Traitement du problème de la sécurité des plates-formes pour le vote par Internet à Genève

Dr Rolf Oppliger

ESECURITY Technologies Rolf Oppliger
BeethovenStrasse 10
CH – 3073 Gümligen
Suisse

http://www.esecurity.ch
mailto:rolf.oppliger@esecurity.ch

3 mai 2002

Ce rapport a été préparé pour le compte de la Chancellerie d'Etat du canton de Genève

Table des matières

Résumé

En janvier 2002, la Chancellerie d'Etat du canton de Genève a publié le rapport final d'un comité nommé pour étudier et évaluer la sécurité d'une application de vote à distance par Internet [Gen02]. Le rapport est parvenu à la conclusion que l'application présentait un niveau raisonnable de sécurité, mais qu'au moins deux problèmes liés à la sécurité devaient être examinés avec soin :

- **Problème de l'authenticité du serveur** : Les utilisateurs d'Internet ne se soucient généralement pas de l'authenticité du serveur et ne vérifient donc pas convenablement les certificats de clés publiques. Ce problème s'applique aussi aux serveurs utilisés pour le vote à distance par Internet.
- **Problème de la sécurité des plates-formes** : les citoyens votant par Internet et leurs plates-formes sont vulnérables aux logiciels malveillants (par exemple virus informatiques, chevaux de Troie etc.) et peuvent donc être attaqués.

Comme solution possible à ces problèmes, le rapport du comité suggère à l'Etat de Genève de faire distribuer des CD-ROM aux électeurs. Ces CD-ROM comporteraient le logiciel et les certificats des clés publiques requis pour authentifier le ou les serveurs de vote par Internet et voter à distance de manière suffisamment sûre. Le rapport fait en outre la distinction entre trois approches de configuration et de distribution des CD-ROM[1].

Dans ce contexte, la Chancellerie d'Etat du canton de Genève a demandé à eSECURITY Technologies Rolf Oppliger d'étudier et de commenter les suggestions présentées dans le rapport du comité et de donner son avis d'expert assorti de recommandations sur la manière de traiter les problèmes de sécurité mentionnés plus haut pour le vote par Internet à Genève. Cet avis doit prendre en compte et mettre en perspective l'état actuel de la technique en matière de sécurité informatique se rapportant au problème d'authenticité du serveur et – point plus important – au problème de la sécurité des plates-formes.

Ce rapport est le résultat de ce mandat. Il fait valoir que la communauté scientifique reconnaît la difficulté du problème de la sécurité des plates-formes et que l'idée généralement répandue

est qu'il est actuellement impossible de mettre en œuvre, à grande échelle, une procédure de vote par Internet suffisamment sûre. Cette argumentation ne tient cependant que si elle applique à un cadre ne prévoyant pas le vote par correspondance. Or l'Etat de Genève ayant mis en œuvre le vote par correspondance depuis une décennie, cette argumentation ne s'applique pas nécessairement. On pourrait en fait soutenir que le niveau de sécurité de tout nouveau système de vote, y compris par exemple le vote par Internet, doit être comparable au niveau de sécurité du vote par correspondance. Et un tel niveau de sécurité semble atteignable.

Dans ce contexte, ce rapport développe certaines approches techniques pour remédier au problème de la sécurité des plates-formes et recommande l'utilisation combinée de feuilles de codes[2] et d'urnes tests (notez que l'utilisation de feuilles de codes va à l'encontre du rapport du comité qui suggérait l'utilisation de CD-ROM distribués par l'Etat de Genève). L'idée fondamentale de l'utilisation de feuilles de codes réside dans le fait que les valeurs constantes (à savoir "OUI" et "NON" dans le cas d'une votation ou du nom des candidats dans le cas d'une élection) sont remplacées par des valeurs variables qui ne peuvent être devinées par un logiciel malveillant qu'avec une probabilité arbitrairement faible (à savoir négligeable). On peut donc supposer qu'un logiciel malveillant ne peut pas modifier un scrutin de manière significative. De plus, l'utilisation de numéros de vérification supplémentaires renvoyés du serveur de vote au votant peut garantir à ce dernier qu'il est connecté à un serveur autorisé et que son vote a bien été reçu. A ce titre, l'utilisation de feuilles de codes convient pour traiter les deux problèmes mentionnés plus hauts (à savoir l'authenticité du serveur et la sécurité des plates-formes). L'utilisation de certificats de clés publiques pour le ou les serveurs de vote reste possible et recommandée, mais elle peut désormais être complétée par un autre mécanisme d'authentification du serveur.

La mise en œuvre du vote par chiffrement semble réalisable à Genève car l'Etat doit de toute manière fournir des cartes de vote personnalisées[3] aux électeurs utilisant le vote par correspondance. Ces cartes de vote peuvent alors être envoyées avec les feuilles de codes nécessaires pour le vote à distance. Le présent rapport donne une vue d'ensemble, commente

[1] Pour utiliser des CD-ROM de manière suffisamment sûre, ceux-ci devraient être initialisables. Le rapport du comité ne prévoit malheureusement pas explicitement cette exigence.
[2] L'utilisation de feuilles de codes nécessite la saisie par le votant d'un numéro de code (c'est-à-dire une chaîne de caractères) au lieu de "OUI" ou "NON" dans le cas d'une votation ou d'un nom de candidat dans le cas d'une élection. Dans les publications, l'utilisation de feuilles de codes pour voter est parfois appelée aussi "vote par chiffrement". Ce terme est aussi utilisé dans ce rapport.
[3] Les cartes de vote doivent être personnalisées car elles comportent un code secret unique servant de numéro personnel d'identification (PIN) permettant d'authentifier le votant.

et met en perspective trois mises en œuvre possibles du vote par chiffrement à Genève et plaide en faveur d'une stratégie évolutive.

Quelques points restent en suspens et doivent être résolus avant de pouvoir mettre en place et utiliser le vote par chiffrement dans l'Etat de Genève.

- Premièrement, il faut vérifier si le vote par chiffrement tel qu'il est présenté dans ce rapport est légalement accepté en Suisse et dans l'Etat de Genève. Ceci doit être vérifié séparément pour chaque mise en œuvre possible.

- Deuxièmement, les notes préliminaires concernant les mises en œuvre possibles doivent être développées afin d'expliquer comment mettre en place et utiliser de manière sûre le vote par chiffrement dans l'Etat de Genève.

- Troisièmement, le vote par chiffrement implique aussi une modification du comportement du votant. Au lieu d'inscrire "OUI" ou "NON" ou de cocher simplement la case correspondante, il doit saisir un numéro de code et/ou vérifier un autre numéro qui est renvoyé par le serveur. C'est une question d'habitude à prendre qui doit être traitée en conséquence. Ceci signifie essentiellement que les études sur le terrain doivent montrer si cette modification du comportement du votant est bien comprise par les électeurs et si elle est acceptée en pratique.

En tout état de cause, le niveau de garantie de la sécurité de l'application du vote par Internet doit être augmenté autant que faire se peut. Ceci nécessite une conception ouverte et une discussion libre, ainsi que des examens et des vérifications par des pairs. Toutefois, cela n'implique pas d'étudier tous les codes sources, ni de publier les logiciels en divulguant leur code source.

1. Introduction

Les élections et les votes sont au cœur de toutes les démocraties. Ce sont en fait des éléments et processus de base pour le bon fonctionnement d'un gouvernement démocratiquement légitimé.

- Les *élections* servent à habiliter des hommes politiques à parler au nom du peuple (c'est-à-dire qu'ils en sont les représentants)

- Les *votations* servent à demander à la population d'exprimer sa volonté politique (c'est-à-dire qu'ils servent à débattre des décisions politiques).

Dans chaque cas, les électeurs inscrits doivent pouvoir procéder à des scrutins et s'exprimer d'une manière préalablement définie. Le terme de *vote électronique* est utilisé dans les documentations techniques pour désigner des élections et des votations prises en charge par des moyens électroniques. Indépendamment du terme *vote électronique,* l'idée de recourir à des moyens électroniques pour procéder à des élections ou des votations a attiré de nombreux pays dans le passé. A titre d'exemple, Thomas A. Edison s'est vu délivrer le brevet des Etats-Unis n° 90.646 en juin 1869 pour un "Enregistreur électrique de votes" destiné à être utilisé au Congrès. Depuis lors, différents systèmes directement ou indirectement liés au vote électronique ont été inventés, approuvés, mis en œuvre, partiellement revus ou rejetés. Certains de ces systèmes ont fait l'objet de brevets[4] tandis que d'autres ont été couverts par d'autres modes de protection de la propriété intellectuelle (les secrets commerciaux par exemple).

Avec l'expansion d'Internet, beaucoup ont proposé de recourir au vote électronique afin de rendre le processus de vote plus pratique et – comme on l'espère – d'augmenter la participation du public aux élections et votations.

Aux fins de ce rapport, le terme *vote par Internet* est utilisé pour désigner toute procédure d'élection ou de votation permettant aux électeurs d'exprimer leur suffrage par Internet. Ceci revient à dire que les suffrages doivent être exprimés de manière électronique et que ces

[4] La liste des brevets des Etats-Unis se rapportant au vote électronique se trouve notamment au http://www.safevote.com/patents .

suffrages électroniques doivent être transmis aux contrôleurs de l'élection utilisant Internet comme moyen d'acheminement des votes. A titre d'exemple, aux Etats-Unis le Parti Démocrate d'Arizona a utilisé le vote par Internet en mars 2000 pour ses primaires à la candidature présidentielle[5]. Cette élection concernait plusieurs milliers de votants et était officielle en ce sens que le résultat était irrévocable. Le système de vote électronique n'était toutefois ni public ni certifié par l'Etat de l'Arizona (puisque cette élection était interne au seul Parti Démocrate). Pour que ce système soit utilisé pour des votes ou des élections publics, il doit être certifié par l'Etat dans lequel son utilisation est prévue. A la date de rédaction du présent document, aucun Etat n'a encore officiellement certifié un tel système. Ce fait devrait être pris soigneusement en considération car le premier Etat certifiant officiellement un système de vote électronique sera au centre de l'attention de tous les médias internationaux.

