Description d'une famille d'attaques possibles contre l'eVoting actuel

Rappel du virus de juin

"In June 2004, a Trojan horse appeared that captured passwords. It looked like an image file, but it was actually an executable that installed an add-on to Internet Explorer. That add-on monitored and recorded outbound connections to the websites of several dozen major financial institutions and then sent usernames and passwords to a computer in Russia. Using SSL didn't help; the Trojan monitored keystrokes before they were encrypted." Bruce Schneier CRYPTO-GRAM, August 15, 2004
Ce virus est une bonne preuve d'existence, sur le terrain, du problème.

Constitution virus add-on LASEC

Le LASEC (EPFL) a élaboré et implanté un virus similaire, dont la démonstration a été faite en attaquant la création d'une boîte aux lettres (eMail), ceci en capturant et modifiant le mot de passe. L'objet ainsi démontré est très similaire au virus de juin, et surtout possède tous le mécanisme nécessaire pour une attaque contre l'eVoting.
Citation de la page du Dr Philippe Oechslin :"Working with malicious terminals. [...] The operating systems and applications used today are all prone to automated or directed attacks. As a result, even if the data exchange with a bank arrives at our computer with absolute security, we still don't know if the telebanking session we see on the screen is the same session that is being carried out over the network. Initial work in this domain includes the implementation of an attack to demonstrate the problem. Using hooks provided by Internet Explorer we have created an interception layer thatcan modify data sent to the screen or typed by the user. For ethical reasons we have not implemented an attack against a telebanking application but against the registration process for a popular free e-mail service. On a more humourous note, we have implemented an automatic transcriber which replaces given pairs of words in any web page. This gives for a refreshing read of the news."

Rappel du mode opératoire de l'eVoting actuel

Le votant s'est identifié par son numéro de carte de vote (personnel et unique par session).
Il a rempli un bulletin (formulaire HTML) en cliquant sur les cases Non/Oui ou rien. Le bulletin est envoyé en clair, via le tube SSL, au serveur qui le chiffre et le retourne (en paramètre) avec une page HTML.
Cette page affiche le bulletin où les choix effectués sont figurés par des imagettes portant OUI, NON ou [rien], sur un arrière-plan coloré avec inscrit un code, de quatre lettres identiques pour chaque choix, qui est personnel au votant et imprimé sur sa carte de vote pour vérification.
Le votant confirme sont choix en fournissant son code secret (équivalentà un mot de passe complétant le numéro d'identification), ce dernier esttransmis (avec le bulletin chiffré) au serveur via SSL.Le vote est achevé.
Il est à noter que 98% des votants utilisent le navigateur MicroSoft-InternetExplorer (MS-IE).

Attaque envisagée (MalWare)

L'attaque vise le navigateur MS-IE, qui possède des ancrages logiciels où des co-logiciels (Add-On) peuvent s'annoncer et ensuite filtrer toutes les entrées (actions clavier et souris) et toutes les sorties (affichage, requête de connexion, etc.).
Avec un virus (ou vers), conçu comme celui du LASEC ou celui de juin, il est déjà possible de connaître les choix du votant et de les transmettre à un tiers (donc lever le secret du vote), ce qui est déjà une attaque grave.

En allant plus loin, et il s'agit alors d'une attaque dramatique, il est possible de modifier discrètement le vote.
Pour ce faire, il y existe plusieurs modes opératoires possibles. Dans l'un, le logiciel complémentaire (add-on) relèverait les choix Oui/Non/Blanc fait par le votant, créerait (et enverrait au serveur) un bulletin avec les réponses fausses voulues, ainsi qu'au moins une réponse de chaque sorte utilisée par le votant (O/N/B).
Au retour du bulletin de confirmation, il placerait les imagettes requises (O/N/B avec le filigrane, telles que reçues depuis le serveur) dans les cases des votes élémentaires (Acceptez-vous....), ceci selon le choix du votant et à la place des choix faux envoyés.
Le votant ne se douterait de rien et confirme en fournissant son code secret...
Le faux bulletin (codé dans la transaction) serait alors versé dans l'urne électronique.

Détections

Dans le premier cas, décrit ci-dessus et repris ci-dessous en [1], il n'y a pas de détection possible. Le virus ou vers n'est pas répertorié dans les fitres antivirus, et ne visant qu'une population extrêmement restreinte, relativement à l'Internet global, il a peu de chance d'y figurer et surtout trop tard. Son action est si spécialisée et discrète que l'utilisateur ne peut s'en apercevoir, et après un vote ou au plus tard après la clôture de la session il peut s'auto-annihiler sans laisser de trace.
Dans le second cas, décrit ci-dessous en [2], il pourrait y avoir découverte d'un léger temps de latence lors de la confirmation du vote.
Dans le troisième cas, décrit en [3], le but est justement de décrédibiliser le vote, et donc l'action est visible, mais il est trop tard pour réagir et le mal est fait.

