Rapport sur la Sécurité du vote électronique

25 juin 2015

Résumé

Les machines à voter, utilisées par plusieurs pays pour les élections, sont des systèmes embarqués devant garantir des propriétés de sécurité importantes. Cette étude portera sur l'état de l'art de la sécurité matérielle et logicielle de ces équipements, ainsi que sur les vulnérabilités découvertes.

Il est important de préciser que cette étude ne porte que sur les systèmes réputés sûrs, utilisés lors d'élections majeurs et fortement contrôlés. Nous laisserons volontairement de côté tous les autres systèmes comme le principe du vote en ligne ou les boîtiers utilisés dans des situations moins sensibles (assemblée générale de copropriétaires, etc...).

1 Un enjeu de société

1.1 Partisans et détracteurs

Les avantages souvent mis en avant sont :
- la rapidité de délibération,
- le moindre de coût supposé (pas d'impression des bulletins)
- dans le cas d'un vote à distance, la possibilité de voter plus facilement (votants handicapés et/ou ne pouvant pas se rendre sur le lieu de vote).

Les détracteurs, eux, insistent sur :
- Le manque d'ergonomie et le risque d'erreurs.
- le manque de fiabilité des dispositifs entraînant la perte de certaines voix.
- la vulnérabilité des dispositifs électroniques face à une attaque physique ou informatique.
- l'opacité technique des solutions utilisées.

1.2 Peu d'études sérieuses disponibles

Ceci est en grande partie dû au fait que l'ensemble du dispositif est tenu secret. Depuis l'architecture matérielle jusqu'aux comptes rendus de certifications de ces systèmes, en passant bien sûr par le code source des logiciels embarqués, aucune de ces informations n'est normalement disponible au public. Conscient du danger, de nombreux groupes d'activistes s'organisent dans le monde pour dénoncer cette opacité. On citera par exemple Le Chaos Computer Club (CCC) en Allemagne, La "Verified Voting Foundation" ou la "Black Box Voting organisation" aux Etats-Unis.

Il ne fait aucun doute que c'est ce manque de transparence qui est finalement responsable des conclusions accablantes auxquelles arrivent les chercheurs qui réussissent à obtenir des machines de ce type pour les décortiquer sérieusement (et démontrer qu'il est possible de les reprogrammer pour tricher). On s'intéressera tout particulièrement à trois modèles de machines à voter : La NEDAP ES3B[1], assez représentative, et dont une variante est utilisée en France. Les Diebold AccuVote-TS qui sont massivement utilisées aux Etats-Unis[2]. Et les EVMs, très utilisées en Inde[3]. On notera au passage que, pour cette dernière étude, la personne ayant reçu la machine de vote fut arrêtée par la police.[4].

Bien que ces études, et leurs conclusions accablantes, aient presque dix ans, nous verrons que des systèmes plus récents peuvent être encore moins sécurisés !

1.3 La situation française

Pour avoir une vision globale de la situation, on pourra s'intéresser à cette publication de 2006[5], qui propose une analyse des enjeux économiques, politiques et industriels posés par ces systèmes de vote, ainsi qu'un bon résumé des problèmes rencontrés dans d'autres pays ayant adopté le vote électronique avant nous.

Depuis cette publication, beaucoup de choses ont évolué car de nombreuses personnes dénoncent ces systèmes de vote. On citera par exemple l'association "Ordinateur-de-vote-org" qui a obtenu, suite à une action en justice, quatre pages (seulement) du cahier d'agrément des machines NEDAP. Le parti pirate de son côté tente de faire purement et simplement interdire le vote électronique.[6] Ils sont loin d'être les seuls, de nombreux projets de lois étant régulièrement déposés à cette fin.[7][8].

La situation actuelle est en effet très ambiguë. Ainsi, depuis le moratoire de 2007, plus aucune commune n'est autorisée à basculer du mode papier au mode électronique. Mais les communes qui avaient déjà obtenu cet accord, une soixantaine environ, peuvent continuer d'avoir recours à ces machines. Comme dans les autres pays, l'ensemble du système est particulièrement opaque et les documents officiels disponibles sur le sujet sont rares. On citera tout de même le "règlement technique fixant les conditions d'agrément des machines à voter"[9], un document qui donne la liste des fonctionnalités que ces systèmes doivent fournir, mais qui devient extrêmement vague dès qu'il aborde les problématiques de sécurité.[10]

1.4 Beaucoup de problèmes constatés

Enfin, avant de parler de sécurité informatique et de fraudes volontaires, le nombre d'anomalies rencontrées quelles qu'en soient les causes doit être signalé. En effet, ce nombre est trop important pour que ce type de système puisse inspirer confiance dans un avenir proche. En conséquence, plusieurs communes ont fait marche arrière[11], quand ce ne sont pas des pays entiers[12]. On pourrait aussi citer le cas des Etats-Unis[13] et de beaucoup d'autres pays.