2. Vote par Internet

Il existe de nombreuses possibilités de mise en œuvre du vote par Internet. Par exemple, une distinction est généralement faite selon les lieux de vote et les personnes ou entités administrant et contrôlant réellement les votants, les plates-formes et les contextes d'exploitation, le vote par Internet dans les bureaux de vote et à distance.

- Le *vote par Internet dans les bureaux de vote* se réfère aux suffrages exprimés dans les bureaux de vote où des responsables de la supervision des élections administrent et contrôlent intégralement les votants, les plates-formes et les contextes d'exploitation.

- A l'opposé, le *vote à distance par Internet* se réfère aux suffrages exprimés depuis des lieux privés (par exemple à la maison, au bureau, à l'école etc.) où le votant (ou une tierce partie agissant en son nom) administre et contrôle le votant, la plate-forme et le contexte d'exploitation.

Compte tenu du fait que les médias se sont axés sur la perspective de l'utilisation d'Internet pour voter, il n'est pas surprenant que les termes "vote par Internet" et "vote à distance par Internet" soient utilisés comme synonymes dans la presse à grand tirage. Comme nous le verrons par la suite, il est cependant logique de distinguer ces deux termes.

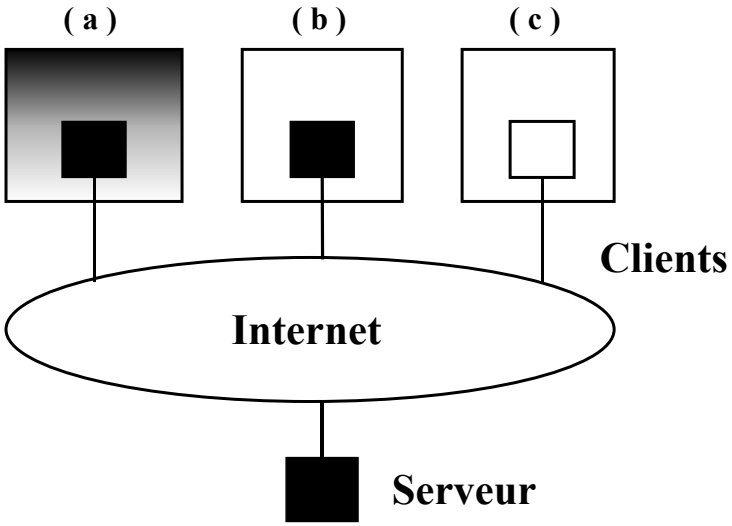
[5] La société election.com a été désignée pour procéder à l'élection. De plus amples informations peuvent être obtenues sur le site de la société à http://election.com.

Dans certaines références (par exemple le document [Cal00]), une distinction supplémentaire est faite entre le vote par Internet dans les bureaux de vote où un lieu de vote de circonscription doit être utilisé, et le vote par Internet dans des bureaux de vote où n'importe quel lieu de vote officiel peut être utilisé. Le présent rapport ne fait pas cette distinction et les deux possibilités sont collectivement dénommées vote par Internet dans les bureaux de vote.

Une troisième possibilité constitue une étape intermédiaire entre le vote par Internet dans les bureaux de vote et le vote à distance par Internet.

- Le *vote en cabine* se réfère au vote effectué en dehors des bureaux de vote officiels dans des lieux publics (comme des galeries commerciales, des bureaux de poste, des bibliothèques, des écoles etc.) où des responsables chargés de la supervision des élections administrent et contrôlent les votants et leurs ordinateurs mais ne peuvent pas intégralement contrôler les lieux mêmes. Des moyens techniques de surveillance et de contrôle peuvent cependant être utilisés pour contrôler à distance le cadre des opérations lorsque cela est nécessaire et approprié.

  Il faut noter que le vote en cabine est de conception similaire à l'utilisation des guichets automatiques du secteur financier.[6]



[6] Dans cette analogie, le vote par Internet en cabine est de conception similaire à l'entrée physique dans une banque et le vote à distance par Internet est de conception similaire aux opérations bancaires sur Internet.

Figure 1 : Les trois possibilités de mise en œuvre du vote par Internet : (a) vote par Internet dans un bureau de vote, (b) vote en cabine, et (c) vote à distance par Internet. Un rectangle sombre représente le fait qu'un votant ou un serveur et sa plate-forme sont administrés par des responsables de la supervision des élections ou qu'ils sont utilisés dans un environnement fiable. Au contraire, un rectangle blanc représente le fait qu'un votant et sa plate-forme ne sont pas administrés par des responsables de la supervision des élections ou qu'ils se trouvent dans un environnement jugé non fiable.

Les trois possibilités de mise en œuvre du vote par Internet sont illustrées à la Figure 1. Dans chaque cas, un votant est relié à Internet (et à un serveur de vote). Du côté du votant, le petit rectangle représente le votant et son ordinateur alors que le grand rectangle représente l'environnement d'utilisation. Un rectangle sombre indique que le votant et son ordinateur sont administrés par des responsables de la supervision des élections ou qu'ils se trouvent dans un environnement fiable. Au contraire, un rectangle blanc indique que le votant et son ordinateur ne sont pas administrés par des responsables de la supervision des élections ou qu'ils se trouvent dans un environnement que l'on ne peut pas considérer comme fiable. Dans le vote par Internet dans un bureau de vote (a), le votant et son ordinateur sont administrés par des responsables de la supervision des élections et ils se trouvent dans un environnement fiable, au bureau de vote (deux rectangles sombres). Dans le vote en cabine (b), le votant et son ordinateur sont administrés par des responsables de la supervision des élections (rectangle sombre) mais se trouvent dans un environnement qui n'est pas considéré comme fiable (rectangle blanc). Dans le vote à distance par Internet (c), ni le votant ni sa plate-forme ne sont administrés par des responsables de la supervision des élections et ils n'opèrent pas non plus dans un environnement fiable (deux rectangles blancs). Comme nous l'examinerons plus en détail ci-dessous, les trois possibilités de mise en œuvre du vote par Internet ont des propriétés et des implications très spécifiques quant à la sécurité.

3. Conditions de sécurité requises pour le vote par Internet

De nombreuses enquêtes et études traitant de la sécurité du vote par Internet en général et du vote à distance par Internet ont été faites (par exemple les documents [Cal00, IPI01, Rub01]). Les résultats montrent que la sécurité (y compris la confidentialité et la fiabilité) figure parmi les principales préoccupations techniques pour que le vote par Internet soit d'emblée un

succès. Les systèmes actuels de scrutin par bulletins constituent une norme qui est adoptée comme base pour le vote par Internet. Ils représentent certains compromis entre la commodité pour l'électeur et la protection contre la fraude et l'utilisation abusive. Il est généralement exigé que les élections et votes effectués sur Internet soient au moins aussi sûrs que les actuels systèmes de scrutin par bulletins. Toutefois, si un Etat permettait le vote par correspondance, ceci établirait la norme de sécurité pour le vote par Internet.

De même, il est essentiel qu'un système de vote par Internet fournisse certaines preuves de sa protection contre les attaques pouvant avoir un effet sur les résultats d'une élection ou d'un vote. Il ne suffit pas de soutenir que la survenue d'une attaque spécifique est peu probable ou même très improbable. Il serait très tentant pour une partie motivée (comme un groupe de pirates informatiques, un groupe de partisans, un gouvernement étranger….) de chercher à s'attaquer à une élection ou un vote. Une telle attaque serait une catastrophe politique et pour les relations publiques – ou pire, si elle réussissait et n'était pas détectée, elle compromettrait les résultats de l'élection ou du vote. Il faut donc prendre pour hypothèse que si une attaque spécifique est possible, elle se produira un jour ou l'autre. Bien avant qu'il n'arrive quoi que ce soit, les gens critiqueront ouvertement les systèmes de vote par Internet faisant l'objet d'attaques spécifiques. Le public risquerait de perdre confiance dans le système (même avant qu'une attaque ne se produise)[7]

Parlant de la sécurité, plusieurs exigences doivent être examinées attentivement. Par exemple, un ensemble de onze règles de sécurité a été joint au mandat du Comité (document [Gen02]). La liste des exigences en matière de sécurité est légèrement différente des principes mentionnés ci-dessus (cette liste n'est pas exhaustive) :

1. Intégrité et sûreté du protocole de vote ;

2. Exactitude des résultats ;

3. Authenticité de l'identité du votant (ou de la personne votant au nom de l'électeur) ;

4. Authenticité du serveur ;

[7] Notez que la confiance est difficile et longue à obtenir mais très rapide à perdre.

5. Secret des suffrages exprimés (y compris par exemple l'anonymat du votant) ;

6. Intégrité des scrutins (y compris par exemple la protection contre des logiciels malveillants [8]);

7. Impossibilité du double vote ;

8. Disponibilité et fiabilité du processus de vote (y compris, par exemple, la protection contre les attaques en déni de service.

Certaines exigences de sécurité sont complémentaires et dépourvues d'interaction (par exemple l'intégrité et l'impossibilité du double vote). D'autres exigences, cependant, sont (ou tout au moins semblent) contradictoires. Par exemple, une manière d'attester l'exactitude d'un processus de vote est la capacité de vérification, ce qui signifie que tout le processus de vote est vérifié de manière raisonnable. La capacité de vérification est cependant parfois en contradiction avec le caractère secret du vote. De très vastes études sont en fait effectuées dans le milieu de la cryptographie pour remédier à cette contradiction apparente et garantir à la fois le secret du vote et l'exactitude des résultats (document [Sch00]). La majeure partie de ces recherches développent des codes et des protocoles pour le calcul sûr de parties multiples (par exemple le document [Hir01]).

