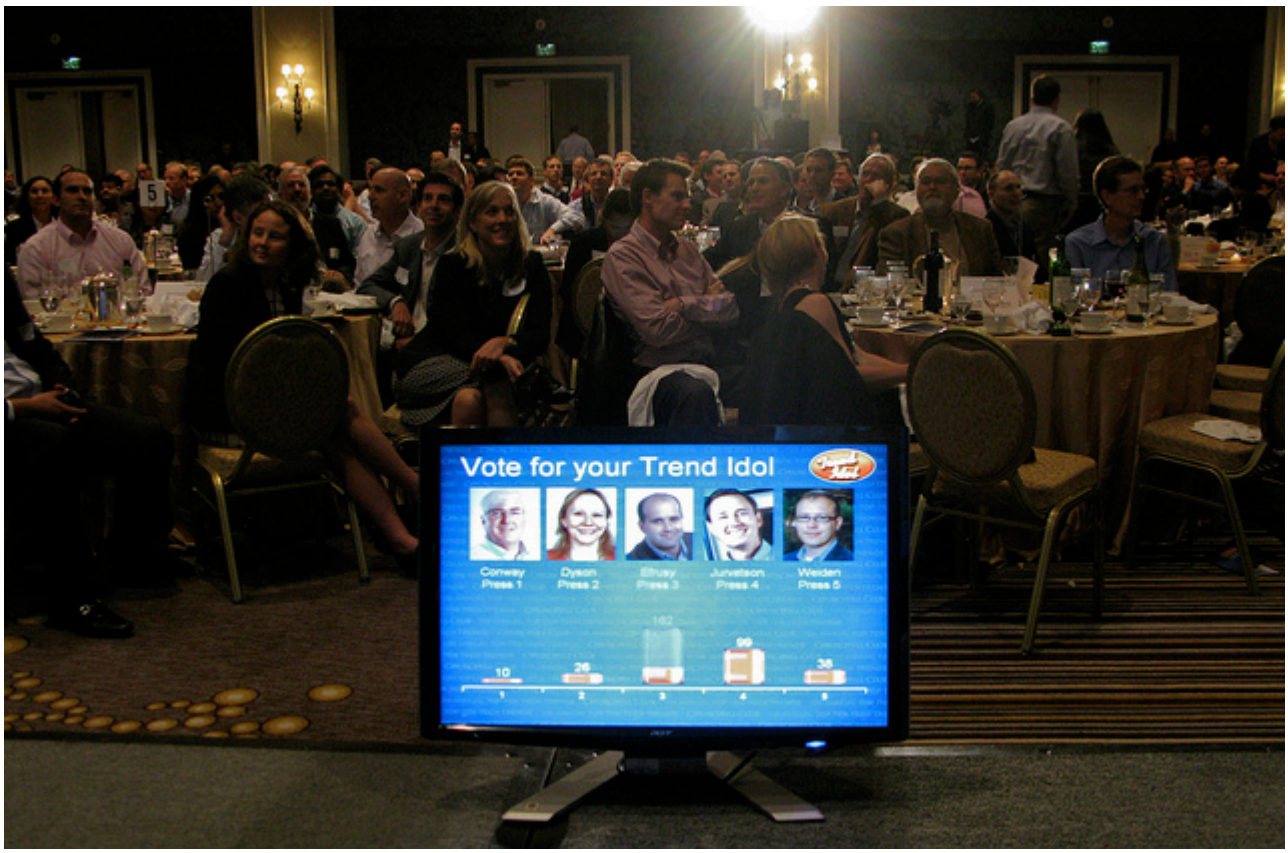
Hacker le vote électronique américain ? Un jeu d'enfants !

Nous imaginant technophiles béats, les gens sont souvent surpris de la prise de position de la grande majorité des partisans du logiciel libre en défaveur du vote électronique (quand bien même on ait accès au code source qui pilote la machine et le processus, ce qui semble être du bon sens mais non partagé).

Ce n'est pas l'expérience ci-dessous, au moment même où se déroulent les élections présidentielles américaines, qui risque de nous faire changer d'avis.



Comment j'ai hacké une machine de vote électronique

Roger Johnston (raconté par Suzanne LaBarre) – 5 novembre 2012 – PopSci.com
(Traduction : Zii, ehsavoie, plink, KoS, aKa, lgodard, MF, Ag3m, greygjhart)

How I Hacked An Electronic Voting Machine

De quoi avez-vous besoin pour truquer une élection ? Des connaissances basiques

en électronique et 30 dollars d'équipement de RadioShack suffisent, révèle le hackeur professionnel Roger Johnston. La bonne nouvelle : nous pouvons empêcher cela.

> *Roger Johnston est à la tête de la « Vulnerability Assessment Team » au Laboratoire National d'Argonne. Récemment, lui et ses collègues ont lancé une attaque de sécurité sur des machines de vote électronique pour montrer la facilité déconcertante avec laquelle quelqu'un peut trafiquer les votes. Encore plus surprenant : les versions de ces ordinateurs seront présentes dans les bureaux de vote de toute l'Amérique ce mardi. Le magazine Harper a rapporté recemment que l'écran tactile Diebold Accuvote-TSX va être utilisé par plus de vingt-six millions de votants dans ving États et que l'ordinateur de vote à bouton pressoirs Sequoia AVC va être utilisée par presque neuf millions de votants dans quatre États. Dans cet article, Johnston révèle comment il a hacké ces machines — et que c'est à la portée du premier venu, du lycéen à la grand-mère de 80 ans.*

La Vulnerability Assessment Team du Laboratoire National d'Argonne scrute une large variété d'équipements électroniques — serrures, sceaux, tags, contrôle d'accès, biometrie, sécurité des cargaisons, sécurité nucléaire — pour tenter de trouver des vulnérabilités et repérer des solutions potentielles. Malheureusement, on n'alloue pas assez de budget à l'analyse de la sécurité des élections dans ce pays. Alors nous nous sommes penchés dessus, histoire de nous occuper, un samedi après-midi.

