaitée.

Recommandation

Nous recommandons l'utilisation du mot "Déchiffrement" à la place de "Décryptage" afin de dissiper tout doute. Afin de conserver la cohérence entre les administrations, nous recommandons de soumettre cette problématique de la terminologie à l'administration fédérale compétente.

1. définition de décryptage http ://fr.wikipedia.org/wiki/Décrypter

2 Utilisation du vidéo-projecteur

Description

La procédure prévoit l'utilisation de deux ordinateurs distincts pour le déchiffrement de l'urne et pour la compilation des résultats notamment avec ceux du vote par correspondance. L'utilisation du vidéo-projecteur permet à l'ensemble des personnes présentes de constater les différentes manipulations qui sont réalisés par les personnes responsables. Avant le début de la séance, les deux ordinateurs sont placés l'un à côté de l'autre. Pour des raisons pratiques un seul vidéo-projecteur est installé et retransmet sur l'écran le bureau du premier ordinateur. Lorsque les manipulations ont été réalisées sur le premier ordinateur, le câble reliant l'ordinateur au vidéo-projecteur est physiquement débranché pour être rebrancher sur le second ordinateur. Cette phase de débranchement/branchement n'est pas toujours maîtrisée techniquement et nécessite souvent des manipulations sur l'ordinateur accueillant le câble afin de sélectionner correctement le canal de sortie de l'image vers le vidéo-projecteur. Cette difficulté a notamment été constatée lors de la séance. Le vidéo-projecteur n'affichant pas immédiatement l'image du bureau de l'ordinateur sur l'écran, plusieurs manipulations ont été effectuées sans aucun contrôle visuel de la part des personnes présentes dans la salle.

Aussi, avant la saisie des mots de passe, le vidéo-projecteur est débranché de l'ordinateur, puis rebranché après validation. Durant cette phase, l'image du bureau de l'ordinateur reste invisible aux autres personnes présentes. Après interrogation auprès des services de la Chancellerie, nous avons constaté que les mots de passe apparaissaient en clair sur l'ordinateur. L'affichage des mots de passe en clair permettrait de faciliter leur saisie par des personnes de la Commission électorale qui ne seraient pas forcément à l'aise avec l'utilisation des ordinateurs.

Risque

Une manipulation non contrôlée peut être effectuée lorsque le vidéo-projecteur n'est pas branché. Selon la Chancellerie, cela ne représente pas un risque, car l'utilisation des ordinateurs se fait dans un ordre précis. Lorsque le deuxième ordinateur est utilisé, une manipulation sur le premier ordinateur n'aurait aucune incidence. Toutefois, une manipulation non contrôlée reste possible selon nous lors de la saisie des mots de passe.

Recommandation

Le vidéo-projeteur doit être constamment branché et retransmettre l'image de l'ordinateur à tout moment afin de permettre un bon contrôle des manipulations effectuées.

L'utilisation d'un commutateur vidéo partageant le vidéo-projecteur permet d'éviter les manipulations risquées. Le commutateur vidéo permettra au personnel de la Chancellerie de préparer les flux vidéos des deux ordinateurs et d'en vérifier le bon fonctionnement avant le début de la séance. L'utilisation d'un commutateur vidéo permet aussi de faciliter la manipulation en la résumant à l'action d'un seul bouton. La phase d'utilisation du commutateur vidéo peut être documentée dans la procédure afin qu'il puisse être constaté qu'aucune manipulation sur aucun des deux ordinateurs ne peut se faire sans que l'image du bureau de ceux-ci ne soit projetée sur l'écran. Afin de faciliter ce contrôle, les deux ordinateurs pourront être disposés dans deux endroits suffisamment éloignés. L'opérateur d'un ordinateur devrait se trouver à une distance lui interdisant de manipuler le deuxième ordinateur. En l'absence d'un commutateur vidéo, l'utilisation de deux vidéo-projecteurs différents branchés à l'avance aux ordinateurs permettrait de réduire le risque présenté.

3 Contrôle des manipulations réalisées sur les ordinateurs

Description

La majorité des manipulations sur chaque ordinateur sont effectuées par une seule et même personne. Un opérateur pour le premier ordinateur effectue le déchiffrement de l'urne et un autre opérateur pour le deuxième ordinateur effectue la compilation des résultats. Lors de la séance du 23 Septembre, une erreur de manipulation a été réalisée par le deuxième opérateur. Cette erreur a rendu impossible la production de résultats de la votation. Toutefois, sur l'écran les résultats apparaissaient en vert, couleur utilisée lorsque les manipulations sont réalisées avec succès. L'opérateur a immédiatement signalé l'erreur qu'il avait lui-même commise, et a pu annuler la manipulation pour la recommencer. Cette manipulation aurait pu ne pas être détectée sans le professionnalisme et l'honnêteté de l'opérateur.