Dans ce contexte, il est aussi important de noter que les exigences en matière de sécurité du vote électronique sont fondamentalement différentes et plus difficiles à remplir que celles du commerce électronique. Dans le commerce électronique, les opérations financières sont effectuées en ligne mais il y a toujours un processus hors ligne distinct pour les vérifier et corriger les erreurs décelées. Ce n'est pas le cas du vote électronique et cela ne peut pas l'être.[9] L'accent fondamental mis sur la sécurité dans le vote électronique doit donc être la prévention des fraudes et des erreurs, sans dépendre d'une quelconque possibilité de correction après

[8] Un *logiciel malveillant* est un logiciel délibérément conçu pour effectuer une action nuisible que l'utilisateur ne veut pas et auxquelles il ne s'attend pas, et pour cacher cette 'action ou la réaliser tellement rapidement qu'il est impossible de l'arrêter. Les codes malveillants sont aussi appelés *malware* et *vandaware*. Ces termes ne sont toutefois pas utilisés dans ce rapport. Les logiciels malveillants sont généralement importés dans des systèmes informatiques par divers mécanismes connus sous les termes de virus informatiques, vers, programmes écrasant les données en mémoire, chevaux de Troie, contournement du dispositif de sécurité, ou bombes logiques.

[9] Ceci est dû au fait qu'il faut rendre impossible la vente des votes. Notez que si un votant a reçu la preuve de ce pour quoi il a voté (à savoir du suffrage qu'il a exprimé), il pourrait le vendre et l'achat et la vente à grande échelle des voix deviendrait un problème).

coup. C'est une exigence beaucoup plus rigoureuse que celle généralement nécessaire à l'heure actuelle pour les opérations financières et celles du commerce électronique. [10]

La plupart des condition de sécurité requises du vote par Internet peuvent être obtenues grâce aux technologies, mécanismes et services existants (par exemple les documents [Opp00, Opp02]). Pour donner un exemple, la question de l'authenticité de l'identité du votant peut être traitée par des codes secrets distribués sur des cartes de vote personnalisées. D'autres technologies pourraient utiliser des certificats de clés privées et de clés publiques. De même, la confidentialité et l'intégrité des votes peuvent être traitées par le protocole *Secure Sockets Layer* (SSL) ou *Transport Layer Security* (TLS) comme le proposent les concepteurs de l'application de vote à distance par Internet de Genève. Il est cependant important de noter que l'utilisation du protocole SSL / TLS protège la confidentialité et l'intégrité des votes uniquement pendant leur transmission sur Internet. Les votes ne sont pas automatiquement protégés, que ce soit du côté de l'électeur ou du côté du serveur. Des technologies, mécanismes et services de sécurité supplémentaires sont en fait nécessaires pour protéger la confidentialité et l'intégrité des votes avant et après leur transmission sur Internet. Cette condition requise dépend de qui fournit réellement la mise en œuvre du protocole SSL / TLS (à savoir le navigateur ou un utilitaire Java fonctionnant sur une machine virtuelle Java). Il y a donc des risques supplémentaires pour la confidentialité des votes (à savoir des risques d'atteinte à la confidentialité) dans l'ordinateur du votant et dans les serveurs officiels :

- Il y a chez le particulier certains risques supplémentaires d'atteinte à la confidentialité liés à l'utilisation locale d'un *spyware* ou logiciel espion [11].

- Dans le cadre institutionnel, il existe certains risques d'atteinte à la confidentialité qui tiennent au fait que les systèmes et réseaux informatiques sont généralement gérés par des administrateurs à distance (plutôt que par les utilisateurs eux-mêmes). Les outils utilisés par ces personnes pour l'administration à distance peuvent aussi être utilisés pour espionner les activités d'autres utilisateurs.

[10] Le différence fondamentale entre le commerce électronique et le vote électronique est aussi tout à fait justement soulignée dans le document [Gen02].

[11] Un *spyware* est un logiciel qui peut être utilisé pour espionner les activités d'un autre utilisateur (sur le même système ou, ce qui est plus grave, sur un autre système). Un *spyware* très connu est, par exemple, Backorifice2000 (BO2K). De plus amples informations sur BO2K et son code source sont disponibles sur le site http://www.bo2k.com.

Seules quelques approches techniques peuvent être utilisées pour la protection contre l'utilisation (abusive) de logiciels espions et d'outils d'administration à distance. Heureusement, l'utilisation des feuilles de codes présentées au chapitre 5.1 en fait partie.

Sur le plan de la sécurité, les trois possibilités de mise en œuvre du vote par Internet (à savoir le vote par Internet dans les bureaux de vote, le vote par Internet en cabine et le vote à distance par Internet) ont des propriétés et des implications de sécurité très spécifiques. Etant donné que des responsables de la supervision des élections contrôlent les votants, les plates-formes et l'environnement d'utilisation dans le vote par Internet dans les bureaux de vote, la gestion de la sécurité d'un tel système semble réalisable. De même, dans le cas du vote en cabine, le votant et son PC sont sous le contrôle des responsables de la supervision des élections et leur sécurité peut donc être assurée. L'environnement opérationnel peut en outre être modifié comme nécessaire et contrôlé pour remédier aux problèmes de sécurité et de confidentialité (par exemple pour empêcher la coercition ou autres formes d'intervention). La plupart des problèmes de sécurité liés au vote en cabine pourraient donc, tout au moins en principe, être résolus par des extensions de technologies existantes. Mais contrairement au vote par Internet dans les bureaux de vote et en cabine, le vote à distance par Internet continue de poser d'importants problèmes de sécurité et des défis tout à fait nouveaux. Sans contrôle officiel du votant et de sa plate-forme, il existe de nombreux moyens d'utiliser des logiciels malveillants pour manipuler un processus de vote et ses résultats.

Dans ce contexte, la confidentialité des scrutins en général et la protection contre les logiciels malveillants en particulier figurent parmi les principales conditions de sécurité requises pour que le vote à distance par Internet soit utilisé à grande échelle. Ronald L. Rivest [12] a conçu le terme "problème de la sécurité des plates-formes" pour se référer au problème de la protection d'une plate-forme intrinsèquement peu sûre contre les logiciels malveillants et les attaques correspondantes (document [Riv01]).

Beaucoup pensent que le problème de sécurité des plates-formes est le tendon d'Achille de tout processus et système de vote à distance par Internet. Le document [IPI01] soutient par exemple que "les systèmes de vote à distance par Internet posent un risque important pour la confidentialité du processus de vote et ne devraient pas être introduits pour être utilisés dans des élections publiques avant que d'importants problèmes techniques et relevant des sciences

[12] Donald L. Rivest est le co-inventeur du système cryptographique des clés publiques RSA.

sociales ne soient résolus." On retrouve des arguments similaires dans le document [Cal00]. En fait, la plupart des recherches et études parviennent aux conclusions suivantes :

- L'environnement dans lequel opère le vote à distance par Internet crée des problèmes de sécurité très particuliers ;

- Les logiciels dont disposent actuellement les électeurs sont beaucoup trop vulnérables pour être utilisée pour le vote à distance par Internet ;

- Il faut encore quelques dizaines d'années pour mettre au point des technologies de sécurité permettant de résoudre le problème.

Dans ce contexte, la plupart des experts en matière de sécurité soutiennent que le vote par Internet dans les bureaux de vote et le vote par Internet en cabine sont réalisables à moyen terme, tandis que le vote à distance par Internet n'est pas faisable. En se référant à nouveau au document [IPI91] "les technologies actuelles et à court terme sont inappropriées pour traiter ces risques". Par contre, il est souvent soutenu que "toute utilisation d'Internet à des fins de vote devrait être élaborée progressivement" et que le vote par Internet "serait mieux servi par une stratégie évolutive que par un changement révolutionnaire" (document [Cal00]). Ceci signifie au fond qu'il faudrait commencer avec des systèmes de vote par Internet dans les bureaux de vote (phase 1), passer ensuite aux systèmes de vote par Internet en cabine (phase 2) pour parvenir enfin aux systèmes de vote à distance par Internet (phase 3).

Quelques propositions abordent la manière de mettre en œuvre le vote par Internet dans les bureaux de vote en phase 1 :

- Dans une brève note sur le vote par Internet [13] Bruce Schneider a suggéré l'utilisation d'une machine informatique de vote de type « guichet automatique de banque » (ATM : Automatic Teller Machine) installée dans un bureau de vote et imprimant aussi des bulletins de vote. Le votant doit vérifier son bulletin en papier et le déposer ensuite dans une urne scellée. La machine à voter fait le décompte mais les bulletins en papier restent

[13] La note intitulée "Voting and Technology" (vote et technologie) se trouve dans le bulletin d'information Crypto-Gram Newsletter du 15 décembre 2000. Une version en ligne de ce bulletin d'information est disponible à l'adresse http://www.counterpane.com/crypto-gram-0012.html.

les bulletins de vote officiels qui peuvent être finalement utilisés pour procéder à un recomptage.

- De manière similaire, un groupe de chercheurs du California Institute of Technology (CalTech), du Massachusetts Institute of Technology (MIT) et de Compaq a proposé une architecture modulaire pour la mise en œuvre à moyen terme du vote par Internet dans les bureaux de vote (document [BJR01]). L'idée de base est la suivante : les responsables de la supervision des élections distribuent aux électeurs légitimes des bulletins de vote électroniques préparés préalablement et vides, appelés « frogs » [14] pour que ces électeurs votent à distance tout en votant dans leur bureau de vote en déposant leurs frogs. Les appareils de vote dans les bureaux de vote sont manipulés et administrés par les responsables de la supervision des élections et peuvent donc apporter un niveau raisonnable de sécurité. En tant que tels, les votes exprimés peuvent être signés de manière numérique en utilisant les clés privées des appareils. Enfin, les frogs servent de piste de vérification pouvant être utilisées en cas de litige et de recomptage.

Le problème de la sécurité des plates-formes étant connu comme difficile à résoudre, plusieurs projets de recherche et de développement n'essaient même pas de le traiter. Ainsi, à la question "Un virus ou un cheval de Troie peut-il attaquer Cyber Vote ?", on trouve dans la la Foire Aux Questions[15] du projet européen *Cyber Vote*[16] la réponse suivante

> "Oui, comme n'importe quel autre logiciel client dans un paysage informatique de PC peu sûr. Il faut utiliser un logiciel anti-virus et respecter de strictes directives de sécurité pour limiter le risque d'attaque par un virus ou un cheval de Troie. Des techniques sûres d'interface utilisateur peuvent être appliquées à l'électeur du Cyber Vote pour empêcher les chevaux de Troie."