2 Le cas de la NEDAP ES3B

L'activiste hollandais Rop Gonggrijp est l'une des personnes dont le nom revient le plus souvent lorsqu'on s'intéresse à l'analyse de ces machines. Il s'est fait connaître pour avoir activement participé à plusieurs études, et à l'interdiction des machines à voter aux Pays-Bas. Ses conclusions sont sans appels. Ces systèmes ne devraient pas être utilisés pour le vote, car leur sécurité est largement insuffisante. Quiconque dispose d'un accès à ces machines peut rapidement les modifier avec toutes les conséquences que l'on peut imaginer.

2.1 Protection matérielle

Commençons par nous intéresser au matériel. L'une des première mesure de sécurité que l'on observe est la présence de serrure. Il faut en effet, lors du processus de vote, utiliser une clef pour ouvrir et fermer le scrutin. La clef utilisée, la même sur toutes les machines de vote, est une C&K YL Series 4 Tumbler Camlock notée A126. Autrement dit une clef si basique, qu'un simple trombone pourrait la remplacer. Mais, à environ un euro la clef, pourquoi s'ennuyer avec un trombone ? Rop Gonggrijp a fait le test et en a commandé une centaine qu'il a reçu sans soucis. Cette clef peut donc difficilement être considérée comme un mécanisme de sécurité efficace.

Concernant les composants, nous sommes vraiment très loin des standards actuels. Inutile de chercher des PUFs, des mécanismes de chiffrement, (secure boot...) ou quoi que ce soit de compliqué. L'électronique embarquée date en effet des années 1980, et cet ordinateur ressemble donc beaucoup

aux anciens micro-ordinateurs. Plus précisément, ce système s'architecture autour d'un processeur 68000, de 256KB d'EPROM, de 8 KB d'EEPROM et de 16 KB de Ram (ainsi que deux ports séries et un port parallèle). Ces composants sont non seulement standards, mais aussi facilement échangeables, car montés sur socket. Il n'y a donc aucune protection particulière, et modifier le programme se fait simplement en échangeant la ROM d'origine avec une nouvelle (ou un émulateur).

Les mécanismes de protection ne concernent pas directement la sécurité, mais plutôt la tolérance aux pannes. En effet, Rop Gonggrijp et son équipe ont constaté que les informations stockées étaient largement redondantes. C'est une véritable protection en cas de coupure de courant, mais cela ne protège pas contre la fraude.

Un autre problème se pose. Sans modifier quoi que ce soit à l'intérieur de cette machine, aucune précaution n'a été prise pour l'empêcher d'émettre des rayonnements électromagnétiques lors de son fonctionnement. Or l'écoute et l'analyse de ces rayonnements peut permettre de déterminer ce qui s'affiche sur l'écran LCD (4 lignes de 40 colonnes) et donc de déterminer qui vote pour qui.

2.2 Protection physique

Puisque toute personne ayant un accès physique à la machine de vote est potentiellement en mesure de la reprogrammer, on peut se demander quels sont les précautions prises pour vérifier que personne n'a modifié quoi que ce soit. Le lieu de stockage de ces machines est il sécurisé ? Comment est assuré leur transport ? Y a t-il des sceaux physiques placés sur l'appareil pour empécher de l'ouvrir sans laisser de traces ? Rien de tout cela. N'importe qui peut ouvrir la machine avec un simple tournevis et remplacer la Rom pour installer le programme de son choix.

2.3 Protection logicielle

La seule véritable "protection" est l'absence de documentation technique disponible. L'équipe de chercheurs a donc du étudier ce système pendant plusieurs semaines avant d'en comprendre le fonctionnement et de pouvoir le reprogrammer.

2.4 Conclusion

On peut parfaitement comprendre le choix d'utiliser d'anciennes technologies. Elles sont peu coûteuses et fiables. Un critère important (et peut être la seule chose qui soit réellement vérifiée par les organismes de certification). On peut difficilement comprendre en revanche qu'il soit aussi facile de modifier la programmation de ces machines sans que cela ne soit détectable.

3 Le cas de la Diebold AccuVote-TS

3.1 Protection matérielle

Le démontage de cette machine (ou l'ouverture de la trappe donnant accès à deux emplacement PC Card) ne pose pas de problème particulier. La clef utilisée est un modèle simple, facilement copiable. Il est aussi possible d'ouvrir entièrement la machine avec un tournevis pour les personnes qui n'auraient ni clef, ni compétence en crochetage. L'architecture matérielle ressemble beaucoup à un PC portable sous Windows CE. La carte mère comprend un processeur RISC à 133 MHz, 32 MB de RAM, 16 MB de flash et une EPROM de 128 KB. A part les protections "environnementales" (batterie de secours), rien ne semble avoir été prévu pour contrer d'éventuelles tentatives de fraude.

