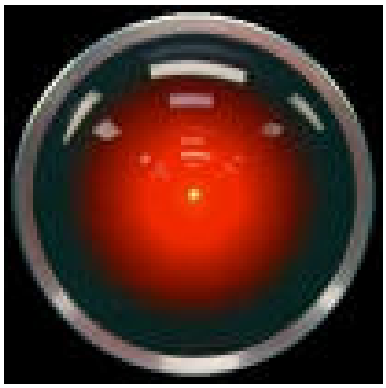
http://clx.asso.fr/spip/?Pouvez-vous-faire-confiance-a

Palladium et DRM - gestion de restrictions numériques

Pouvez-vous faire confiance à votre ordinateur ?

- L'Association - Libre et Libertés Numériques -



Date de mise en ligne : jeudi 24 octobre 2002

De qui votre ordinateur devrait-il recevoir ses ordres ? La plupart des personnes pensent que leurs ordinateurs devraient leur obéir, et ne pas obéir à quelqu'un d'autre. Avec un plan qu'elles appellent "Trusted Computing" ("L'informatique de confiance"), de grandes sociétés de médias (y compris du cinéma et de l'industrie du disque), ainsi que des sociétés d'informatique telles que Microsoft et Intel, projettent de faire en sorte que votre ordinateur leur obéisse au lieu de vous obéir. Les programmes propriétaires ont déjà inclus des dispositifs malveillants auparavant, mais ce plan rendrait cette pratique universelle.

Par définition, vous ne contrôlez pas ce que fait un logiciel propriétaire ; vous ne pouvez ni étudier son code source ni le modifier. Il n'est pas étonnant que les hommes d'affaires intelligents trouvent des moyens pour exercer un contrôle sur vos actions et ainsi en tirer avantage à vos dépends. Microsoft l'a déjà fait plusieurs fois : une version de Windows a été conçue pour renseigner Microsoft sur tous les logiciels installés sur votre disque dur ; une mise à jour de "sécurité" récente du lecteur de multimédias de Windows (Windows Media Player) a imposé l'accord des utilisateurs sur de nouvelles restrictions. Mais Microsoft n'est pas seul dans ce cas : le logiciel de partage de musique "KaZaa" est conçu de sorte que les associés de la compagnie KaZaa puisse louer l'utilisation de votre ordinateur à leurs clients. Ces dispositifs malveillants sont souvent secrets, mais même une fois que vous en avez connaissance, il est difficile de les enlever, puisque vous ne disposez pas du code source de l'application.

Dans le passé, il s'agissait d'incidents isolés. "L'informatique de confiance" les rendrait dominants. "L'informatique déloyale" ("Treacherous Computing") est un nom plus approprié, parce que le projet est conçu pour s'assurer que votre ordinateur vous désobéira systématiquement. En fait, il est conçu pour que votre ordinateur s'arrête de fonctionner comme ordinateur polyvalent. Chaque opération pourra exiger une permission explicite.

L'idée technique fondamentale de "l'informatique déloyale" est que l'ordinateur inclut un dispositif numérique de chiffrage et de signature, et les clefs sont maintenues secrètes (la version Microsoft de ce système s'appelle "Palladium"). Les logiciels propriétaires utiliseront ce dispositif afin de contrôler le lancement de tel ou tel programme, à quels documents ou données vous pourrez accéder, et avec quels programmes vous pourrez lire ou modifier ces documents ou données. Ces logiciels téléchargeront régulièrement de nouvelles règles d'autorisation par Internet, et vous les imposeront. Si vous ne laissez pas votre ordinateur récupérer périodiquement ces nouvelles règles depuis Internet, certaines options cesseront de fonctionner.

Naturellement, Hollywood et l'industrie du disque projettent d'employer l'informatique déloyale pour le "DRM" (Digital Restriction Management - gestion de restrictions numériques), de sorte que des vidéos ou de la musique téléchargées ne puissent être jouées que sur un ordinateur donné. Le partage des fichiers sera totalement impossible, du moins en utilisant les fichiers que vous obtiendriez auprès de ces sociétés et que serez autorisés à lire. Vous, le public, devez avoir la liberté et la possibilité de partager ces informations (je m'attends à ce que quelqu'un trouve une manière de produire des versions non codées, de télécharger et de partager celles-ci, ainsi le DRM ne s'appliquera pas entièrement, mais ce n'est pas une excuse pour laisser ce système s'implanter).

Rendre impossible le partage des fichiers vidéos et musicaux est une mauvaise chose, mais ça pourrait être pire. Il existe des projets pour généraliser ce dispositif aux messages électroniques et aux documents - ayant pour résultat un email qui disparaîtrait au bout de deux semaines, ou des documents qui pourront seulement être lus sur les ordinateurs d'une société mais pas sur ceux d'une autre.

Imaginez que vous recevez un courrier électronique de votre patron vous indiquant de faire quelque chose que vous

pensez risqué ; un mois plus tard, lorsque la situation s'envenime, vous ne pouvez plus utiliser ce message pour prouver que la décision n'était pas de vous. "Obtenir l'ordre par écrit" ne vous protège pas quand l'ordre est écrit avec une encre qui disparaît.