La réponse de la Foire aux Questions ne s'étend pas malheureusement sur ce que recouvre le terme " techniques sûres d'interface utilisateur".

[14] Un « frog » peut être représenté par exemple par une carte mémoire flash "non intelligente" munie d'un dispositif de verrouillage. L'architecture cependant est neutre sur le plan technologique et peut être mise en œuvre en utilisant aussi d'autres technologies.
[15] http://www/eucybervote.org/faq-security.html#q35

En résumé, la communauté scientifique reconnaît que le problème de la sécurité des plates-formes est difficile à résoudre. L'opinion largement répandue selon laquelle il est actuellement impossible de mettre en œuvre, à grande échelle, le vote à distance par Internet de manière suffisamment sûre n'a cependant de sens que si elle s'applique à un cadre ne prévoyant pas le vote par correspondance. L'Etat de Genève ayant mis en œuvre le vote par correspondance depuis une décennie, cette argumentation ne s'applique pas nécessairement. On pourrait en fait soutenir que le niveau de sécurité de tout nouveau système de vote, y compris par exemple le vote par Internet, doit uniquement être comparable au niveau de sécurité du vote par correspondance. Or ce niveau de sécurité semble atteignable.

4. Analyse plus approfondie du problème de la sécurité des postes de travail

Lorsqu'on parle du vote à distance par Internet, on suppose en général que le votant est une application (un programme) fonctionnant sur une plate-forme constituée d'un PC [17] et d'un système d'exploitation de type général comme Windows, UNIX ou Linux. Dans une configuration classique, le PC est celui que l'électeur utilise chez lui (à savoir dans le cadre de son domicile) ou au travail (c'est-à-dire dans le cadre professionnel). En tant que tel, il est administré et utilisé par l'électeur ou une tierce partie agissant au nom de celui-ci.

Les systèmes d'exploitation couramment utilisés sont des progiciels ouverts (c'est-à-dire non fermés)[18]. Les utilisateurs changent couramment les fonctionnalités des systèmes en ajoutant des modules de logiciel comme des mises à jour, des modifications provisoires, des gestionnaires de périphériques, des fichiers de bibliothèque dynamique des liens (DLL) et autres extensions obtenues auprès de sources arbitraires. Les modules de logiciel sont parfois ajoutés au système d'exploitation avec pour effet annexe d'installer ou de mettre à jour un logiciel d'application. Les utilisateurs ignorent en fait souvent que leur système d'exploitation a été changé et ils n'ont certainement aucun moyen d'approuver ou de certifier la sécurité de ces changements. Tout comme des modules de logiciel réguliers, des logiciels malveillants peuvent aussi modifier à volonté un système d'exploitation.

---

[16] http://www/eucybervote.org/

[17] Dans ce rapport, le terme "PC" comprend aussi les assistants personnels de communication (APC) avec les systèmes d'exploitation correspondants.

[18] Noter qu'un progiciel ouvert n'est pas la même chose qu'un système utilisant des logiciels à code source ouvert aux utilisateurs.

Les logiciels d'application comme un navigateur Internet sont conçus de manière encore plus ouverte et peuvent être modifiés plus facilement par l'adjonction de modules logiciels (extensions, utilitaires Java, commandes ActiveX, scripts JavaScript, etc…) [19] Dans de nombreux cas, les modules logiciels sont téléchargés à l'insu de l'utilisateur au moment où il visite un site Web, bien qu'ils aient le pouvoir de modifier les logiciels installés et le comportement de son PC. La presse a maintes fois relaté des exemples d'utilisation abusive de ce pouvoir. Le Chaos Computer Club (CCC) allemand a par exemple démontré en 1997 qu'une commande ActiveX pouvait générer et placer en file d'attente un transfert électronique de fonds en utilisant la version européenne du logiciel Quicken. La commande ActiveX était introduite uniquement à des fins de démonstration et ses développeurs n'ont pas tenté de cacher ses actions. Il est par conséquent possible et très probable que des commandes ActiveX, opérant de manière plus furtive, puissent être écrites et diffusées et être ainsi plus dangereuses. Il en va de même pour tous les langages de programmation et de script actuellement utilisés.

La facilité d'extensibilité du système d'exploitation et des logiciels d'application est extrêmement précieuse pour la souplesse d'adaptation d'un PC. Elle fait partie de ce qui a permis les cycles d'évolution extrêmement rapides de l'industrie informatique. Le danger sous-jacent réside cependant dans le fait que tout module logiciel peut héberger un code malveillant destiné à attaquer un PC depuis l'intérieur. Ken Thompson [20] a par exemple démontré, dans la conférence qu'il a donnée à l'ACM Turing Award en 1984, qu'il est très difficile de détecter un code malveillant dans un élément arbitraire d'une logiciel et qu'aucun examen ou vérification du niveau source, quelle qu'en soit l'ampleur, ne peut changer cela [21]. La raison tient au fait qu'un code malveillant peut être introduit à chaque étape des processus de production, de compilation et d'exécution des logiciels. Un compilateur modifié qui introduit de manière autonome un cheval de Troie dans un logiciel compilé est par exemple très difficile à détecter (et c'est un euphémisme). Thompson a donc conclu que "vous ne pouvez pas vous fier à un code que vous n'avez pas totalement créé vous-même" (document [Tho84]).

[19] Ce type de logiciel est parfois appelé "code mobile". Ce terme n'est pas utilisé dans ce rapport, essentiellement parce que le "code mobile" n'est généralement pas plus mobile qu'un autre code. L'élément caractéristique de ce code est plutôt qu'il est exécuté de manière automatique et transparente chez le client.
[20] Ken Thompson est l'un des développeurs du système d'exploitation UNIX.
[21] Cette déclaration ne sous-entend pas qu'il est inutile d'examiner les codes sources. Cela veut seulement dire que l'inspection des codes sources ne garantit pas que le logiciel concerné ne comporte pas de code malveillant. Une inspection des codes sources donne cependant une impression générale du style de programmation et de ses propriétés dans le domaine de la sécurité.

Or il n'est malheureusement pas possible de créer soi-même tous les codes qui sont nécessaires à l'exploitation d'un PC actuel.

Le même type d'argumentation sur le manque de fiabilité des codes s'applique de toute évidence aux logiciels sous licence et aux logiciels publiés en source ouverte. Il est en fait difficile de dire si un logiciel, dont le code source est ouvert au public, est plus ou moins sûr et fiable qu'un logiciel sous licence. Le simple fait qu'un logiciel soit publié en source ouverte ne signifie pas nécessairement que nombreux seront ceux qui regarderont le code et que ces personnes sont assez qualifiées pour l'examiner. En fait, la plupart des développeurs de logiciels à code source ouvert au public s'intéressent davantage à l'ajout de nouvelles fonctions à une base logicielle existante qu'à l'étude et l'examen approfondis dudit code source. Quoi qu'il en soit, les propriétés de sécurité et de fiabilité d'un module logiciel doivent être étudiées au cas par cas, et cette étude doit être indépendante de son modèle sous licence.

Il existe en outre un théorème fondamental de la théorie de l'informatique selon lequel il ne peut y avoir de test général pour décider si un système et ses logiciels hébergent ou non un code malveillant. [22] Ceci est malheureux et signifie qu'un logiciel anti-virus disponible dans le commerce ne peut détecter et neutraliser que les virus informatiques connus (d'une manière générale, ils analysent des quantités importantes de données pour des schémas de virus informatiques connus). Ils ne peuvent donc rien (ou pas grand chose) contre les virus informatiques inconnus. Il ne faut jamais oublier cela lorsqu'on parle de systèmes d'exploitation et de logiciels d'application supposés "sains".

Tous ces éléments étant pris en compte, il faut admettre que les ordinateurs personnels tels qu'ils sont utilisés aujourd'hui sont des plates-formes dangereuses pour effectuer des opérations devant être sûres. Ceci est vrai pour le commerce électronique et encore davantage pour le vote électronique (les arguments pour lesquels le vote électronique est encore plus critique sur le plan de la sécurité sont énoncés plus haut). Si le vote à distance par Internet était autorisé à partir d'ordinateurs personnels équipés de systèmes d'exploitation et de navigateurs standard, il serait très simple pour un programmateur malintentionné de concevoir un logiciel malveillant, d'amener les électeurs à télécharger ce logiciel (éventuellement sans le

[22] Ce théorème est le corollaire d'un autre énonçant que le problème d'interruption est indécidable. Cela signifie essentiellement qu'il n'existe aucun algorithme pouvant décider pour toutes les machines de Turing possibles et toutes les chaînes d'entrée possibles si une machine de Turing et une chaîne d'entrée données s'arrêtent après un moment défini.

savoir), et de faire en sorte que le logiciel espionne les votes ou les modifie à l'insu du votant. Par conséquent, il faut rendre impossible – ou du moins très difficile – de concevoir un logiciel pouvant faire de telles choses de manière autonome.

5. Approches techniques visant à remédier au problème de la sécurité des plates-formes

Il convient tout d'abord de noter que l'utilisation de la cryptographie n'aide pas à traiter – ni même à résoudre – le problème de la sécurité des plates-formes pour le vote à distance par Internet. Plutôt qu'un problème de cryptographie, la question de la sécurité des plates-formes tient au mode de réalisation et à la mise en œuvre de l'interface entre le votant et un protocole cryptographique de vote. Presque tous les protocoles cryptographiques de vote partent de l'hypothèse qu'un électeur a une base informatique (à savoir une plate-forme) sûre et fiable exécutant sa partie du protocole. Plus précisément, la plate-forme est supposée afficher correctement au votant le vote choisi et soumettre ce vote pendant l'exécution du protocole de vote. La plate-forme est donc supposée agir comme mandataire du votant. En d'autres termes : la plate-forme est le votant pour ce qui est du protocole de vote (document [Riv01]). Même si l'on ajoute une couche supplémentaire de cryptographie, le problème de l'interface appropriée et sûre du votant avec cette nouvelle couche reste à résoudre.
Contrairement au recours à la cryptographie, quelques approches techniques peuvent être utilisées pour remédier au problème de la sécurité des plates-formes pour le vote à distance par Internet. La classification est tirée du document [Cal00] [23] :

1. un système d'exploitation et une application de vote "sains" ;

2. un dispositif spécial de sécurité pour le PC;

3. des dispositifs fermés sûrs ;

4. des systèmes d'exploitation de PC sûrs ;

5. des feuilles de codes ;

6. des scrutins tests ;

7. l'obscurité et la complexité.

