Pouvez-vous faire confiance à votre ordinateur ?

Richard M. Stallman

21 octobre 2002

De qui votre ordinateur devrait-il recevoir ses ordres ? La plupart des gens pensent que leur ordinateur devrait leur obéir, et non obéir à quelqu'un d'autre. Grâce à un projet qu'elles appellent *trusted computing* (l'« informatique de confiance »), de grandes sociétés de médias (incluant des sociétés de cinéma et des maisons de disques), en collaboration avec des sociétés informatiques comme Microsoft et Intel, prévoient de faire en sorte que votre ordinateur leur obéisse au lieu de vous obéir. Dans le passé, des programmes propriétaires ont déjà inclus des dispositifs malveillants, mais ce projet rendrait le procédé universel.

« Logiciel propriétaire » signifie, fondamentalement, que vous ne contrôlez pas ce qu'il fait : vous ne pouvez pas en étudier le code source, ni le modifier. Il n'est pas surprenant que des hommes d'affaires intelligents trouvent des façons d'utiliser ce contrôle pour vous désavantager. Microsoft l'a fait plusieurs fois : une des versions de Windows a été conçue de façon à informer Microsoft sur tous les logiciels de votre disque dur ; un correctif « de sécurité » récent dans Windows Media Player a obligé les utilisateurs à accepter de nouvelles restrictions. Mais Microsoft n'est pas seul : le logiciel de partage de musique KaZaa est conçu pour qu'un partenaire commercial de KaZaa puisse louer à ses clients l'utilisation de votre propre ordinateur. Ces fonctions malveillantes sont souvent secrètes, mais même une fois que vous en avez connaissance, il est difficile de les enlever, puisque vous ne disposez pas du code source.

Dans le passé, il s'agissait d'incidents isolés. L'« informatique de confiance » généralisera ce phénomène. Un nom plus approprié serait « informatique déloyale » *(treacherous computing)*, car ce projet est conçu pour s'assurer que votre ordinateur vous désobéira systématiquement. En fait, il est conçu pour empêcher votre ordinateur de fonctionner comme un ordinateur à vocation universelle. Toute opération nécessitera une autorisation explicite.

L'idée technique sous-jacente de l'« informatique déloyale » *(treacherous computing)* est que l'ordinateur comprenne un procédé de chiffrement et de signature, dont les clefs sont gardées secrètes et ne vous sont pas divulguées. (La version Microsoft de ce procédé est appelée « Palladium ».) Les logiciels propriétaires utiliseront ce dispositif pour contrôler quels autres programmes vous pouvez utiliser, quels documents ou quelles données vous pouvez lire, et avec quels programmes vous avez le droit de les lire. Ces programmes téléchargeront de nouvelles règles d'autorisation par Internet et vous imposeront automatiquement ces règles. Si vous ne permettez pas périodiquement à votre ordinateur d'obtenir les nouvelles règles, certaines fonctionnalités cesseront automatiquement de fonctionner.

Évidemment, Hollywood et les maisons de disques prévoient d'utiliser l'informatique déloyale pour la « gestion des droits numériques » *(Digital Restrictions Management)*, afin que les vidéos et la musique téléchargées ne puissent être jouées que sur un ordinateur précis. Le partage sera complètement impossible, du moins avec les fichiers autorisés que

vous obtiendriez de ces sociétés. Vous, le public, devriez avoir à la fois la liberté et la capacité de partager ces choses. (Je m'attends à ce que quelqu'un trouve une façon de produire des versions non cryptées et de les offrir en téléchargement, si bien que le DRM ne sera pas un succès total. Mais cela n'excuse en rien ce principe de restriction.)

Rendre le partage impossible est déjà grave, mais il y a pire. Il existe des projets qui visent à utiliser la même méthode pour les e-mails et les documents électroniques. Ainsi, certains mails disparaîtraient au bout de deux semaines, ou certains documents ne pourraient être lus que sur les ordinateurs d'une société précise.

Imaginez que vous recevez un e-mail de votre patron qui vous ordonne de faire quelque chose que vous estimez risqué ; un mois plus tard, si des ennuis surviennent, vous ne pourrez plus utiliser cet e-mail pour prouver que la décision n'était pas la vôtre. « Avoir un document écrit » ne vous protège pas, quand ce document est écrit à l'encre sympathique.

Imaginez que vous receviez un e-mail de votre patron exposant une politique illégale ou moralement scandaleuse — par exemple, détruire un audit de votre société, ou exposer votre pays à des risques dangereux par négligence. Aujourd'hui vous pouvez l'envoyer à un journaliste et montrer ces activités. Avec l'informatique déloyale, le journaliste ne sera pas capable de lire le document ; son ordinateur refusera de lui obéir. L'informatique déloyale devient un paradis pour la corruption.