3.2 Protection logicielle

L'étude réalisée ne fait mention d'aucune protection d'aucune sorte. Il s'agit simplement d'un Windows CE un peu modifié pour ne lancer que le logiciel de vote par défaut. Avant cela, pendant la phase de boot, cette machine vérifie qu'une carte mémoire n'a pas été insérée avec une mise à jour à installer.

Cette vérification ne fait appel à aucune forme de signature, et teste simplement la présence de fichiers nommés fboot.nb0 pour la mise à jour du bootloader, ou nk.bin pour la mise à jour (remplacement) de l'OS actuellement installé par celui qui se trouve sur la carte.

Ainsi attaquer cette machine revient simplement à insérer une carte contenant une version modifiée du système puis de la démarrer. Mieux, il est alors possible d'insérer un virus dans le système, virus qui se copiera automatiquement sur n'importe quelle carte insérée dans la machine (transfert de configurations de votes, mise à jour...), avant de s'installer, toujours automatiquement et silencieusement, sur des machines qui ne seraient pas encore infectées.

3.3 Conclusion

Cette machine, qui utilise des composants plus récents que la précédente et véritable système d'exploitation, est en réalité beaucoup plus facilement modifiable que la précédente.

4 Le cas des machines indiennes (EVMs)

En 2004, les machines à voter EVM ont été utilisées en Inde pour les éléections législatives. Ce choix a été motivé d'une part, par la nature particulière de la population indienne qui est une des plus importante au monde (plus de 800 millions de personnes) et d'autre part par le fait que chaque citoyen, ne disposant pas automatiquement de papier physique d'identité, est identifié et authentifié par des caractères biométriques.

Bien que les spécifications techniques des EVMs soient confidentielles, certains éléments ont fuité et ont fait l'objet d'une analyse de sécurité[3].

4.1 Protection matérielle

Un premier point problématique est le stockage du firmware sur une mémoire non volatile mais non accessible à la lecture depuis l'extérieur : aucune vérification de l'intégrité du firmware livré avec la machines n'est possible.

Le design simple de la machines est très facile à comprendre et en fait une cible potentielle pour un faussaire : Durant son étude, Hari Prasad a construit une réplique de machine à voter EVM. Il en a, en outre implémenté deux attaques matérielles :

— la première a consisté à insérer un afficheur 7-segments doté d'un micro-contrôleur remplaçant l'afficheur légitime, chargé d'afficher les résultats : le contrôleur embarqué, piloté par un smartphone sur bluetooth, permet d'altérer l'affichage des votes, et de compromettre la sincérité du scrutin.

— la seconde est la réalisation d'un PCB altérant les EEPROM stockant les votes : le dispositif se clipse sur les EEPROM, calcule le nombre de votes à voler, et, en fonction d'un interrupteur physique, ré-ecrit l'EEPROM avec des voix débitées à tous les candidats sauf au candidat privilégié qui lui, sera crédité des votes désrobés. Cette attaque repose sur le manque de protection matérielle sérieuse empêchant la ré-écriture des EEPROMs stockant les résultats.

L'accès physique de la machine est sensé être protégé par un sceau sous forme d'autocollant, et se rompt lorsque le boitier est ouvert. Néanmoins, ANDREW W. APPEL a prouvé que ces sceaux pouvaient être retirés avec un simple pistolet à chaleur[14].

4.2 Protection logicielle

L'étude réalisée dispose de peu d'éléments sur la sécurité logicielle : En effet, le code source est tenu secret, et la source ayant fourni l'EVM étudiée a souhaité qu'elle reste fonctionnelle, ce qui interdit toute extraction du firmware par des techniques intrusives etc)

Un point marquant au niveau de la sécurité logicielle de cette machine est que le firmware est intégré en dur dans le CPU, et ne peut être modifié : L'intérêt de cette technique est que l'installation d'un firmware malveillant est impossible , mais cela empêche également toute mise à jour de sécurité.

En outre, le nombre de bulletin n'est pas chiffré, ni signé.

Enfin, une dernière protection purement fonctionnelle est mise en place : le firmware ne tolère que 5 votes par minute, ce qui est sensé empêcher, de façon dérisoire, que des organisateurs du scrutin puissent ajouter massivement de faux votes en peu de temps.

4.3 Conclusion

L'EVM, disposant d'une conception simplifiée, en fait une machine très peu chère, et résistante à des conditions d'utilisation extrême. Néanmoins, ce faible coût est incompatible avec la mise en place de mesures de sécurité evoluées.

