Failles confirmées dans des machines de vote électronique

Publié le vendredi 3 août 2007
Voir en ligne : https://www.france-science.org/Failles-confirmees-dans-des.html

A la demande de Debra Bowen, Secrétaire d'Etat de Californie, un rapport sur la sécurité des systèmes de vote électronique aux Etats-Unis a été rendu public le 30 juillet dernier. Il en ressort que trois machines très largement utilisées présentent des failles de sécurité, de fiabilité ou d'intégrité. Les tests ont été menés par l'équipe Red Team, composée d'experts de l'université de Californie.

Les machines incriminées (Diebold's GEMS 1.18.24/AccuVote, Hart Intercivic System 6.2.1 et Sequoia's WinEDS version 3.1.012/Edge/Insight/400-C) utilisent toutes des mécanismes d'écrans tactiles ou à touches pour l'enregistrement du vote. La Sénateur Diane Feinstein rebondit sur cette étude pour appuyer les récentes tentatives du groupe démocrate qui visent à rendre obligatoire l'ajout d'imprimantes sur ces machines et à promouvoir les systèmes équipés de scanners pour lire les bulletins (voir "Difficulté pour trouver un consensus sur le vote électronique", BE Etats-Unis 88 http://www.bulletins-electroniques.com/actualites/43864.htm).

Au même moment sur la côte Est des Etats-Unis, le Secrétaire d'Etat de Floride Kurt Browning vient de recevoir le 27 Juillet dernier une étude commandée auprès du laboratoire Security and Assurance in Information Technology (SAIT) de l'université de Floride. Ce document révèle 14 failles suite au processus de certification des nouvelles machines Diebold Accuvote OS et TSx qui devront être utilisées dans l'état. La plupart des problèmes relevés sont liés à la mauvaise utilisation des technologies de cryptographie autour de la sécurisation des données. Par exemple, sur les 2048 bits de la clé RSA utilisée dans la machine, seuls les premiers 160 bits sont vérifiés. Kurt Browning a demandé au constructeur Diebold de corriger ces failles sous 3 semaines sous peine de changer de système de vote pour les prochaines élections. Bien que des observateurs aient fait remarquer que ces tests ont été menés dans des conditions de laboratoire difficiles à reproduire dans le cadre d'un isoloir, il a été démontré que certains modèles de machines Diebold peuvent être ouverts avec des clés dupliquées à partir d'images trouvées sur Internet.

Il ne faut toutefois pas généraliser le résultat de ces rapports à l'ensemble des Etats-Unis, et encore moins aux systèmes de vote électronique utilisés dans d'autres pays. Des experts s'accordent à penser que les machines à voter américaines souffrent de problèmes de conception majeurs induits par une législation différente dans chacun des 50 états. Les constructeurs doivent donc mettre au point autant de machines et de logiciels au point, compliquant le processus de validation des équipements.

Source :

- What the U.S. Is Doing Wrong with E-Voting, 30 Juillet 2007 : http://www.eweek.com/article2/0,1895,2164289,00.asp
- Florida voting chief aims to block hackers, 1 Août 2007 : http://www.miamiherald.com/news/florida/story/188769.html
- Senate to Hold Hearing on Security of Voting Machines, 31 Juillet 2007 : http://blog.wired.com/27bstroke6/2007/07/senate-to-hold-.html

Pour en savoir plus, contacts :

- "Overview of Red Team Reports", University of California : http://sos.ca.gov/elections/voting_systems/ttbr/red_overview.pdf
- Lettre du Secrétaire d'Etat de Floride Kurt Browning à David Byrd, Président de Diebold Election Systems, 31 Juillet 2007 : http://election.dos.state.fl.us/pdf/SAITbrowningLetter.pdf
- "Difficulté pour trouver un consensus sur le vote électronique", BE Etats-Unis 88 : http://www.bulletins-electroniques.com/actualites/43864.htm

- "La fiabilité du vote électronique en question ", BE Etats-Unis 85 : http://www.bulletins-electroniques.com/actualites/43864.htm
Code brève
ADIT : 50660

Rédacteur :

Vincent Reboul deputy-stic.mst@ambafrance-us.org