Toutes les approches ne sont malheureusement pas réalisables ou applicables techniquement. Leurs avantages et leurs inconvénients sont présentés et commentés brièvement ci-dessous.

5.1 Un système d'exploitation et une application de vote "sains"

Cette approche nécessite du votant qu'il lance son PC à partir d'un CD-ROM (ou support similaire à lecture seule) contenant un système d'exploitation et le logiciel d'application de vote client qui sont supposés être "sains". Le CD-ROM doit être conçu, produit et distribué par l'Etat ou par un représentant digne de confiance de celui-ci.

[23] Tous les termes ne sont pas bien choisis. Ils sont néanmoins utilisés pour des raisons de cohérence.

Il y a fondamentalement deux possibilités pour concevoir l'application de vote client :

1. Le client permet au votant d'utiliser directement Internet pour voter ;

2. L'application permet au votant de remplir et d'authentifier un bulletin. Ce bulletin est ensuite soumis à un serveur d'application à un certain moment ultérieur (pas nécessairement en utilisant le logiciel client d'application de vote).

Dans le premier cas, le CD-ROM doit comprendre un système d'exploitation suffisamment complet, intégrant notamment tout le logiciel de mise en réseau nécessaire pour accéder à Internet. Dans le second cas, le CD-ROM doit comprendre uniquement un petit système d'exploitation ne disposant pas de logiciel de mise en réseau. Dans ce cas, il est cependant nécessaire d'authentifier le bulletin de vote après qu'il a été rempli.. Cette authentification nécessite le calcul d'un code d'authentification de message qui peut être vérifié sur le serveur de vote. Le calcul et la vérification de ce code d'authentification de message nécessitent une clé secrète partagée entre l'application de vote cliente et le serveur. Une telle clé existe sous la forme du code secret dans l'application de vote à distance par Internet de Genève.

Cette approche a pour principal avantage d'obtenir un certain niveau de garantie que le logiciel fonctionnant sur le PC utilisé pour le vote à distance par Internet n'est pas compromis par un logiciel malveillant. Il est toutefois difficile d'évaluer le niveau de garantie, et cela essentiellement parce qu'il est difficile de dire à quel point un système d'exploitation et son logiciel d'application sont réellement "sains". Il est arrivé dans le passé que des vendeurs de logiciels aient expédié des produits qui avaient été infectés par un logiciel malveillant.

Cette approche comporte aussi de nombreux inconvénients. En premier, il est très difficile de concevoir et de produire un CD-ROM à partir duquel la plupart des ordinateurs personnels actuels peuvent être lancés. Il se peut que certains ordinateurs personnels ne puissent même pas être configurés pour être initialisables à partir d'un CD-ROM, et ces ordinateurs doivent être modifiés au niveau du système d'exploitation des entrées/sorties. Ce point dépasse certainement les capacités techniques de nombreux utilisateurs. Le CD-ROM doit par ailleurs être complet et comporter tous les pilotes de périphériques et modules logiciels nécessaires pour utiliser le PC pour le vote à distance par Internet. La quantité de logiciels dépend

principalement de la possibilité choisie parmi les deux énumérées plus haut pour la conception de l'application de vote cliente. Dans le premier cas par exemple, le CD-ROM doit aussi comprendre les pilotes pour la plupart des modems actuellement utilisés, ainsi qu'une mise en œuvre intégrale des protocoles TCP/IP. Du point de vue du votant, le principal inconvénient tient au fait qu'il doit initialiser le PC avant de remplir le bulletin ou de voter. Ceci est peu pratique, voire impossible dans certains cas. Une autre question demeure en suspens, à savoir comment les votants devraient configurer leurs ordinateurs personnels pour la connectivité à Internet dans le premier cas cité plus haut (sans que l'Etat agisse comme un prestataire d'accès à Internet). Enfin - mais ce n'est pas le point le moins important - il est difficile et pas toujours possible de décider, du côté du serveur, si un votant a lancé son PC à partir d'un CD-ROM officiel et s'il utilise le logiciel d'application de vote client à partir du CD-ROM. Notez par exemple que l'application de vote cliente peut (et est très susceptible d'être) un navigateur normal.

En résumé, la distribution et l'utilisation d'un système d'exploitation et d'un logiciel de vote "sains" constituent une approche théoriquement intéressante. Sa mise en œuvre est cependant difficile et coûteuse à un degré prohibitif. A ce titre, elle ne doit pas être considérée dans ce rapport comme une solution viable au problème de la sécurité des plates-formes.

5.2 Installation d'un dispositif spécial de sécurité sur le PC

Cette approche nécessite un dispositif spécial de sécurité relié au PC du votant (par exemple par un port USB). Le but de ce dispositif est d'afficher le bulletin de vote, d'accepter les choix entrés par le votant, d'effectuer ensuite certains calculs cryptographiques et d'envoyer le résultat. Sur ce plan, le vote est intégralement effectué dans le dispositif spécial de sécurité du PC, et l'ordinateur auquel il est connecté sert uniquement d'appareil de connexion à Internet. Ce qui est important pour le dispositif spécial de sécurité, c’est qu'il doit être logiciellement fermé, en d’autres termes que sa base logicielle installée ne puisse pas être modifiée (et donc pas attaquée par un code malveillant).

Le principal avantage de cette approche est le niveau élevé de protection contre les logiciels malveillants et les attaques correspondantes. Le dispositif spécial de sécurité sur le PC ne pouvant être utilisé que pour le vote à distance par Internet, il peut être fermé aux logiciels et extrêmement sûr. L'U.S. Institute for Computer Sciences and Technology avait déjà souligné

ce point en 1988 (document [Sal88]). D'un autre côté cependant, le fait que le dispositif spécial de sécurité sur le PC soit destiné à une seule fin implique qu'il doit être fourni par l'Etat qui organise le vote ou par un représentant légitime de l'Etat. Le principal inconvénient de cette approche réside dans le coût prohibitif de sa diffusion à grande échelle. Elle n'est donc pas retenue comme une solution viable pour la sécurité des plates-formes dans ce rapport.

5.3 Dispositifs fermés sûrs

De même que pour le dispositif spécial de sécurité sur les ordinateurs personnels, il est possible que des dispositifs spéciaux, fermés aux logiciels, pouvant accéder à Internet puissent être développés et diffusés pour les applications de commerce électronique. Si tel était le cas, ces mêmes dispositifs pourraient aussi être utilisés pour le vote à distance par Internet.

A la date de la rédaction de ce rapport, il n'existe aucun dispositif fermé sûr disponible à grande échelle ni susceptible de le devenir bientôt. Cette approche n'est donc pas considérée comme une solution viable dans ce rapport.

5.4 Systèmes d'exploitation de PC sûrs

Cette approche suppose l'existence et le large déploiement de systèmes d'exploitation d'ordinateurs personnels intrinsèquement plus sûrs que ceux actuellement utilisés. Malheureusement, la conception, le développement, la mise en œuvre et la diffusion d'un système d'exploitation de PC sûr sont très difficiles, tant en théorie qu'en pratique. Certains projets de recherche et de développement sont en cours comme la Trusted Computing Platform Alliance (TCPA[24]) ou l'Extremely Reliable Operating System (EROS [25]). Il n'est cependant pas certain que l'un de ces projets aboutisse un jour et que les systèmes d'exploitation en résultant soient utilisés à grande échelle.

Puisqu'ils ne sont actuellement pas disponibles, les systèmes d'exploitation d'ordinateurs personnels sûrs ne sont pas pris en compte comme une solution possible au problème de la sécurité des plates-formes dans ce rapport.

5.5 Feuilles de codes

L'idée est ici d'utiliser des chaînes de caractères semblant aléatoires (représentant des codes ou des numéros de code) pour voter. Cependant, l'utilisation de feuilles de codes nécessite une modification du comportement des électeurs. Le votant saisit un numéro de code au lieu d'inscrire "OUI" ou "NON" (dans le cas d'une votation) ou le nom d'un candidat (pour une

[24] http://www.trustedpc.org/home.home.htm

élection). Tous les numéros de code doivent être distribués sur des feuilles de codes personnalisées et toutes ces feuilles remises de manière confidentielle, par courrier par exemple. Dans les deux cas, les feuilles de codes doivent être fournies indépendamment du PC de l'électeur (à savoir l'ordinateur qu'utilisera l'électeur pour voter). En effet, si les feuilles de codes se trouvaient dans ce PC, un logiciel malveillant pourrait les obtenir et les utiliser pour changer le scrutin. De même, les numéros de code doivent être choisis de manière aléatoire ou pseudo-aléatoire dans un ensemble suffisamment vaste de valeurs possibles pour rendre la probabilité de leur découverte par un logiciel malveillant arbitrairement faible (c'est-à-dire négligeable).
L'utilisation de feuilles de codes pour le vote est parfois aussi appelée "vote par chiffrement" dans les documents techniques (document [Cha01]). Comme nous le verrons par la suite, il existe de nombreuses possibilités de mise en œuvre du vote par chiffrement. Dans une mise en œuvre intégrale par exemple, le serveur peut renvoyer un numéro de vérification au votant qui peut l'utiliser pour vérifier qu'il a bien voté sur un serveur légitime et que le vote a été convenablement enregistré par celui-ci. Elément plus intéressant, il est possible de travailler uniquement avec des numéros de vérification. Les mises en œuvre possibles du vote par chiffrement sont plus traitées de manière plus détaillée au Chapitre 8.