Les logiciels de traitement de texte comme Microsoft Word pourraient utiliser l'informatique déloyale lorsqu'ils enregistrent vos documents, pour s'assurer qu'aucun traitement de texte concurrent ne pourra les lire. Aujourd'hui nous sommes obligés de faire des expérimentations laborieuses pour percer les secrets du format de fichier Word, et rendre les logiciels libres de traitement de texte capables de lire ce format. Si Word enregistre les documents en utilisant l'informatique déloyale, la communauté du logiciel libre n'aura aucun moyen de développer un logiciel pour les lire — et même si nous le pouvions, de tels programmes pourraient être interdits par la loi DMCA *(Digital Millenium Copyright Act)*.

Les programmes qui utilisent l'informatique déloyale téléchargeront régulièrement de nouvelles règles d'autorisation par Internet et appliqueront ces règles automatiquement à votre travail. Si Microsoft ou le gouvernement américain n'aiment pas ce que vous avez écrit dans l'un de vos documents, ils pourraient créer de nouvelles règles imposant à tous les ordinateurs de refuser de lire ledit document. Chaque ordinateur obéirait dès le téléchargement de ces nouvelles instructions. Vos écrits seraient sujets à de l'effacement rétroactif comme dans *1984* de G. Orwell. Même *vous*, pourriez ne plus pouvoir le lire.

Vous pensez peut-être pouvoir découvrir ce qu'un logiciel utilisant l'informatique déloyale peut faire de malveillant, apprendre à quel point cela vous est néfaste, et que vous pourrez décider de l'utiliser ou pas. Il faudrait être myope et idiot pour l'utiliser, mais le problème est que votre décision aura une portée bien faible. Une fois que vous devenez dépendant du programme que vous utilisez, vous êtes pris au piège et ils le savent ; à ce moment ils peuvent changer les règles du jeu. Certaines applications téléchargeront automatiquement des mises à jour qui feront tout autre chose — et ils ne vous laisseront pas le choix de mettre à jour ou non.

Aujourd'hui vous pouvez éviter de voir vos libertés contraintes par un logiciel propriétaire, en ne l'utilisant pas. Si vous utilisez GNU/Linux ou tout autre système libre et si vous évitez d'y installer des logiciels propriétaires, alors vous pouvez décider ce que fait votre ordinateur. Si un logiciel libre a une fonction malveillante, d'autres développeurs de la communauté l'enlèveront et vous pourrez utiliser la version corrigée. Vous pouvez aussi utiliser des applications libres et des outils libres sur des systèmes qui ne le sont pas ; cela ne vous octroie pas une liberté totale, mais beaucoup d'utilisateurs le font.

L'informatique déloyale met en danger

l'existence des systèmes d'exploitation et des logiciels libres, parce que vous ne serez peut-être plus du tout autorisé à les utiliser. Certaines formes d'informatique déloyale pourraient exiger que le système d'exploitation soit spécifiquement autorisé par une compagnie particulière. Des systèmes d'exploitation libres ne pourraient pas être installés. D'autres formes d'informatique déloyale exigeraient que chaque programme soit spécifiquement autorisé par l'éditeur du système d'exploitation. Vous ne pourriez pas utiliser d'applications libres sur un tel système. Si vous y parveniez et que vous divulguiez la façon de faire, cela pourrait être un délit.

Aux États-Unis, il y a déjà des propositions de loi qui demandent à tous les ordinateurs de fonctionner avec l'informatique déloyale, et dans le même temps demandent l'interdiction de connecter à internet les ordinateurs anciens. Le CBDTPA (nous l'appelons le *Consume But Don't Try Programming Act*, c'est-à-dire « consommez, mais n'essayez pas de programmer ») est l'une d'entre elles. Même si elles ne vous forçaient pas légalement à vous reporter sur l'informatique déloyale, la pression visant à vous la faire accepter pourrait être énorme. Aujourd'hui les gens utilisent souvent le format de Word pour communiquer, bien que cela pose plusieurs sortes de problèmes (voir ce lien). Si les seuls ordinateurs capables de lire les derniers documents Word en date sont ceux qui utilisent l'informatique déloyale, de nombreuses personnes s'y plieront, s'ils voient la situation seulement en termes d'action individuelle (c'est à prendre ou à laisser). Pour lutter contre l'informatique déloyale, nous devons réagir et agir de façon collective.

Pour plus d'information sur l'informatique déloyale, voir ce lien.

