L’élection américaine sous surveillance

Partage international n° 194 – Octobre 2004

Interview de Andy Stephenson par Monte Leach

Lors de l’élection américaine de novembre 2004, environ 80 % des votes s’effectueront par le biais d’un système électronique. Les trois grands fabriquants de ces machines – Diebold, Sequoia et ES&S – sont des sociétés privées dont la technologie a été critiquée pour insuffisances de protections contre la fraude et les défaillances techniques. L’année dernière, Bev Harris, une grand-mère de 52 ans, a trouvé sur Internet les programmes secrets de la machine à voter Deibold et les a rendus publics. Après avoir examiné ces logiciels, des informaticiens ont affirmé qu’ils contenaient des « erreurs flagrantes », qui restent toujours à corriger. B. Harris a aussi découvert un répertoire du nom de « rob-Georgia » (arracher la Géorgie) contenant des instructions destinées à remplacer les fichiers du scrutin juste avant les élections de novembre 2002. On sait qu’un retournement inattendu se produisit cette année là : le candidat républicain au siège de sénateur de Georgie remporta la victoire, donnant ainsi le contrôle du Sénat aux républicains.
Bev Harris a créé l’association « Black Box Voting », et avec son associé, Andy Stephenson, ils se chargent de contrôler les machines à voter, aux Etats-Unis. Ils recherchent les erreurs dans les systèmes, fournissant des manuels de sécurité aux surveillants des bureaux de vote et faisant connaître aussi largement que possible les problèmes informatiques relatifs aux scrutins électroniques et leurs solutions.

Monte Leach a interviewé Andy Stephenson directeur de Black Box Voting *pour* Partage international.

Partage international : *Quels genre de problèmes avez-vous découverts sur les machines à voter, aux Etats-Unis ?*
Andy Stephenson : Les machines à écran tactile qui vont être utilisées par des millions d’électeurs en novembre posent vraiment un problème. Elles ne produisent aucun enregistrement physique du vote, si bien que les électeurs n’ont aucun moyen de vérifier que leur voix est bien comptabilisée comme prévu. Mais plus inquiétant encore, nous avons découvert que le logiciel utilisé par Diebold était très vulnérable aux attaques. Les appareils à écran tactile ou à scanner optique de Diebold comptabiliseront 30 % des voix à la prochaine échéance. Le centralisateur – un ordinateur où tous les votes sont transmis et comptés – est très vulnérable. Les votes peuvent êtres modifiés en moins de 90 secondes.

PI. *Comment serait-ce possible ?*
AS. Par exemple, dans le comté de King (Etat de Washington), là où j’habite, on utilise un système par scanner optique. L’électeur coche la case face au nom du candidat, et transmet l’information par l’intermédiaire d’un lecteur optique à un ordinateur qui comptabilise les voix. A la fin de la journée, les votes sont envoyés par modem vers un ordinateur central. Dans le comté de King, il existe 48 modems connectés à l’ordinateur central, soit 48 portes ouvertes à quiconque connaîtrait le numéro de téléphone pour s’introduire dans le système.
Nous avons plus de 500 bureaux de vote dans ce comté, chacun avec un ou deux employés connaissant ce numéro de téléphone. Pour le comté de King, mille personnes peuvent donc appeler l’ordinateur central et se connecter à l’aide d’un portable équipé d’un modem ou même d’un téléphone cellulaire. Ils ont alors libre accès à tout le système et peuvent effectuer tous les changements qu’ils souhaitent. Ils peuvent lancer un programme de cinq lignes, un script Visual Basic, qui fonctionne sur les systèmes Windows. Quiconque ayant des rudiments de programmation peut changer le résultat du scrutin. On estime que dans tous les pays, 100 000 personnes disposent des connaissances nécessaires pour modifier le système.
Pourquoi quelqu’un irait-il s’ennuyer avec les 4 000 ou 5 000 machines à voter, alors qu’il suffit de se connecter à l’ordinateur central et de changer les résultats sans laisser de traces ? Et si vous laissez des traces, vous pouvez entrer dans le système et les effacer sans problème.