Le principal avantage du vote par chiffrement est de permettre la protection contre les logiciels malveillants sans qu'il soit nécessaire de lancer un PC ou d'installer et configurer un nouveau matériel ou logiciel. Cette approche offre également une protection contre les risques de piratage mentionnés au Chapitre 3. Si un votant saisit un numéro de code (au lieu de "OUI" ou "NON"), toute personne utilisant un logiciel espion ou un outil d'administration à distance est dans l'incapacité de décider si le votant a réellement voté "OUI" ou "NON" (ceci n'est pas vrai pour la mise en œuvre d'un "numéro de vérification seulement"). Une telle personne verrait uniquement un numéro de code semblant aléatoire. D'un autre côté, les principaux inconvénients résident dans la nécessité de distribuer des feuilles de codes personnalisées et dans la modification du comportement des votants.

En résumé, l'utilisation de feuilles de codes est une solution viable pour le problème de sécurité des plates-formes et fait partie de la solution recommandée au Chapitre 7.

5.6 Scrutins tests

[25] http://www.eros-os.org

Cette approche nécessite l'organisation de scrutins tests spéciaux auprès de votants et la vérification systématique de la bonne réception de ces votes par le serveur. Si les scrutins tests sont réalisés de manière statistiquement significative, il sera possible de détecter des attaques, dont certaines peuvent venir de logiciels malveillants. A ce titre, les scrutins tests peuvent aussi être considérés comme un système de détection d'intrusion (SDI) spécialement conçu et utilisé pour le vote à distance par Internet.

Le principal avantage de cette approche est qu'elle fonctionne indépendamment de tout modèle d'attaque et donne une mesure quantitative de l'ampleur de l'attaque détectée. Elle peut aussi être utilisée pour détecter toute cause systématique de perte de bulletins de vote et pas seulement en raison d'attaques par des logiciels malveillants. A l'opposé, le principal inconvénient de cette approche tient au fait que les scrutins tests ne protègent pas des attaques; ils ne font que les détecter *a posteriori*. De ce fait, il est préférable de les utiliser conjointement à une ou plusieurs approches préventives.

Ce rapport considère, comme le rapport du Comité, que le recours à des scrutins tests est une solution viable au problème de la sécurité des plates-formes. Elle fait effectivement partie de la solution recommandée au Chapitre 7.

5.7 Obscurité et complexité

Cette approche (aussi connue sous le nom de "sécurité par l'obscurité" dans les documents techniques), est connue depuis longtemps (mais pas particulièrement comme un succès) dans le domaine de la sécurité informatique. Son principe est que tout ce qui se rapporte au processus de vote (par exemple le format des scrutins électroniques, les éléments internes du logiciel de vote etc.) est tenu secret avant le vote et peut être changé de manière aléatoire pendant le vote lui-même. En outre, tout est en outre rendu le plus complexe possible.

Le principal avantage de cette approche réside dans le fait qu'elle rend la conception de logiciels malveillants difficile et longue. Elle comporte en revanche un inconvénient :il est difficile, voire impossible, de préciser une durée minimale nécessaire pour concevoir un logiciel malveillant. Fait plus ennuyeux, l'histoire a montré que la "sécurité par l'obscurité" fonctionne mal en pratique. Récemment, l'industrie du DVD a appris cette leçon de manière

désagréable[26]. L'obscurité et la complexité ne sont donc pas retenues comme des solutions viables au problème de la sécurité des plates-formes.

6. Analyse du rapport du Comité

En janvier 2002, la chancellerie d'Etat de la République de Genève a publié le rapport final d'un comité[27] nommé pour étudier et évaluer la sécurité d'une application de vote à distance par Internet [Gen02]. Le rapport est parvenu à la conclusion que l'application présentait un niveau raisonnable de sécurité, mais qu'au moins deux problèmes liés à la sécurité devaient être examinés avec soin :

- **Problème de l'authenticité du serveur** : Les utilisateurs d'Internet ne se soucient généralement pas de l'authenticité du serveur et ne vérifient donc pas convenablement les certificats de clés publiques. Ce problème s'applique aussi aux serveurs utilisés pour le vote à distance par Internet.

- **Problème de la sécurité des plates-formes** : les citoyens votant par Internet et leurs plates-formes sont vulnérables aux logiciels malveillants (virus informatiques, chevaux de Troie etc. par exemple) et peuvent donc être attaqués.

Comme solution possible à ces problèmes, le rapport du Comité suggère à l'Etat de Genève de faire distribuer des CD-ROM aux électeurs (Les CD-ROM ont été choisis comme support car ils peuvent être en lecture seule et parce que les lecteurs correspondants sont nombreux parmi les utilisateurs d'Internet). Ces CD-ROM comporteraient le logiciel et les certificats des clés publiques requis pour authentifier le / les serveurs de vote par Internet et voter à distance de manière suffisamment sûre. Il suggère en outre que le logiciel client comporte un mécanisme authentifiant automatiquement le ou les serveurs d'une manière qui soit transparente pour le votant.

Plus précisément, le rapport fait la distinction entre trois approches de configuration et de distribution des CD-ROM (avec des niveaux accrus de sécurité) :

[26] En 1999, Jon Johanson, âgé de 15 ans, a créé le programme DeCSS (DeContents Scramble System) qui lui permettait de voir ses DVD sur un poste Linux. Le DeCSS fait échec au système de protection du droit d'auteur appelé Contents Scramble System (CSS).

[27] Le comité se composait de représentants de l'Etat de Genève, du Conseil Européen pour la Recherche Nucléaire (CERN), de l'hôpital de Genève et de l'Université de Genève.

1. Les CD-ROM comprennent les versions les plus récentes des logiciels standard (à savoir des navigateurs) nécessaires pour participer à un processus de vote à distance. Le logiciel est quant à lui configuré préalablement pour comporter les certificats de clés publiques nécessaires à l'authentification du ou des serveurs de vote.

2. Les CD-ROM comportent le logiciel client spécialement créé pour l'application de vote à distance par Internet de Genève. [28]

3. Similaire à la seconde approche. La condition imposée supplémentaire est que le logiciel client ne puisse être utilisé que dans un contexte minimal et moins vulnérable.

Pour commencer, il est important de noter que ces trois approches semblent identiques mais restent fondamentalement différentes de l'approche technique exposée et commentée au Chapitre 5.1. En fait, l'approche présentée au Chapitre 5.1 nécessite le lancement du PC à partir d'un CD-ROM contenant un système d'exploitation et une application de vote "sains". L'utilisation d'un système d'exploitation "sain" est particulièrement importante pour protéger un logiciel d'application devant opérer de manière sûre et fiable en s'appuyant sur lui. Mais le simple fait d'installer ou de réinstaller un logiciel d'application ne protège pas un PC de logiciels malveillants (notez que le PC peut déjà avoir été contaminé et manipulé au niveau du système d'exploitation). En conséquence, la simple installation ou réinstallation d'un logiciel d'application n'apporte pas de solution viable à la sécurité des plates-formes s'agissant du vote à distance par Internet. Il faut en revanche s'assurer que le PC démarre à partir d'un système d'exploitation qui est supposé "sain", avant que le logiciel d'application en question ne soit installé et exécuté. [29]

Ces remarques préliminaires faites, les approches citées plus haut n'ont un sens que si le PC du votant est lancé à partir du CD-ROM. Selon des propos officieux (conversation personnelle), le comité veut rendre le CD-ROM amorçable. Le rapport du comité n'indique cependant pas explicitement cette intention. Seule la troisième approche peut être interprétée

[28] Pour des raisons non évidentes, le rapport du comité considère que cette approche est similaire à celle adoptée par le secteur financier pour soutenir les opérations bancaires par Internet. La plupart des solutions bancaires pour Internet utilisent toutefois des logiciels clients standard.

[29] Une autre possibilité consisterait à installer à partir de zéro un système d'exploitation. Cette possibilité est toutefois encore moins confortable pour les électeurs. Elle n'est donc pas traitée plus en détail dans ce rapport.

d'une manière exigeant des CD-ROM amorçables (une autre interprétation demanderait l'exécution d'utilitaires Java dans une machine virtuelle Java (MVJ)).

Même si l'une des approches exige que les CD-ROM soient amorçables, ces approches comporteraient toujours les inconvénients exposés au Chapitre 5.1, lesquels l'emportent nettement sur les avantages. En conséquence, la distribution de CD-ROM ne peut pas être recommandée. Sur un plan pratique, les deuxième et troisième approches sont encore moins bonnes car elles impliquent que l'Etat devienne développeur et éditeur de logiciels.

7. Recommandations

Il faut tout d'abord souligner que la communauté scientifique reconnaît que le problème de la sécurité des plates-formes est difficile à résoudre. L'opinion largement répandue selon laquelle il est actuellement impossible de mettre en œuvre, à grande échelle, le vote à distance par Internet de manière suffisamment sûre n'a cependant de sens que si elle s'applique à un cadre ne prévoyant pas le vote par correspondance. L'Etat de Genève ayant mis en œuvre le vote par correspondance depuis une décennie, cette argumentation ne s'applique pas nécessairement. On pourrait en fait soutenir que le niveau de sécurité de tout nouveau système de vote, y compris par exemple le vote par Internet, doit uniquement être comparable au niveau de sécurité du vote par correspondance. Or ce niveau de sécurité semble atteignable.

Il est recommandé de traiter le problème de la sécurité des plates-formes par l'utilisation combinée de feuilles de codes et d'urnes tests (au lieu de la distribution de CD-ROM par l'Etat)[30]. L'utilisation de feuilles de codes est particulièrement adaptée à l'application de vote à distance par Internet de Genève car des cartes de vote personnalisées doivent de toute manière être fournies aux électeurs. Les cartes de vote sont envoyées par courrier. Chaque envoi par courrier peut donc aussi comporter une feuille de codes en plus de la carte de vote. Les feuilles de codes présentent l'avantage majeur de pouvoir servir à traiter les deux problèmes cités plus haut (à savoir l'authenticité du serveur et la sécurité des plates-formes). Il est en outre recommandé que les numéros de code comportent des redondances (c'est-à-dire des totaux de vérification) pour détecter des erreurs lorsqu'un votant saisi un chiffre erroné.

[30] Si des CD-ROM sont distribués, il est vivement recommandé de les rendre amorçables, comme exposé au chapitre précédent.