Risque

Des erreurs de manipulations peuvent être réalisées sans contrôle et peuvent générer des affichages incohérents des résultats sur l'écran.

Recommandations

Le logiciel de compilation des résultats doit être corrigé afin de ne pas autoriser la manipulation constatée lors de la séance du 23 septembre. L'ensemble des logiciels doivent être modifiés soit afin d'y :

- inclure le principe des "quatre yeux" nécessitant l'intervention de deux opérateurs différents pour le déclenchement de chaque manipulation. Cette modification doit être aussi répercutée au sein de la procédure. La désignation de deux opérateurs différents lors de chaque votation, dont un externe aux services de la Chancellerie, permettra de réduire les risques d'erreur de manipulation.
- éliminer les manipulations au profit d'une automatisation accrue.

Dans le cas où une manipulation incorrecte serait tout de même réalisée, le retour en arrière ne doit être possible qu'après la saisie d'un mot de passe de sécurité détenu par une personne autre que l'opérateur. Cette manipulation extraordinaire doit faire l'objet d'une inscription au procès-verbal.

4 Transfert des résultats au moyen d'une clé USB

Description

Plusieurs clés USB sont utilisées dans le processus de déchiffrement de l'urne et de la compilation des résultats. La première clé USB disposant de la clé privée de chiffrement est conservée dans une enveloppe scellée selon les procédures standards de conservation. Une deuxième clé USB est utilisée pour effectuer le transfert des résultats entre les deux ordinateurs. À la fin de l'étape de déchiffrement, lorsque les résultats sont produits sous forme de fichiers, seuls les résultats de la commune fictive de test sont vérifiés. Les fichiers sont ensuite transférés sur la clé USB puis sur le deuxième ordinateur.

Risque

Les données des résultats peuvent être compromises lors de ce transfert sur un média non-sécurisé. La clé USB pourrait, par exemple, contenir une intelligence qui n'écrirait que le nombre total de votants et créerait à la volée des résultats.

Recommandation

Dans l'ensemble de la procédure, l'utilisation d'une simple clé USB non contrôlée constitue le risque le plus important. L'utilisation d'une clé USB neuve encore dans son emballage, d'un support "write-once" ou d'un système de stockage sécurisé réduirait le risque. Enfin, un contrôle d'intégrité de l'ensemble des fichiers des résultats effectué sur les deux ordinateurs, au moyen d'un algorithme cryptographique de hashage sûr, comme par exemple SHA-512, permettrait de supprimer le risque d'un transfert compromis des résultats. Cette recommandation ne serait plus nécessaire si la recommandation 7 est mise en œuvre.

5 Transfert des données vers les autres cantons

Description

Sans avoir pu assister à la procédure de transfert des fichiers des données contenant les résultats vers les autres cantons, il nous a été signalé par les services de la Chancellerie que ce transfert avait lieu avec l'aide de la technologie FTP. Selon la Chancellerie, les données échangées entres cantons sont cryptées et signées, chaque utilisateur disposant de sa propre identité numérique, la procédure ayant été validée par la Chancellerie fédérale. Pourtant cette technologie FTP extrêmement efficace est connue pour son niveau de sécurité très faible. Les identifiants et les mots de passe sont transférés en clair sur le réseau.

Risque

Les données transférées vers les autres cantons peuvent être interceptées et modifiées avant réception de celles-ci par les autorités cantonales.

Recommandation

L'utilisation de certaines méthodes de sécurisation des transferts de données telles que OpenSSH permettrait de réduire le risque. Nous recommandons d'analyser la méthode existante et d'analyser l'utilisation de méthodes alternatives plus sûres. Cette recommandation est une invitation à étudier cet aspect du transfert des données, n'ayant nous-même pas pu constater le fonctionnement, ni connaître les détails techniques actuellement mis en place.

Lors de l'étude du code source, nous demanderons des précisions complémentaires concernant les méthodes cryptographiques utilisées.

6 Utilisation de plate-formes dédiées à la sécurité

Description

Le vote électronique est une application hautement critique et exigeante en terme sécurité. Nous avons constaté que l'ensemble des logiciels fonctionnent sur des systèmes d'exploitation standard, type Windows. La plupart des systèmes vitaux pour les administrations et les entreprises fonctionnent aujourd'hui sur des systèmes d'exploitation hautement sécurisés. Les solutions libres sont particulièrement prisées car elle permettent un contrôle précis de l'ensemble du système d'exploitation, tout en proposant une indépendance technique et politique vis-à-vis de l'éditeur.