5 Et il y a pire...

Dans ces trois exemples, il est nécessaire qu'au moins une personne ait accès physiquement à la machine qu'il souhaite modifier (ou à une carte mémoire qui sera utilisée pour configurer le vote dans le cas de la Diebold). Mais existe t-il des systèmes de vote encore plus vulnérables ? Des systèmes qu'il serait possible d'attaquer à distance ? Malheureusement, la réponse est oui[15]. Par exemple en Virginie ou des systèmes incroyablement vulnérables étaient encore utilisés cette année. Nous parlons ici de machines sous windows XP qui n'avaient pas étés mis à jour depuis 2004. De machines équipés de cartes Wifi configurés en WEP. De machines dont le mot de passe administrateur était "admin" et dont la clef WEP était "abcde". Des machines directement connectées à Internet sans la moindre protection d'aucune sorte. Attaquer ces systèmes se limitait donc à se connecter, à trouver puis récupérer la base de données contenant l'ensemble des votes au format Microsoft Access, à les modifier comme on le souhaitait et à ré-uploader le fichier sur la machine. Confrontée à l'évidence, la commission électorale de Virginie n'a pas eu d'autre choix que de mettre fin à la certification dont bénéficiaient ces machines depuis de longues années.

6 Le futur

De nombreuses recherches sont en cours pour concevoir et normaliser des techniques fiables, garantissant l'honnêteté des votes, et permettant à chaque citoyen de vérifier que son vote à été correctement pris en compte. On citera par exemple les travaux du français Frédéric Connes[16][17], ou ceux de Melanie Volkamer[18]. Beaucoup de cryptologues s'intéressent aussi de près au sujet, certains très connus comme Ronald Rivest[19]. Mais dans l'immédiat, il ne semble pas exister de systèmes parfaits : Ergonomiques, transparents et totalement inattaquables. Le vote électronique impose aujourd'hui de faire confiance à autrui, ce qui semble difficilement compatible avec le principe même du vote.

Références

[1] Willem-Jan Hengeveld Rop Gonggrijp. Nedap/groenendaal es3b voting computer, a security analysis. http://wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf, octobre 2006.

[2] Edward W.Felten Ariel J.Feldman, J.Alex Halderman. Security analysis of the diebold accuvote-ts voting machine. http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/pub/ts06full.pdf, Septembre 2006.

[3] Rop Gonggrijp Hari K. Prasad, J.Alex Halderman. Security analysis of india's electronic voting machines. https://indiaevm.org/evm_tr2010-jul29.pdf, Juillet 2010.

[4] Christophe Auffray. Un chercheur en détention pour avoir audité la sécurité d'une machine de vote électronique. *zdnet.fr*, Aout 2010.

[5] Chantal Enguehard. Le vote électronique en france : opaque et invérifiable. http://pagesperso.lina.univ-nantes.fr/info/perso/permanents/enguehard/perso/RI_halshs-00085041.pdf, Decembre 2006.

[6] Emilien Ercolani. Le parti pirate veut interdire le vote électronique. *linformaticien.com*, Juillet 2012.

[7] Xavier Berne. Un sénateur dépose une loi pour interdire les machines à voter. *NextImpact*, Juillet 2014.

[8] Xavier Berne. Un député dépose une loi interdisant les machines à voter. *NextImpact*, Janvier 2015.

[9] Règlement technique fixant les conditions d'agrément des machines à voter. http://www.interieur.gouv.fr/content/download/1775/18612/file/reglement_technique_machine_voter.pdf, Novembre 2003.

[10] Chantal Enguehard. La sécurité des machines à voter n'est pas vérifiée : c'est prévu ! *agoravox.fr*, Avril 2007.

[11] Elise Vincent. Les machines à voter maintenues dans 77 communes. *LeMonde.fr*, Mai 2007.

[12] rikiai. L'irlande abandonne le vote électronique. *lefigaro.fr*, Juillet 2012.

[13] lexpress.fr. Elections américaines : la sécurité du vote électronique en question. *lexpress.fr*, Novembre 2012.

[14] A. W. Appel. Certification of decembrer 1. https://indiaevm.org/evm_tr2010-jul29.pdf, 2008.

[15] Dan Goodin. Meet the e-voting machine so easy to hack, it will take your breath away. *arstechnica.com*, Avril 2015.

[16] Frédéric Connes. La sécurité des systèmes de vote. Master's thesis, Université Panthéon-Assas (Paris-II), 2009. http ://www.fconnes.org/fr/publications.php.

[17] Frédéric Connes. A simple e-voting protocol. http://www.fconnes.org/docs/evoting_protocol.pdf, Aout 2008.

[18] Melanie Volkamer. *Evaluation of Electronic Voting*. Springer Science and Business Media, 2009.

[19] Ronald L. Rivest. The threeballot voting system. https://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf, Octobre 2006.