Certaines mises en œuvre possibles du vote par chiffrement sont présentées et commentées succinctement au Chapitre 8. Les explications sont uniquement destinées à éclaircir les idées de base. Avant de lancer un projet correspondant, il est recommandé de procéder à une étude de marché et de rechercher des sociétés qui ont développé et commercialisent des technologies de vote par chiffrement. Une enquête préliminaire a par exemple trouvé une société appelée SureVote [31]. SureVote a été fondée par le docteur David Chaum qui possède une très vaste expérience des technologies de l'anonymat et de l'amélioration de la confidentialité sur Internet [32]. La technologie mise au point par SureVote est brevetée dans de nombreux pays (dont la Suisse) (document [PCT01]).

8. Mises en œuvre possibles

On dispose d'au moins trois manières d'implémenter le vote par chiffrement à Genève. Il est par exemple possible de recourir aux numéros de code et numéros de vérification (ce qui représente une mise en oeuvre complète). On peut aussi utiliser soit les numéros de code seulement (c'est-à-dire la mise en oeuvre "numéros de code seulement") soit les numéros de vérification (mise en oeuvre "numéros de vérification seulement"). Ces possibilités sont présentées et commentées brièvement plus loin.

8.1 Remarques préliminaires

Le vote par chiffrement utilise des numéros de code et des numéros de vérification. Les numéros n'ont pas besoin d'être longs ; leur longueur doit rendre suffisamment faible la probabilité de deviner convenablement un numéro. Par exemple : si le numéro comporte 10 chiffres binaires (bits), la probabilité de deviner un numéro est de $1/2^{10} = 1 / {}^{1'024} = 0.000975562 \approx 0{,}01$ %. Ceci semble suffisant puisque les numéros ne peuvent pas être vérifiés hors ligne. 10 bits peuvent être représentés par des chiffres décimaux $\log 2^{10} = \log 2^{1'024}$ ce qui est légèrement supérieur à 3 chiffres. Par conséquent, 4 chiffres décimaux peuvent être utilisés pour encoder un numéro de code et une certaine redondance pour déceler des erreurs [33].

[31] http://www.sure-vote.com

[32] David Chaum est par exemple l'inventeur d'un système de signature aveugle qui est largement utilisé pour la mise en œuvre des mouvements d'espèces numériques anonymes. Avant de créer SureVote, David Chaum avait fondé et dirigé la société néerlandaise DigiCash pour commercialiser cette technologie.

Il existe de nombreuses possibilités de générer des numéros à 10 bits. On peut, par exemple, utiliser une fonction algorithmique (*hash*) unidirectionnelle et tronquer les résultats en 10 bits [34]. Dans la suite, le terme *h(K, M)* est utilisé pour se référer au résultat d'une fonction algorithmique unidirectionnelle saisie pour le message *M* (*h* est une fonction algorithmique unidirectionnelle et *K* est une clé secrète). Ce résultat représente un code d'authentification de message (MAC). Les documents techniques comportent de nombreuses propositions de calcul et de vérification des MAC (par exemple la construction HMAC comme spécifiée dans le document [KBC97]).

Pour mettre en œuvre le vote par chiffrement on prend pour hypothèse qu'il y a une ou deux clés cryptographiques indépendantes et sans rapport (à savoir K_1 et K_2) pour chaque processus de vote. Les clés doivent être choisies de manière aléatoire et gardées secrètes (c'est-à-dire que seul le ou les serveurs de vote doivent y avoir accès). Il est en outre supposé que la chaîne *M* se réfère à la concaténation du numéro de référence pour le vote et du numéro de référence pour la carte de vote. Dans ce cas, le numéro de code pour le *choix* (le *choix* étant "OUI" ou "NON") dans le cas d'une votation, et le nom d'un candidat dans le cas d'une élection) peut être calculé comme *trunc(h(K_1,M | choix*), et le numéro de vérification peut être calculé comme *trunc(h(K_2,M | choix*)). Dans chaque cas, | se rapporte à la concaténation et *trunc* à une fonction qui tronque l'argument à une longueur spécifique. Pour les numéros de code (numéros de vérification), la longueur est de 10 bits (13 bits). Pour les numéros de code, 3 bits de redondance sont ajoutés pour lui permettre de détecter des erreurs. Les votants n'étant pas tenus de saisir les numéros de vérification, l'utilisation de la redondance pour détecter les erreurs n'est pas nécessaire pour ces numéros.

8.2 Mise en oeuvre intégrale

Dans le cas d'une mise en oeuvre intégrale, chaque votant reçoit une carte de vote personnalisée et un bulletin de vote par courrier. La carte de vote se compose des deux parties suivantes : [35]

[33] Le plan de redondance n'est pas plus amplement traité dans ce rapport.
[34] Noter que les fonctions hash donnent généralement des valeurs hash comportant 128 (MD5) ou 160 nombres binaires (SHA-1) et que ces valeurs peuvent être représentées en 32 ou 40 caractères hexadécimaux.
[35] La carte peut être conçue de manière à pouvoir être séparée en deux avant que le vote n'ait lieu.

- Une partie comprend la *carte de vote* qui est semblable à celle utilisée jusqu'ici. Elle comporte les quatre éléments suivants :
    - un numéro de référence pour le vote
    - un numéro de référence pour la carte de vote
    - un code secret
    - un code de vérification du serveur.

  Le numéro de référence pour la carte de vote est déjà défini et se compose de 12 chiffres décimaux (les chiffres sont séparés en trois groupes de quatre chiffres chacun). De même, le code secret existe déjà et se compose de 6 caractères alphanumériques. Le code secret est caché et doit être gratté par le votant. En plus du numéro de référence pour la carte de vote et le code secret, la carte de vote comprend un numéro de référence pour le vote et un code de vérification du serveur. La date du vote (sous une certaine forme définie) peut être utilisée pour référencer le vote et une autre chaîne constituée de 6 caractères alphanumériques peut servir de code de vérification du serveur. Tout comme le numéro de référence de la carte de vote et le code secret, le code de vérification du serveur est unique pour chaque votant. Il est recommandé d'utiliser le même jeu de caractères pour encoder le code de vérification du serveur et le code secret. Contrairement au code secret, le code de vérification du serveur n'a pas besoin d'être caché et ne doit pas être gratté par le votant.

- L'autre partie comprend la feuille de codes qui est utilisée pour voter effectivement sur Internet. Pour chaque question, la feuille de codes doit comporter les éléments suivants :

  - un numéro de code pour voter "OUI" ;

  - un numéro de code pour voter "NON" ;

  - un numéro de vérification pour voter "OUI" ;

  - un numéro de vérification pour voter "NON".

  Comme cela a été abordé dans les remarques préliminaires, chaque numéro de code ou de vérification comprend 4 chiffres décimaux (par exemple 3567).

Si un votant décide de voter au bureau de vote ou par correspondance, il détache de la carte de vote la partie correspondant à la feuille de codes et détruit cette dernière.[36] Si toutefois le votant décide de voter sur Internet, il doit s'identifier auprès du serveur de vote en utilisant son numéro de référence pour la carte de vote. Il doit ensuite utiliser la feuille de codes pour traduire ses réponses (à savoir "OUI" ou "NON") dans les numéros de code correspondants et vérifier les numéros de vérification que renvoie en conséquence le serveur. Le serveur enregistre les réponses codées dans une base de données. Si le votant est certain de vouloir voter, il appuie sur un bouton correspondant et s'identifie à l'aide du code secret. Pour s'assurer qu'il est connecté à un serveur de vote véritable, le votant doit aussi contrôler le code de vérification du serveur qui lui est renvoyé par ce dernier. Ce code doit correspondre au code de vérification du serveur inscrit sur la carte de vote. (Notez que cette vérification est complémentaire et doit être effectuée en plus de l'identification du serveur qui utilise les certificats de clés publiques).

8.3 Mise en oeuvre du "Numéro de code seulement"

Si l'on ne se soucie pas trop du problème de l'authenticité du serveur, on peut aussi travailler uniquement avec des numéros de code. Dans ce cas cependant, il est recommandé que le votant vérifie le certificat de clé publique fourni par le serveur de vote.

8.4 Mise en oeuvre du "Numéro de vérification seulement"

Cette mise en oeuvre fonctionne aussi avec les numéros de vérification seulement. Dans ce cas, le votant ne doit pas saisir de numéro de code pour chaque question, mais inscrit "OUI" ou "NON" (ou clique sur une case correspondante) et le serveur renvoie le numéro de vérification. [37] Ici encore, le votant doit vérifier ce numéro.

D'un point de vue fonctionnel, cette mise en oeuvre semble équivalente à la mise en oeuvre intégrale, à deux différences près :

1. Dans une mise en oeuvre "Numéro de vérification seulement", le votant utilise une interface classique pour voter. Ceci signifie en fait qu'il lui est demandé de cliquer dans des cases. Les numéros de vérification sont renvoyés au votant qui doit les vérifier

[36] Cette mesure n'est pas critique sur le plan de la sécurité.

manuellement. Il n'y a malheureusement aucun moyen technique d'automatiser cette vérification manuelle. Si l'on ne se soucie pas de l'authenticité du serveur, il n'y a aucune possibilité de déterminer la survenue d'un événement malveillant. Il faut noter que ceci diffère de l'utilisation de numéros de code (où le votant doit saisir un numéro de code et où il n'est pas possible d'ignorer le nouveau mode de vote).

2. L'utilisation de numéros de code assure la confidentialité des votes même en présence d'un logiciel espion et d'outils d'administration à distance. La mise en oeuvre d'un "Numéro de vérification seulement" n'apporte de toute évidence pas ce niveau de confidentialité (car il n'utilise pas de numéros de code).

Ces différences devraient être soigneusement prises en considération avant d'opter pour une mise en oeuvre "Numéro de vérification seulement".

8.5 Stratégie évolutive

Les variantes présentées ci-dessus comportent des avantages et des inconvénients. Sur le plan de la sécurité, la mise en oeuvre intégrale est préférée. Une mise en oeuvre "Numéro de code seulement" n'est pas très logique car elle ne simplifie pas beaucoup les choses. En revanche, une mise en oeuvre "Numéro de vérification seulement" simplifie le comportement de l'utilisateur et semble être une bonne option pour le vote par chiffrement.