Risque

Bien qu'une bonne sécurisation d'un système d'exploitation standard est possible, le risque d'être sujet à des failles non-connues ou non-corrigées est important.

Recommandation

L'utilisation de systèmes d'exploitation conçus pour la sécurité et reconnus pour leur développement exigeant tels que OpenBSD ou SELinux [1] assurerait une maîtrise complète par les services de la Chancellerie. L'application de la virtualisation [2] aux différents services logiciels du vote électronique permet le partitionnement des différentes ressources sur une même plate-forme de serveurs assurant ainsi une meilleure efficacité et sécurité. Avec une telle solution, la sécurisation des ordinateurs utilisés lors de la séance serait plus aisément assurée. Si nous reconnaissons qu'une migration vers des systèmes d'exploitation tels que OpenBSD ou SELinux, ainsi qu'une virtualisation des machines sont des projets techniques importants, les avantages en termes de sécurité seront vites récompensés. Nous recommandons ainsi la programmation de cette migration dans les étapes futures du développement du système de vote électronique pour l'ensemble des appareils utilisés.

1. Security-focused operating system http ://en.wikipedia.org/wiki/Security-focused_operating_system
2. La virtualisation http ://fr.wikipedia.org/wiki/Virtualisation_(informatique)

7 Mise à disposition publique de l'urne et de la clé privée

Description

Les systèmes vérifiables ont pour but de permettre aux électeurs de retracer les différentes étapes du processus de vote et de constater l'exactitude du résultat d'un scrutin. Chaque électeur peut vérifier si le suffrage pris en compte dans le résultat du scrutin correspond bien au suffrage qu'il a donné. Il peut d'autre part vérifier si le résultat du scrutin est bien le reflet de l'ensemble des suffrages exprimés.

Risque

La perte de confiance dans un système dit de "black-box" constitue pour nous un risque important. Ce risque est réel car des systèmes de vote électronique ont déjà du renoncer à leur exploitation suite à des problèmes soit techniques soit de mise en œuvre ayant engendré une perte de confiance.

Recommandation

Si la vérification de la prise en compte du vote individuel nécessite la modification du système de vote, la vérification du résultat du scrutin nous semble être facilement réalisable sans aucune modification du système. Après l'annonce des résultats officiels par la Chancellerie à 12h00, le fichier contenant l'urne chiffrée, les clés de chiffrement ainsi que les mots de passe pourraient être publiés et mis à disposition du public sur le site Internet du service des votations. Sans mettre en danger la phase de vote ainsi que la procédure de déchiffrement, la mise à disposition de ces données au public permettrait le développement de calculateurs indépendants et citoyens. La multiplication de ceux-ci conforterons la précision du calcul des résultats de la solution développée par la Chancellerie. Cette recommandation, si elle était suivie, n'engendrerait aucun coût ni risque supplémentaires pour la Chancellerie. Elle serait en outre compatible avec la restriction imposée par la loi sur la publication du code source du logiciel. Cette recommandation permet de répondre à notre interrogation principale décrite dans les remarques générales à savoir la mise en place d'un contrôle citoyen effectif sur les aspects logiciels de la procédure du déchiffrement de l'urne.

8 Mots de passe

Description

Lors de la phase de déchiffrement, deux mots de passe différents détenus par quatre membres de la Commission électorale doivent être saisis. Avant la saisie, le vidéo-projecteur est débranché de l'ordinateur, puis rebranché après la validation des mots de passe. Durant cette phase, l'image du bureau de l'ordinateur reste invisible aux autres personnes présentes. Après interrogation auprès des services de la Chancellerie, nous avons constaté que les mots de passe apparaissaient en clair sur l'ordinateur. L'affichage des mots de passe en clair permettrait de faciliter leur saisie par des personnes de la Commission électorale qui ne seraient pas forcément à l'aise avec l'utilisation des ordinateurs.

Recommandations

Aujourd'hui, l'utilisation de l'informatique est largement répandue. Notamment l'utilisation des services sécurisés par mots de passe fait partie intégrante d'un usage de base d'un ordinateur. Tout en appréciant la volonté de faciliter la tâche aux membres de la Commission électorale, nous considérons que cette fonctionnalité n'est plus nécessaire.

