

Analyse succincte du processus de vote électronique

Par Jean Charles Delépine, UPJV

Le vote électronique s'est terminé il y a peu de temps, son résultat n'a que peu d'importance mais le Président de l'Université nous promettait un vote sécurisé et fiable. La fiabilité est impossible, on le sait déjà (lire ou relire http://www.agoravox.fr/article.php?id_article=53919 pour s'en assurer).

Voici donc une petite analyse, peu poussée et en vrac, visant l'ergonomie et la sécurité du processus utilisé. C'est forcément un peu long, lisez ou sautez à la conclusion.

Curieux de nature (on ne devient pas informaticien pour rien) j'ai regardé un étudiant aller jusqu'au moment où il pourrait voter (ce qu'il n'a pas fait, je vous rassure).

L'étudiant s'est naturellement rendu sur le site de l'université et a cliqué sur la ligne clignotante "vous avez reçu un mail" il a donc été redirigé vers le webmail étudiant, ... et n'y a pas trouvé de mails intéressants...
Il fait en effet partie des quelques étudiants qui ont fait rediriger leurs mails vers leur boîte personnelle (en l'occurrence gmail, personne n'est parfait).

Je lui fait remarquer et nous allons donc sur gmail, je vois immédiatement le mail en question, mais l'étudiant le cherche pendant quelques minutes : l'adresse de l'expéditeur est en effet fort mal choisie et le champ commentaire (le Jean Charles Delépine que vous voyez dans la ligne "De:" de ce mail) est inexistant contrairement à tout les bons usages. L'étudiant ignore donc naturellement ce mail comme il ignore tout les spams sans même regarder leur sujet, mieux choisi lui. Je ne l'aide pas (mais je lui dis que j'ai vu le mail), il fini par l'ouvrir.

Pour la petite histoire, quelques étudiants ont écrit à cette adresse, ils ont reçus en retour un message sybillin dont voici un extrait :

```
Original-recipient: rfc822;depomail@jedepose.com
Final-recipient: rfc822;depomail%jedepose.com@ims-ms-daemon
Action: failed
Status: 5.2.2 (Over quota)
```

Ce message indique que la boîte mail utilisée par cette société est pleine. Ils ont donc envoyé plusieurs milliers de mails mais n'ont pas su provisionner un espace suffisant pour accepter de recevoir des réponses à leurs mails !

Merci à la présidence de contacter ces personnes, certainement quelques gus dans un garage, et de leur proposer mes services. Huissier c'est un métier, le mail en est un autre. J'ai à proposer un contrat professionnel pour un prix très avantageux.

À mes lecteurs, n'utilisez cette société pour rien de plus confidentiel que des cartes postales, on va le voir.

Dans le premier mail, donc, nous avons un identifiant, le mail est non crypté, lu via une connexion à gmail elle même non cryptée, le tout à travers une connexion wifi... autant dire que cet identifiant est distribué à qui le veut bien.

Il nous faut un deuxième mail, il est du même accabit. Nous avons donc notre identifiant et notre code, mais nous ne sommes potentiellement pas les seuls.

Étudiants (et personnels) imprudents, on ne le répètera jamais assez, ne lisez votre mail qu'avec une connexion sécurisée ! Si votre client mail ou votre fournisseur ne le permettent pas, changez en !

Bref. Nous cliquons tout de même sur le lien proposé dans ce mail.

Mauvaise surprise ! La connexion vers le mail certifié par la société jedepose.com n'est pas sécurisée elle non plus ! Deuxième chance pour le potentiel vilain de récupérer les codes voulus ainsi que le mail confidentiel conservé par cette société !

Pire : si le mail avait été lu depuis une connexion sécurisée, pas de chance, les informations sensibles que nous avons protégées sont ici divulguées !

Recueillir ces informations est un jeu d'enfant, les outils existent sous tous les systèmes et sont très connus. Pas besoin d'être informaticien pour les connaître, juste être curieux et savoir cliquer.