PI. *Que faire pour prévenir le problème ?*
AS. Il existe des parades. Mais récemment en Californie, nous nous sommes entretenus avec des responsables du scrutin. Nous leur avons communiqué des procédures simples pour réduire les risques. Et voici leur réponse : *« Nous ne ferons rien avant la prochaine élection. »*

PI : *Quelles protections recommandez-vous ?*
AS. Nous voulons qu’il n’existe aucun lien avec le

centralisateur. Ni ligne téléphonique, ni modem, ni communication sans fil ou via Internet. Aucune communication avec l'ordinateur centralisateur ne devrait être autorisée à quiconque. Tous les bulletins devraient être acheminés depuis le bureau de vote vers l'ordinateur centralisateur et comptés en central. Ainsi, personne ne disposerait d'un accès externe à cette machine de comptage.
De plus, tout système de vote devrait fournir un bulletin sur lequel l'électeur pourrait contrôler son vote. Ce papier devrait valoir preuve absolue de l'enregistrement de l'élection. Il devrait être l'arbitre final.
De plus, les résultats de chaque machine devraient être imprimés deux fois à la fin de la journée. Une copie serait affichée dans la circonscription électorale pour que le public puisse vérifier que le comté a enregistré correctement le résultat de son bureau de vote.

PI. *Existe-t-il des problèmes sur les machines à voter fabriquées par d'autres constructeurs ?*
AS. Oui. Les machines Sequoia utilisent Visio, un produit Microsoft. Un simple programme Visual Basic peut intervertir les commandes : faire en sorte qu'en touchant « Oui » à l'écran, le système enregistre « Non ». Les programmeurs de Sequoia, ou quiconque ayant accès au système avant le scrutin, pourrait introduire ce programme.

PI. *Le public peut-il y faire quelque chose ?*
AS. Les gens devraient s'engager et travailler pour les élections, devenir inspecteur ou juge de scrutin. Le jour des élections, dans un bureau de vote, si quelque chose ne parait pas clair, il y a probablement un problème. Vous pouvez alors contacter notre organisation. Nous aurons 800 bénévoles disponibles, et des listes de personnes à contacter si quelque chose vous semble bizarre. Prenez contact avec nous, et nous prendrons toute action appropriée, comme par exemple avertir la presse ou intervenir auprès d'autres personnes.

PI. *A quoi doivent prendre garde ceux qui s'engagent comme bénévoles ?*
AS. Si vous voyez un employé de Diebold qui connecte un portable à une machine à voter, cela peut être un problème.
Par exemple, lors des primaires du 2 mars 2004, dans le comté de Riversid, Californie, on a vu un employé de Sequoia rencontrer un de ses collègues à l'extérieur d'un bureau de vote. *« Voici ma carte personnelle,* lui a-t-il dit. *Entrons et voyons si elle marche. »* Il entra et stoppa le comptage des votes. Il introduisit sa carte, intervint sur la base de données, retira sa carte, puis se rendit à l'aéroport et rentra au Colorado. C'était une violation manifeste de la loi californienne.

PI. *Les Etats ou la nation s'efforcent-ils de changer les choses ?*
AS. En dehors de « Black Box Voting », il existe des groupes à travers le pays qui travaillent à cela. L'association « True Majority » travaille sur les traces papier.

PI. *Quel conseil donneriez-vous pour conclure ?*
AS. Inscrivez vous et votez. Et pour davantage d'informations, visitez notre site : blackboxvoting.org.

Etats-Unis **Auteur** : Monte Leach, journaliste radio indépendant et éditeur de la revue Share International pour les Etats-Unis, il réside à San Francisco.
Thématiques : politique
Rubrique : Entretien ()