Réponse du Dr Philippe Oeschlin, 1er assistant du Prf Vaudenay (EPFL-LASEC) et chargé de cours, spécialiste des attaques virales

L'attaques que vous présentez est tout à fait faisable.
Je peux en imaginer deux autres, outre l'espionnage. Permettez-moi de les résumer ci-dessous:

0) Espionnage du vote
0a) par piratage du browser
- nécessite: piratage du browser web
- fonctionnement: on intercepte les choix du votant lorsqu'ils sont soumis au serveur (avant qu'il ne soient chiffrés dans le tunnel SSL). On soumet une copie de ces choix en envoyant un mail, ou un paquet ping accèdant à une page web.
0b) par espionnage des événements clavier et souris
- nécessite: installation frauduleuse d'un logiciel d'enregistrement des événements. (Ces logiciels sont typiquement utilisés pour enregistrer des macros, afin d'éviter les tâches répétitives)
- fonctionnement: on enregistre les endroits ou le votant a cliqué, et le texte qu'il tape dans les formulaires du vote. On en déduit le vote qui a été fait. On envoie le résultat sur Internet

1) Falsification de l'image de confirmation (votre attaque)
- nécessite: piratage du browser web
- fonctionnement: Lors de l'envoi du vote, on modifie le vote à notre avantage mais de manière à ce que chaque type de réponse (Oui, Non, blanc) utilisé par le votant, apparaisse aussi dans notre vote modifié. Lorsqu'arrive la confirmation du vote dans une image, on coupe et colle (cut&past) les

vignettes de réponse de manière à recréer les vote que voulait le votant. Content du résultat, le votant procéde à la confirmation de son vote.

2) Modification invisible du vote après confirmation
- nécessite: piratage du browser web
- fonctionnement: On laisse le votant procéder au vote jusqu'au moment ou il a vu la confirmation du vote, qu'il tape son code de confirmation et qu'il clique sur le bouton qui confirme son vote. Plutôt que d'envoyer cette confirmation au serveur, on mémorise le code de confirmation et on envoie la séquence de commande qui serait envoyée si le votant voulait modifier son vote à notre avantage. Lorsque nous recevons la confirmation du vote modifié, nous sommes en possession du code de confirmation pour confirmer ce vote. L'affichage des réponses du serveur peut facilement être supprimé.

3) Modification visible du vote après confirmation (attaque de la souris folle)
- nécessite: installation frauduleuse d'un logiciel de télécommande de la souris. Ce genre de logiciel est typiquement utilisé pour enregistrer et exécuter des tâches répétitives)
- fonctionnement: On laisse le votant procéder au vote jusqu'au moment ou il a vu la confirmation du vote, qu'il tape son code de confirmation et qu'il tente de cliquer sur le bouton qui confirme son vote. On intercepte l'événement qui correspond au click et on télécommande la sourispour qu'elle exécute la séquence d'opérations nécessaires à revenir en arrière et à modifier le vote. Comme on a espionné la session, on est en possession de toutes les informations nécessaires à l'opération.

Diffusion du MalWare:

La plupart des attaques nécessitent la diffusion de malwares. Cela est possible par un ver qui se propage partout, par un e-mail infecté ou par un site web que l'on aurait piraté et sur lequel on déposerait une copie du malware. Dans tous les cas on peut cibler les adresses pour gagner en efficacité:
- ver:
on ne propage le ver qu'à des adresses appartenant à des provider suisses. Dans le cas d'internet par le câble, et sauf erreur dans le cas de l'ADSL, il est même possible de trouver quelles plages d'adresses correspondant au canton de Genève et lancer le ver sur ces adresses.
- virus:
on peut chercher une première série d'adresses e-mail genevoises en cherchant sur google des pages qui parlent de genève et qui contiennent des adresses e-mail. En infectant ces personnes et en favorisant la propagation vers des adresses e-mail suisses trouvées sur les machines infectées on peut espérer atteindre rapidement un grand nombre de genevois. On peut aussi utiliser des "aspirateurs d'adresses e-mail" (logiciels qui cherchent des adresses e-mail sur toutes les pages d'un site web, et le pointer sur des site genevois.
- site piraté:
si on arrive à pirater un site de l'administration genevoise, ou un site dont le public est genevois, on pourrait infecter spécifiquement des genevois.

Implantation du MalWare:

La difficulté de l'implantation dépend du type d'attaque, de l'expérience de l'attaquant et du moment. En effet, si les votations ont justement lieu deux semaines après qu'une vulnérabilité de Windows ait été publiée, il faudra moins d'un jour à un débutant pour écrire un ver qui infecte 500'000 machines en quelques jours (ce qui s'est passé avec Sasser ce printemps). Le vecteur de propagation

peut donc être très facile à trouver.
Quand à l'attaque elle-même, une attaque de type phishing peut être montée en deux ou trois jours par une personne qui n'est pas un spécialiste de l'informatique (d'après Sophos, il existe des kits de phishing sur internet). Une attaque de souris folle ou de piratage nécessite peut-être dix jours de travail à un informaticien.

Parades

Les parades sont difficiles et dans le mode actuel impossibles. Si on part du principe que l'on ne peut pas être sûr qu'il n'y ait pas de logiciels malicieux sur le poste on sera toujours exposé au déni de service sur le poste client et à la levée du secret de vote.
Avec un dialogue client-serveur HTML, le seul moyen d'éviter que des informations puissent être modifiées dans le browser serait d'ajouter à tous les messages de confirmation une information contenue sur la feuille de vote plus une information unique au message qui est confirmé (il faudrait donc que la feuille ait un code de confirmation différent pour chaque possibilité de vote).