¿Puede confiar en su computadora?

por **Richard Stallman**

¿De quién debería recibir órdenes su computadora? Mucha gente piensa que sus computadoras deberían obedecerles a ellos, en vez de a otras personas. Mediante un plan al que llaman "computación confiable" ("trusted computing", en inglés), grandes corporaciones de los medios de comunicación (incluyendo las compañías cinematográficas y de la industria discográfica) junto con compañías de computadoras tales como Microsoft e Intel, están planificando hacer que su computadora los obedezca a ellos en vez de a usted. (La versión de Microsoft de este esquema se llama "Palladium"). Los programas propietarios han incluido características maliciosas en el pasado, pero este plan haría esto universal.

Software propietario significa, fundamentalmente, que usted no controla lo que hace; no puede estudiar el código fuente o modificarlo. No es sorprendente que hábiles hombres de negocios encuentren formas de usar su control para ponerle a usted en desventaja. Microsoft ha hecho esto varias veces; una versión de Windows fue diseñada para reportar a Microsoft todo el software en su disco duro; una reciente actualización de "seguridad" en el Reproductor Multimedia de Windows requería que los usuarios aceptaran nuevas restricciones. Pero Microsoft no está solo: el software para intercambio de música KaZaa está diseñado de forma que un asociado de negocios de KaZaa pueda alquilar el uso de su computadora a sus clientes. Estas características maliciosas son normalmente secretas, pero una vez que usted se entera de ellas es difícil eliminarlas, dado que no dispone del código fuente.

En el pasado, estos fueron incidentes aislados. "Computación confiable" los haría omnipresentes. "Computación traidora" es un nombre más apropiado, porque el plan está diseñado para asegurarse de que su computadora sistemáticamente lo desobedecerá. De hecho, está diseñado para que la misma deje de funcionar como una computadora de propósito general. Cada operación puede requerir de una autorización explícita.

La idea técnica detrás de la computación traidora es que la computadora incluye un dispositivo de cifrado y firma digital, y las claves se mantienen secretas para usted. Los programas propietarios usan este dispositivo para controlar qué otros programas puede ejecutar, a qué documentos o datos puede acceder y a qué programas se los puede transferir. Esos programas continuamente descargarán nuevas reglas de autorización a través de Internet, e impondrán dichas reglas automáticamente a su trabajo. Si usted no permite a su computadora obtener las nuevas reglas periódicamente de Internet, algunas capacidades dejarán automáticamente de funcionar.

Por supuesto, Hollywood y las compañías discográficas planean usar la computación traidora para "DRM" ("Administración de Restricciones Digitales" o "Digital Restriction Management", en inglés), así los vídeos y la música descargados podrán ser reproducidos sólo en una computadora específica. Compartir será completamente imposible, al menos usando los archivos autorizados que deberá obtener de dichas compañías. Usted, el público, debería tener la libertad y la habilidad de compartir esas cosas. (Espero que alguien encuentre la forma de producir versiones no cifradas, y de subirlas y compartirlas, así DRM no tendrá éxito completamente, pero esto no es excusa para el sistema).

Hacer imposible el compartir ya es lo suficientemente malo, pero se pone peor. Existen planes para usar la misma facilidad al enviar documentos por correo electrónico -- resultando en mensajes que desaparecen en dos semanas, o documentos que sólo pueden ser leídos en las computadoras de determinada compañía.

Imagínese si usted recibiera un mensaje de correo electrónico de su jefe diciéndole que haga algo que usted piensa que es arriesgado; un mes después, cuando el tiro sale por la culata no puede usar el mensaje para mostrar que la decisión no fue suya. "Ponerlo por escrito" no lo protege si la orden está escrita en tinta que desaparece.

Imagínese si usted recibe un mensaje de correo electrónico de su jefe estableciendo una política que es ilegal o inmoral, tal como destrozar los documentos de auditoría de su compañía, o permitir que una amenaza peligrosa para su país avance sin ser controlada. Actualmente, usted puede enviar esto a un periodista y exponer la actividad. Con la computación traidora, el periodista no será capaz de leer el documento; su computadora se negará a obedecerlo. La computación traidora se transforma en un paraíso para la corrupción.

Los procesadores de texto tales como Microsoft Word podrían usar la computación traidora cuando usted guarde sus documentos, para asegurarse de que ningún procesador de texto de la competencia podrá leerlos. Actualmente debemos averiguar los secretos del formato de Word mediante laboriosos experimentos, para que los procesadores libres puedan leer documentos de Word. Si Word cifra los documentos usando computación traidora cuando los guarda, la comunidad del software libre no tendrá la posibilidad de desarrollar software para leerlos -- y si pudiéramos, tales programas podrían ser prohibidos por la Digital Millennium Copyright Act (Ley de Copyright del Milenio Digital).