Imaginez que vous obtenez un email de votre patron, vous demandant d'agir illégalement ou d'effectuer une action moralement indigne, comme déchiqueter les résultats de l'audit de votre compagnie, ou permettre à une menace dangereuse pour votre pays de se propager. Aujourd'hui vous pouvez envoyer ce message à un journaliste et lui présenter les faits. Avec "l'informatique déloyale", le journaliste ne pourra pas lire le document ; son ordinateur refusera de lui obéir. L'"informatique déloyale" devient un paradis pour la corruption.

Les logiciel de traitement de texte tels que Word de Microsoft pourraient employer "l'informatique déloyale" quand ils enregistrent vos documents, pour s'assurer qu'aucun autre traitement de texte concurrent ne puisse les lire. Aujourd'hui nous devons deviner les secrets du format Word par des expériences laborieuses afin de programmer des traitements de texte libres qui puissent lire les documents au format Word (les .doc). Si Word chiffre les documents en utilisant "l'informatique déloyale" quand il les enregistre, la communauté du Logiciel Libre n'aura pas la possibilité de développer un programme capable de les lire - et même si nous le pouvions, de tels programmes seraient interdits par la DMCA (Digital Millenium Copyright Act - Loi de copyright du millénaire Numérique).

Les programmes qui utilisent "l'informatique déloyale" téléchargeront régulièrement de nouvelles règles par Internet, et imposeront ces règles automatiquement à votre travail. Si Microsoft ou le gouvernement des Etats-Unis, n'aime pas ce que vous énoncez dans un document écrit, ils seraient en mesure d'ajouter de nouvelles instructions indiquant à tous les ordinateurs de refuser de lire ce document. Chaque ordinateur obéirait, sitôt qu'il aurait téléchargé les nouvelles instructions. Vos écrits seraient sujets à l'effacement rétroactif "façon 1984" ; Au final, vous ne pourriez même plus les relire.

Vous pourriez penser que vous serez capable de découvrir quelles mauvaises choses fait une application de "l'informatique déloyale", saurez étudier de quelles façons elles sont néfastes, et décider de les accepter ou non. Il faudrait être myope et idiot pour accepter, et il se trouve que la bonne affaire que vous pensez faire ne tiendra pas toujours. A partir du moment où vous devenez dépendant de l'utilisation d'un programme, vous êtes accrochés et ils le savent ; ils peuvent alors se permettre de changer la donne. Quelques applications récupéreront automatiquement les mises à jour qui fonctionneront alors de façon différente - et elles ne vous permettront pas de choisir de mettre à jour ou non.

Aujourd'hui vous pouvez éviter de voir vos libertés restreintes par le logiciel propriétaire en ne l'utilisant pas. Si vous exploitez GNU/Linux ou un autre système d'exploitation libre, et si vous évitez d'y installer des applications propriétaires, alors vous êtes responsable et pouvez décider de ce que fait votre ordinateur. Si un Logiciel Libre contient un dispositif malveillant, des développeurs de la communauté l'enlèveront, et vous pourrez utiliser la version corrigée. Vous pouvez également utiliser des programmes et des applications libres sur les systèmes d'exploitation non-libres ; ceci ne vous procure pas une entière liberté, mais beaucoup d'utilisateurs le font.

L'"informatique déloyale" met l'existence des systèmes d'exploitation libres et des applications libres en danger, parce que vous ne pourrez pas les utiliser du tout. Quelques versions de "l'informatique déloyale" exigeraient que, pour se lancer, le système d'exploitation bénéficie d'une autorisation spécifique, délivrée par une société. Des systèmes d'exploitation libres ne pourront pas être installés. Quelques versions de l'"informatique déloyale" exigeraient que, pour s'exécuter, chaque programme bénéficie d'une autorisation délivrée spécifiquement par le programmeur du système d'exploitation. Vous ne pourriez pas utiliser d'applications libres sur un tel système. Si vous trouveriez une façon pour le faire, et le dites à quelqu'un, cela pourrait être considéré un crime.

Il y a déjà des propositions de lois aux Etats-Unis pour exiger de tous les ordinateurs qu'ils utilisent "l'informatique

déloyale", et pour interdire de relier de vieux ordinateurs à Internet. La CBDTPA (nous l'appelons le "Consume But Do Not Try Programming Act" - Consommons mais n'essayons pas de programmer) est l'une d'elles. Mais même s'ils ne vous forcent pas à passer à "l'informatique de confiance" par des lois, les pressions pour l'accepter peuvent être énormes. Aujourd'hui les gens utilisent souvent le format de Word pour s'échanger des documents, bien que cela cause plusieurs problèmes (cf la page http://www.gnu.org/philosophy/no-word-attachments.fr.html). Si seulement une machine de "l'informatique déloyale" pouvait lire les documents créés avec la dernière version de Word, beaucoup de personnes l'utiliserait, d'un point de vue individuel (Prends-le ou laisse-le - take it or leave it). Pour s'opposer à l'"informatique déloyale", nous devons nous regrouper et refuser la situation comme un choix collectif.