Barrer la route à l'informatique déloyale nécessitera qu'un grand nombre de citoyens s'organisent. Nous avons besoin de votre aide ! L'*Electronic Frontier Foundation* et la *Public Knowledge* font campagne contre l'informatique déloyale, ainsi que le *Digital Speech Project* lancé par la *Free Software Foundation*. Ne manquez pas de visiter ces sites web pour pouvoir vous inscrire et les aider dans leur travail.

Vous pouvez aussi nous aider en écrivant au bureau des affaires publiques d'Intel, d'IBM, de HP/COMPAQ, ou à votre revendeur informatique, expliquant que vous ne voulez pas subir de pression pour acheter des systèmes informatique « de confiance » et que vous ne voulez donc pas qu'ils en produisent. Ainsi la voix du consommateur devra être entendue. Si vous faites ceci à titre individuel, envoyez s'il vous plaît des copies de vos lettres aux organisations ci-dessus.

P.S. :

1. Le Projet GNU distribue le logiciel GPG *(GNU Privacy Guard)*, un programme qui utilise le cryptage avec clef publique et la signature numérique, que vous pouvez utiliser pour envoyer des e-mails sécurisés et privés. Il est utile d'explorer en quoi GPG diffère de l'informatique déloyale et de voir ce qui fait que l'un est utile alors que l'autre est si dangereux.
   Quand quelqu'un utilise GPG pour vous envoyer un document crypté et que vous utilisez GPG pour le décoder, il en résulte un document non crypté que vous pouvez lire, transmettre, copier et même crypter de nouveau pour l'envoyer de façon sécurisée à quelqu'un d'autre. Un logiciel d'informatique déloyale vous laisserait lire les mots à l'écran, mais ne vous laisserait pas produire un document non crypté que vous pourriez utiliser d'une autre façon. GPG, un logiciel libre, met la sécurité à disposition des utilisateurs ; et ils l'utilisent. L'informatique déloyale est conçue pour imposer des restrictions aux utilisateurs ; ici, c'est elle qui les utilise.
2. Microsoft présente Palladium comme une mesure de sécurité, et prétend qu'il nous protégera contre les virus ; mais c'est faux, de toute évidence. Lors d'une présentation en

octobre 2002, le département de recherche de Microsoft a déclaré que l'une des caractéristiques de Palladium est que les systèmes d'exploitation et les logiciels existants continueront de fonctionner ; par conséquent, les virus seront toujours capables de faire tout ce qu'ils peuvent faire aujourd'hui.

En fait, quand Microsoft parle de « sécurité » à propos de Palladium, ils ne donnent pas à ce mot le sens généralement admis : il ne s'agit pas de protéger votre machine des choses que vous ne voulez pas. Il s'agit de protéger les données de votre ordinateur de sorte que vous ne puissiez pas les utiliser d'une autre façon que celle voulue par d'autres. Lors de la même présentation, une diapositive a dressé une liste de plusieurs types de secrets que Palladium pourrait servir à garder, dont « les secrets de tiers » et « les secrets d'utilisateur » (mais les « secrets d'utilisateur » étaient entre guillemets, reconnaissant que ce n'est pas pour cela que le Palladium est vraiment conçu).

La présentation a fait une utilisation fréquente d'autres termes que nous associons fréquemment au contexte de sécurité, comme « attaque », « code malveillant », « canular », aussi bien que « de confiance ». Aucun d'eux n'est utilisé avec sa signification habituelle : « attaque » ne veut pas dire que quelqu'un essaye de vous nuire, mais plutôt « vous, essayant de copier de la musique » ; « code malveillant » signifie « code installé par vous, pour faire ce que quelqu'un d'autre ne veut pas voir votre ordinateur exécuter » ; « canular » ne signifie pas que quelqu'un vous cherche à vous duper, mais que vous tentez de contourner Palladium. Et ainsi de suite.

3. Une déclaration précédente faite par les développeurs de Palladium affirme que le principe de base est le suivant : quiconque a développé ou rassemblé des informations devrait avoir un contrôle total sur votre manière de les utiliser. Cela représenterait une véritable révolution tant du point de vue éthique que du point de vue légal, et créerait un système de contrôle sans précédent. Les problèmes liés à ces systèmes n'arrivent pas par hasard : ils sont le résultat de l'objectif principal. Et c'est cet objectif que nous devons rejeter.

1. Cette traduction de Sébastien Morin repart du texte original de Richard M. Stallman. Elle est inspirée de la traduction de Matthieu Piaumier d'une part, et de celle de Christophe Combelles d'autre part. Cette version vous est offerte dans les termes de la licence GNU/FDL. Le code source au format LaTeX est disponible sur mon site et sur Framasoft.net.