Il existe en fait une stratégie évolutive qui commence par la mise en oeuvre "Numéro de vérification seulement" et aboutit à la mise en oeuvre intégrale. Une telle stratégie peut être recommandée pour Genève. Dans ce cas cependant, les urnes tests deviennent encore plus importantes (pour détecter toute anomalie).

9. Questions en suspens et travail futur

Quelques questions doivent encore être résolues avant que le vote par chiffrement puisse être mis en œuvre et utilisé dans à Genève.

[37] Relevons à ce stade qu'il est important que les numéros de vérification pour "OUI" et "NON" soient distincts.

Premièrement, il faut vérifier si le vote par chiffrement tel qu'il est présenté dans le rapport est légalement accepté en Suisse et dans le canton de Genève[38].

- Deuxièmement, les notes préliminaires concernant les différentes mises en œuvre possibles (présentées au Chapitre 8) doivent être développées et étendues à la manière de mettre en place et d'utiliser de manière sûre le vote par chiffrement dans l'Etat de Genève.

- Troisièmement, le vote par chiffrement implique aussi une modification du comportement du votant. Au lieu d'inscrire "OUI" ou "NON" ou de cocher simplement la case correspondante, il doit saisir un numéro de code et/ou vérifier un autre numéro renvoyé par le serveur. C'est une habitude à prendre qui doit être traitée en conséquence. Ceci signifie essentiellement que les études sur le terrain doivent montrer si cette modification du comportement du votant est bien comprise par les électeurs et acceptée en pratique.[39]

Il faut répondre à la première question avant de se consacrer à quelque degré que ce soit aux deux autres.

En tout état de cause, le niveau de garantie de la sécurité de l'application du vote par Internet doit être augmenté autant que faire se peut. Ceci nécessite une conception ouverte et une discussion libre, ainsi que des examens et des vérifications par des pairs. Toutefois, cela n'implique pas d'étudier tous les codes sources, ni de publier les logiciels en divulguant leur code source.

[38] Il faut noter qu'en utilisant le vote par chiffrement, un votant n'inscrit ni "OUI" ni "NON", il clique simplement dans la case correspondante. Le votant doit saisir un numéro de code semblant aléatoire dans une zone faisant partie d'une interface graphique utilisateur (GUI). C'est une nouveauté et il faut vérifier qu'elle est conforme au cadre légal. Ceci doit être vérifié séparément pour chaque mise en œuvre possible.

[39] Dans ce contexte, il est important de noter que tout nouveau processus ou procédure démocratique (par exemple le vote à distance par Internet) garantit un niveau extrêmement élevé de sécurité mais que les mesures de sécurité mises en place ne peuvent pas être lourdes pour les votants au point de les décourager d'y participer.

A. Acronymes et abréviations

ACM	Association for Computing Machinery
ATM	= GAB – guichet automatique de banque
BIOS	= BIOS – système d'exploitation des entrées/sorties
BO2K	Backorifice 2000
CCC	Chaos Computer Club
CD	= CD - disque compact
CSS	DeContents Scramble System
DeCSS	DeContents Scramble System
DLL	= DLL – bibliothèque dynamique des liens
CERN	Conseil Européen pour la Recherche Nucléaire
DVD	= DVD
EFT	= TEF - Transfert électronique de fonds
EROS	Extremely Reliable Operating System
FAQ	Foire aux questions
GUI	= GUI – Interface graphique utilisateur
HMAC	Code d'authentification de messages hash
IDS	= SDI – Système de détection d'intrusion
IFIP	International Federation for Information Processing
IT	TI – Technologie de l'information, informatique
JVM	= MVJ – machine virtuelle Java
MAC	Code d'authentification de message
PC	Ordinateur personnel
PCT	= PCT – Traité de Coopération en matière de Brevets
PDA	= APC – Assistant personnel de communication
PIN	= PIN – Numéro personnel d'identification
ROM	= ROM – en lecture seule
RSA	Rivest, Shamir et Adleman
SSL	Secure Sockets Layers = couche de prises sécurisées
TC	= CT – Comité Technique
TCPA	Trusted Computing Platform Alliance
TLS	Transport Layer Security – Sécurité de la couche transport
U.S.	Etats-Unis
WG	Groupe de travail

B Références

[**BJR01]** Shuki Bruck, David Jefferson et Ronald L. Rivest, "A Modular Voting Architecture*" Proceedings of the Workshop on Trustworthy Elections (W0TE '01)*, août 2001
http://www.theory.lcs.mit.edu¯rivest/BruckJeffersonRivest-AmodularVotingArchitecture-doc.pdf

[Cal00] California Secretary of State, California Internet Voting Task Force, Rapport final, janvier 2000
http://www.ss.ca.gov/executive/ivote/

[Cha01] David Chaum, "Sure Vote: Technical Overview". *" Proceedings of the Workshop on Trustworthy Elections (W0TE '01)*, diapositives de présentation, août 2001
http://www.vote.caltech.edu/wote01/pdfs/surevote.pdf

[GeN02] Chancellerie d'Etat de Genève, Rapport du Comité Sécurité sur l'application de vote par Internet, Janvier 2002.
http://www.geneve.ch/chancellerie/E-Gouvernment/data/rapport_securite_internet.pdf

[Hir01] Martin Hirt, *Multi-party Computation : Efficient Protocols, General Adversaries, and Voting*, Thèse de doctorat, ETH Zurich, Retirage en tant que Vol. 3 de la Série de l'ETH sur la sécurité de l'information et la cryptographie, Hartung-Gorre Verlag, Constance, ISBN 3-89649-747-2, 2001.

[IPI01] Internet Policy Institute, Report of the National Workshop on Internet Voting: Issues and Research Agenda, Mars 2001.
http://www.internetpolicy.org/research/e_voting_report.pdf/

[KBC07] Hugo Krawezyk, Mihir Bellare et Ran Canetti, "HMAC: Keyed-Hashing for Message Authentification", Request for Comments 2104, février 1997.
http://sunsite.cnlab-switch.ch/ftp/doc/standard/rfc/21xx/2104

[Opp00] Rolf Oppliger, *Security Technologies for the World Wide Web*[39], Artech House, Norwood, MA, ISBN 1-58053-045-1, 2000
http://www.esecurity.ch/Books/wwwsec.html

[Opp02] Rolf Oppliger, *Internet and Intranet Security, Second Edition*, Artech House, Norwood, MA, ISBN 1-58053-166-0, 2002
http://www.esecurity.ch/Books/iis2e.html

[PCT01] David Chaum, *Physical and Digital Secret Ballot System*, brevet international publié sous le Traité de coopération en matière de brevets (PCT), WO 01/55940 A1, 2 août 2001.

[Riv01] Ronald L. Rivest, "Electronic Voting", *Proceedings of Financial Cryptography '01*, février 2001.

[39] Une seconde édition de ce livre sera publiée en 2003.

http://theory.lcs.mit.edu/~rivest/Rivest-ElectronicVoting.pdf

[Rub01] Aviel D. Rubin, "Security Considerations for Remote Electronic Voting over the Internet", *Proceedings of the 29th Research Conference on Communication, Information and Internet Policy (TPRC2001)*, octobre 2001
http://avirubin.com/e-voting.security.html

[Sal88] Roy G. Saltman, "Accuracy, Integrity and Security in Computerized Vote-Tallying", Institute for Computer Sciences aand Technology, NBS Special Publication 500-158, Gaithersburg, MD, août 1988.
http://www.itl.nist.gov/lab/specpubs/500-158.htm

[Sch00] Berry Schoenmakers, "Fully Auditable Electronic Secret-Ballot Elections", *Xootic Magazine*, juillet 2000, vol. 8, n° 1
http://www.win.tue/nl/xootic/magazine/jul-2000/schoenmakers.pdf

[Tho84] Ken Thompson, "Reflections on Trusting Trust", *Communications of the ACM*, Vol. 27, n° 8, août 1984, pp. 761-763
http://www.acm.org/classics/sep95/

C Sites Web

- CalTech-MIT Voting Technology Project
  http://www.vote.caltech.edu
- Election.com
  http://election.com
- ETH Zürich E-Voting Project
  http://www.crypto.ethz.ch/research/sdc/vote/
- Euroopean Cyber Vote Project
  http://www.eucybervote.org
- MIT Electronic Voting Bibliography
  http://theory.lcs.mit.edu/~cis/voting/greenstadt-voting-bibliography.html
- Site Web de Rebecca Mercuri sur le vote électronique
  http://www.notablesoftware.com/evote.html
- SureVote
  http://www.sure-vote.com
- Université d'Osnabrück, Groupe de recherches "Internetwahlen"
  http://www.internetwahlen.de
- VoteHere
  http://votehere.com
- Workshop on Trustworthy Elections 2001 (WOTE '01)
  http://www.vote.caltech/edu/wote01/

D A propos de l'auteur

Rolf Oppliger est titulaire d'une maîtrise (1991) et d'un doctorat (1993) en informatique de l'Université de Berne et du venia legendi (1999) de l'Université de Zurich. Il est enseigne à l'Université de Zürich et donne de temps à autre des cours dans d'autres universités et écoles polytechniques de Suisse et d'Allemagne. Il a fondé eSECURITY Technologies Rolf Oppliger (http://www.esecurity.ch) en 1999 pour fournir des services de conseil, d'éducation et d'ingénierie scientifiques dans le domaine de la sécurité informatique. Il travaille par ailleurs pour l'Unité de Stratégie Fédérale Suisse pour l'Informatique et est actuellement rédacteur en chef de la série Computer Security Series, publiée par Artech House. Il a publié neuf livres[40] et de nombreuses communications scientifiques, articles et rapports traitant essentiellement de la sécurité. Il est membre de l'ACM, de l'IEEE Computer Society et de l'IFIP TC 11 WG 4 sur la sécurité des réseaux.

[40] Deux livres sont cités dans ce rapport.