Afin de faciliter la mise en œuvre des recommandations 2 et 7, les options suivantes devraient être étudiées :

Option 1 : Afin de conserver le secret du mot de passe, nous recommandons la modification du logiciel afin que celui-ci ne fasse plus apparaître les mots de passe en clair. Différentes techniques sont disponibles :

- le remplacement de chaque caractère par une étoile (*),
- le remplacement de chaque caractère par un nombre aléatoire d'étoiles [1].

L'affichage complètement invisible du mot de passe reste la solution la plus sûre. Toutefois elle ne permet pas un contrôle visuel de la manipulation.

Option 2 (préférée) : Lors de chaque nouvelle votation, des nouveaux mots de passe sont utilisés. Nous pouvons dès lors accepter que les membres de la Commission électorale ne soient tenus au secret du mot de passe que jusqu'au moment de le saisir sur l'ordinateur, le faisant apparaître en clair sur l'écran. Si la mesure de protection (débranchement du vidéo-projecteur) n'apporte aucune sécurité, en revanche elle ajoute un élément de

1. Cette technique affiche un nombre de caractères différent de celui que contient réellement le mot de passe et empêche de connaître le nombre réel de caractères que contient le mot de passe. Cela permet toutefois d'aider à la saisie en fournissant un retour visuel à la saisie d'un caractère du mot de passe.

confusion. Afin d'éviter l'utilisation de mots de passe proches lors des différentes votations ou des mots de passe trop simples, nous recommandons aussi de sensibiliser les membres de la Commission électorale aux techniques de création et de mémorisation des mots de passe. De nombreuses méthodes existent et peuvent faire l'objet d'une formation annuelle.

Enfin, afin de diminuer les risques d'oubli des mots de passe, nous recommandons d'étudier la possibilité d'utiliser des méthodes de sécurité partagée, telle que Shamir-Shared [2].

Selon la Chancellerie, les membres de la Commission électorale sont tenus au secret du mot de passe après la publication des résultats afin de garantir la préservation des preuves en cas de recours. Dans le cas d'une procédure judiciaire par exemple, la Chancellerie doit être en mesure de procéder au dépouillement de l'urne électronique plusieurs semaines après la séance de déverrouillage. Dès lors, afin de garantir que le contenu de l'urne n'a pas été altéré, les mots de passe doivent rester secrets y compris au-delà de la séance de déverrouillage. Toutefois une préservation de l'urne pourrait être garantie par le gel de la base avant le déchiffrement. Dans le cas d'une procédure judiciaire, les enquêteurs pourront constater que la base de donnée étudiée est bien la même que celle utilisée lors de la séance de déchiffrement.

2. Shamir's Secret Sharing http ://en.wikipedia.org/wiki/Shamir's_Secret_Sharing

9 Publication des analyse des votes

Lors de notre visite, les services de la Chancellerie nous ont fait part de l'existence de travaux universitaires réalisés sur les résultats de vote électronique. Ces travaux représentent des analyses des votes en fonction des thématiques et bureaux de vote. Ces travaux permettent d'établir certaines corrélations et de déterminer la cohérence des résultats du vote électronique avec ceux du vote traditionnel. Ces analyses se basant sur des données déjà publiques et utilisant des méthodes d'analyses connues, nous encourageons la Chancellerie à les publier à titre informatif.

Conclusion

Comme déjà énoncé dans les remarques générales, le processus actuel de réalisation des tâches ainsi que de leur contrôle est globalement solide concernant les étapes physiques de la séance de déchiffrement de l'urne, mais nécessite des adaptations. Des améliorations sont proposées dans les points 2, 3, 4 et 8. Le point 4, concernant le transfert des données des résultats entre les deux ordinateurs sur un média non sécurisé, a été identifié comme comportant un risque important et nécessite à notre avis une modification de la procédure lors des prochains scrutins. Par contre, le contrôle de ce qui se passe "sur l'écran" nous a paru très faible. Les points 1, 5, 6, 7 et 9 visent à compléter le contrôle existant et l'étendre dans les aspects logiciels de la procédure. Nous sommes convaincus que leur mise en œuvre aura un impact positif durable sur le niveau de confiance. De manière générale, nous recommandons donc *une automatisation accrue des tâches informatiques* afin d'éviter les erreurs de manipulation ou les possibilités d'une interaction frauduleuse, ainsi que *le développement d'un contrôle des aspects logiciels* notamment par l'adoption d'outils ouverts et reconnus dans le domaine de la sécurité. Ces recommandations seront complétées par le rapport d'étude du code source.