Pour de plus amples informations au sujet de l'"informatique déloyale", voir la page http://www.lebars.org/sec/tcpa-faq....

Bloquer "l'informatique déloyale" exigera d'un grand nombre de citoyens de s'organiser. Nous avons besoin de votre aide ! La "Electronic Frontier Foundation" (www.eff.org) et la "Public Knowledge" (www.publicknowledge.org) font campagne contre "l'informatique déloyale", ainsi que le projet Digital Speech commandité par la FSF (www.digitalspeech.org). Veuillez visiter ces sites et ainsi vous pourrez vous inscrire et appuyer leur travail.

Vous pouvez également aider en écrivant aux sièges sociaux d'Intel, IBM, HP/Compaq, ou à tout autre constructeur à qui vous avez acheté un ordinateur, expliquant que vous ne voulez pas subir de pression pour acheter les systèmes informatiques "de confiance" et que vous ne voulez pas qu'ils en produisent. Vous contribuerez ainsi à augmenter la pression des consommateurs sur les constructeurs. Si vous le faites de votre propre chef, envoyez s'il vous plaît les copies de vos lettres aux organismes ci-dessus.

Post-scriptum :

*1. Le projet de GNU distribue le GNU Privacy Guard (*GPG), un programme qui permet le chiffrage par clefs publiques et signatures numériques, que vous pouvez utiliser pour envoyer des emails sécurisés et privés. Il est utile d'étudier comment GPG diffÚre de l'"informatique déloyale", et de voir ce qui rend l'un utile et l'autre si dangereux.

Quand quelqu'un emploie GPG pour vous envoyer un document chiffré, et que vous utilisez GPG pour le décoder, le résultat est un document non codé que vous pouvez lire, transférer, copier, et même re-chiffrer pour l'envoyer de maniÚre sécurisée à quelqu'un d'autre. Une application de l'"informatique déloyale" vous laisserait lire les mots sur l'écran, mais ne vous permettrait pas de produire un document non codé que vous pourriez utiliser d'autres maniÚres. GPG, un logiciel libre, aide à mettre en place des dispositifs de sécurité disponibles pour les utilisateurs ; ils l'utilisent. L'"informatique déloyale" est conçue pour imposer des restrictions aux utilisateurs ; dans ce cas c'est elle qui les "utilise".

2. Microsoft présente Palladium comme un dispositif de sécurité, et prétend qu'il protégera vos données contre les virus. Mais ce discours est évidemment faux. Une présentation réalisée par Microsoft Research (le département Recherche/Développement de Microsoft) en octobre 2002 a montré qu'une des caractéristiques de Palladium consiste à permettre aux systÚmes d'exploitation et aux applications existantes de continuer de fonctionner ; donc, les virus continueront à faire toutes les choses qu'ils font aujourd'hui.

Quand Microsoft parle de "sécurité" à propos de Palladium, il ne s'agit pas de notre définition de la sécurité : protéger votre machine contre des choses que vous ne voulez pas. Elle signifie protéger vos données stockées sur votre machine contre l'accÚs par vous, d'une maniÚre que d'autres ne veulent pas. Un diaporama dans la présentation montre plusieurs types d'informations secrÚtes que Palladium pourrait conserver, y compris des secrets de tiers et des "secrets d'utilisateurs" - mais "secrets d'utilisateurs" est mis entre guillemets, ce qui signifie que Palladium n'est pas véritablement conçu pour ce type d'informations.

Dans la présentation on trouve fréquemement d'autres termes que nous associons habituellement à la notion de sécurité, tels que "attaque", "code malveillant," "spoofing," ainsi que "confiance" (trusted). Aucun d'eux ne désigne ce que signifie normalement ces mots. Une "attaque" ne signifie pas que quelqu'un essaye de vous blesser. Il signifie que vous essayez de copier de la musique. "Code malveillant" signifie un code

installé par vous pour faire ce que quelqu'un d'autre ne veut pas que votre machine fasse. "Spoofing" ne signifie pas quelqu'un qui vous dupe, il signifie que vous dupez Palladium. Et ainsi de suite.

3. Un rapport précédent, écrit par les partisans de Palladium a énoncé le principe de base suivant : que celui qui a développé ou a rassemblé l'information devrait avoir le contrÎle total de la façon dont vous l'utilisez. Ceci représenterait un renversement révolutionnaire des idées passées de l'éthique et du systÚme légal, et créerait un systÚme de contrÎle sans précédent. Les problÚmes spécifiques de ces systÚmes ne sont aucunement des accidents ; ils résultent du principe de base. C'est ce but que nous devons rejeter.

Note de l'éditeur NewsForge : Cet article est paru pour la premiÚre fois dans le nouveau livre de Richard Stallman, "Logiciel Libre, Société Libre". C'est la premiÚre fois que l'article est paru en ligne, et Stallman a ajouté certaines précisions.

Note du traducteur Fabien ILLIDE : Merci aux relecteurs pour l'aide à la traduction de cet article.