Passons encore et continuons.

Tout ceci nous amène à un site qui lui, on ne l'espérait plus, est sécurisé : <http://www.jevoteenligne.com/vote/u-picardie/>

Les spécialistes vont me dire, que c'est du http pas du https, donc que non, ce n'est pas sécurisé ! J'ai repris ce lien sur le site de l'UPJV, pas dans le mail, dans le mail le liens est bien en https, et la société a visiblement l'habitude de ses clients, la connexion http est immédiatement transformée en https. Merci à eux, on a peut-être enfin affaire à des pros. Mais le vers est déjà dans le fruit.

Arrêtons nous un peu sur ce site.

Il s'agit d'un site de la société EXTELIA dont voici un extrait la pub :

Parmi les clients de cette société nous retrouvons :

Conseil de Prud'hommes
Conseil Général du Val d'Oise
Direction Générale des Impôts
Ministère des Affaires Etrangères
Ministère de l'Emploi, de la Cohésion Sociale et du Logement
SNCF (on y reviendra)

Voici un extrait de la publicité de cette entreprise :

Extelia est l'unique représentant industriel français du Ministère de l'Intérieur au sein du consortium européen ePoll

Voilà une entreprise qui, objectivement, a sérieusement besoin d'être en bon terme avec le gouvernement. Je n'en tirerai aucune conclusion, ce serait malhonnête, j'en conviens.

Passons.

Je remarque un "et linux" ajouté un peu comme un cheveu sur la soupe dans la liste des systèmes supportés et j'imagine les négociations qu'il a dû y avoir pour que surtout ces deux mots soient ajoutés.

Notre site test notre navigateur et lance un application java qui semble générer un certificat (à priori sans mot de passe) et nous arrivons enfin sur la page nous permettant de voter. Nous n'avons pas essayé.

L'ensemble de cette procédure me semble d'un bon accabi, un peu comme la ligne maginot protégeait correctement ce qui était derrière elle, je remarque tout de même un bouton "Modifier", grisé pour l'instant puisque nous n'avons pas voté, je reste curieux de son fonctionnement...

Un peu de "social engineering" maintenant. Nous avons vu que cette entreprise a travaillé avec la SNCF dont les élections viennent de se terminer. Un peu d'imagination, un zest de chance, et nous arrivons sur le site :

<https://www.jevoteenligne.com/vote/sncf/secure/welcome.do>

Bien. Cette entreprise gère donc ses différents vote en cour sur la même machine ou tout au moins sur le même portail. Anecdote pour la plupart, c'est une information qui, en sécurité a son importance. Les risques encourus par tout les sites d'une machine mutualisée sont ceux courus par le site le plus sensible. Que savons nous des autres votes en cours ? La présidence s'en est elle inquiétée ? Mystère.

Pour résumer, si un vote concurrent est un cours pour une association de bouliste le site cours à priori un moindre danger que si c'est un vote de l'OTAN.

En conclusion donc, ce vote, je le disais, ne pouvait pas être fiable.

Mais il aurait pu, facilement, être plus sécurisé. Si les membres de la DISI avaient été un tant soit peu consultés, si la procédure avait été soumise aux deux correspondants RSSI (Responsables de la Sécurité des Systèmes d'Information), l'essentiel des problèmes de sécurité que je soulève ici auraient été facilement corrigés. Si le processus avait été testé, les problèmes d'ergonomie auraient été vus. Si...

En conséquence, par la présente, constatant que pour un projet important de l'UPJV, touchant de près sa sécurité, je n'ai pas, et mon collègue non plus, été consulté, je démissionne de mon rôle de correspondant RSSI (suppléant).

Mis en page avec l'accord de l'auteur par **Le SNASUB/Fsu au service des personnels administratifs, ITRF et des Bibliothèques de l'académie d'Amiens**