On appelle cela une attaque de l'homme du milieu. C'est une attaque classique sur les appareils de sécurité. On implante un microprocesseur ou un autre appareil électronique dans la machine de vote, et cela vous permet de contrôler le vote et de tricher ou non. Basiquement, on interfère avec la transmission de l'intention du votant.

Nous avons utilisé un analyseur logique. La communication digitale est une série de zéros et de uns. Le voltage augmente, diminue. Un analyseur logique rassemble les voltages oscillants entre haut et bas et vous présentera ensuite les données digitales dans une variété de formats. Mais il y a plein de manières de

faire. Vous pouvez utiliser un analyseur logique, un microprocesseur, un ordinateur — en gros, n'importe quoi qui vous permette de voir l'information qui est échangée et ensuite vous laisse comprendre ce qu'il faut faire pour imiter l'information.

Nous avons donc espionné les communications entre le votant et la machine. Dans un cas, le votant appuie sur des boutons (c'est une machine à voter avec des boutons poussoirs) et dans l'autre, il interagit avec un écran tactile. Puis, nous avons écouté les communications entre le logiciel de la machine et le votant. Disons que je veux que Jones gagne l'élection, et que vous votez pour Smith. Alors, mon microprocesseur va dire à la machine de voter pour Jones si vous essayez de voter pour Smith. Mais si vous votez pour Jones, je n'interviendrai pas dans les communications. Parfois on bloque les communications, parfois on les déforme, parfois on ne fait que les regarder et les laisser passer. C'est ça l'idée. Deviner quels sont les échanges en cours, puis les modifier si besoin est, y compris ce qui sera présenté au votant.

Nous pouvons faire ceci car la plupart des machines, autant que je sache, ne sont pas chiffrées. C'est simplement un format de communication standard. Il est donc très simple de deviner les informations échangées. N'importe quelle personne qui fait de l'électronique numérique — un amateur ou un fan d'électronique — peut le deviner.

Le dispositif que nous avons intégré dans la machine à écran tactile valait en gros 10 $. Si vous voulez une version de luxe où vous pouvez le contrôler à distance jusqu'à environ 800 mètres, il vous en coutera 26 $. Ce n'est pas très cher. Vous pouvez trouver ça chez RadioShack. Je suis allé à des salons scientifiques dans des lycées où les gosses avait des projets avec des processeurs plus sophistiqués que ceux nécessaires pour truquer ces machines.

Parce qu'il n'y a pas de financements pour ce genre de tests de sécurité, il faut compter sur des gens qui achètent des machines d'occasion sur eBay (dans ce cas l'écran tactile Diebold Accuvote TS Electronic Voting Machine et la machine à boutons Sequoia AVC Advantage Voting Machine). Ces deux machines étaient un peu vieilles, et nous n'avions pas de manuel ou de schéma de circuits. Mais, dans le cas du Sequoia AVC, nous avons deviné comment elle marchait en moins de deux heures. En deux heures nous avions une attaque viable. L'autre machine nous a pris un peu plus de temps car nous ne comprenions pas comment

l’affichage sur un écran tactile fonctionnait. Nous avons dû donc apprendre, mais ce n’était qu’une question de jours. C’est un peu comme un tour de magie, vous devez le pratiquer beaucoup. Si nous avions pratiqué longtemps, voir mieux, si quelqu’un de très bon avait pratiqué pendant deux semaines, nous aurions mis 15 à 60 secondes pour exécuter ces attaques.

Les attaques nécessitent un accès physique à la machine. C’est facile pour les personnes en interne qui les programment pour une election ou les installent. Et nous pouvons supposer que ce n’est pas si difficile pour des personnes extérieures. Beaucoup de machines à voter gisent dans la cave de l’église, le gymnase ou le préau de l’école élémentaire, sans surveillance pendant une semaine ou deux avant l’election. Généralement elles ont des serrures très bon marché que n’importe qui peut ouvrir ; quelquefois elles n’en ont même aucune. Personne ne s’identifie auprès des machines quand il prend son poste. Personne n’est chargé de les surveiller. Leurs scellés ne sont pas si différents des dispositifs anti-fraude sur les paquets de nourriture et les médicaments en libre service. Falsifier un produit alimentaire ou un médicament, vous pensez que c’est difficile ? Ça ne l’est vraiment pas. Et un grand nombre de nos juges d’élections sont de petites vieilles à la retraite, et, Dieu les garde, c’est grâce à elles que les élections marchent, mais elles ne sont pas forcement fabuleusement efficaces pour détecter des attaques subtiles de sécurité.

Formez les personnels chargés de la vérification des scellés, et ils auront une chance de détecter une attaque raisonnablement sophistiquée. Faites des vérifications sur les personnes en interne et cette menace sera bien moins sérieuse. Dans l’ensemble il manque une bonne culture de la sécurité. Nous avons beau avoir des machines de vote avec des défauts, avec une bonne culture de la sécurité nous pouvons avoir des élections sans fraude. D’un autre côté, on peut avoir des machines fabuleuses, mais sans une culture de la sécurité à la hauteur, cela ne servira à rien. Il faut vraiment prendre du recul. Notre point de vue est qu’il sera toujours difficile d’arrêter un James Bond. Mais je veux faire avancer les choses jusqu’à un niveau où au moins ma grand-mère ne puisse pas truquer les élections, et nous en sommes encore loin.

Crédit photo : Steve Jurvetson (Creative Commons By)