Los programas que usen computación traidora continuamente descargarán nuevas reglas de autorización desde Internet, e impondrán dichas reglas a su trabajo. Si a Microsoft, o al gobierno de los EEUU no les agrada lo que usted dice en un documento que escribió, podrán publicar nuevas restricciones diciendo a todas las computadoras que se rehusen a dejar que alguien lea dicho documento. Cada computadora del mundo obedecerá cuando descargue las nuevas instrucciones. Su escrito estará sujeto a un borrado retroactivo estilo 1984. Hasta usted podría ser incapaz de leerlo.

Podría pensar que usted puede averiguar que cosas sucias hace una aplicación de computación traidora, estudiar qué tan dañinas son, y decidir si aceptarlas. Sería ingenuo aceptarlo, pero el punto es que el trato que cree que está haciendo no se mantendrá. Una vez que usted dependa del uso del programa, estará enganchado y ellos lo saben; entonces pueden cambiar el trato. Algunas aplicaciones automáticamente bajarán actualizaciones que harán algo diferente -- y no le darán la posibilidad de elegir si desea la actualización o no.

Actualmente puede evitar ser restringido por software propietario no usándolo. Si ejecuta GNU/Linux u otro sistema operativo libre, y si evita instalar aplicaciones propietarias sobre él, entonces usted está al mando de lo que su computadora hace. Si un programa libre tiene una característica maliciosa, otros desarrolladores en la comunidad la quitarán y usted puede usar la versión corregida. Puede también ejecutar aplicaciones y herramientas libres en sistemas operativos no libres; esto falla completamente en darle libertad, pero muchos usuarios lo hacen.

La computación traidora pone en peligro la existencia de sistemas operativos y aplicaciones libres, porque usted ya no podrá ejecutarlas. Algunas versiones de la computación traidora requerirán que el sistema operativo esté específicamente autorizado por una compañía particular. Los sistemas operativos libres no podrán ser instalados. Algunas versiones de la computación traidora requerirán que cada programa sea específicamente autorizado por el desarrollador del sistema operativo. No podrá ejecutar aplicaciones libres en tales sistemas. Si usted averigua cómo hacerlo y se lo dice a alguien, eso podría constituir un delito.

Existen proyectos de ley en EEUU que requieren que todas las computadoras soporten computación traidora, y que se prohiba la conexión de computadoras antiguas a Internet. La CBDTPA (la llamamos Ley Consuma Pero No Trate de Programar, Consume But Don't Try Programming Act, en inglés) es uno de ellos. Pero inclusive si no lo fuerzan legalmente a migrar hacia la computación traidora, la presión para aceptarla puede ser enorme. Actualmente las personas usualmente utilizan el formato Word para comunicarse, aunque esto causa varios tipos de problemas (vea "Podemos Acabar con los Archivos Adjuntos en Word"). Si solamente una máquina de computación traidora puede leer los últimos documentos de Word, mucha gente migrará hacia ella, si ven la situación sólo en términos de acción individual (tómalo o déjalo). Para oponernos a la computación traidora, debemos unirnos y confrontar la situación como una elección colectiva.

Para mayor información sobre computación traidora, vea <http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html>.

Bloquear la computación traidora requerirá que se organicen un gran número de ciudadanos. ¡Necesitamos su ayuda!. La Electronic Frontier Foundation (Fundación Frontera Electrónica) y Public Knowledge (Conocimiento Público) están organizando campañas en contra de la computación traidora, así como también el Digital Speech Project (Proyecto Expresión Digital) esponsorizado por la FSF. Por favor, visite estos sitios Web para poder sumarse y apoyar de su trabajo.

También puede ayudar escribiendo a las oficinas de asuntos públicos de Intel, IBM, HP/Compaq, o cualquiera a quien usted le haya comprado una computadora, explicándole que no quiere ser presionado a comprar sistemas de computación "confiable", por lo cual no está de acuerdo en que ellos los produzcan. Esto puede ejercer la presión del poder del consumidor. Si usted hace esto, por favor envíe copias de sus cartas a las organizaciones antes citadas.

Posdatas

1. El proyecto GNU distribuye GNU Privacy Guard, un programa que implementa cifrado de clave pública y firmas digitales, el cual puede utilizase para enviar mensajes de correo electrónico seguros y privados. Es muy ilustrativo examinar cómo GPG se diferencia de la computación traidora, y ver qué hace a una tan útil y a la otra tan peligrosa.

   Cuando alguien usa GPG para enviarle un documento cifrado y usted usa GPG para decodificarlo, el resultado es un documento no cifrado que usted puede leer, reenviar, copiar e inclusive re-cifrar para enviarlo de forma segura a un tercero. Una aplicación de computación traidora lo dejaría leer las palabras en la pantalla, pero no producir un documento no cifrado que pudiera usar de otras formas. GPG, un paquete de software libre, pone las funciones de seguridad a disposición de los usuarios: ellos lo usan. La computación traidora está diseñada para imponer restricciones a los usuarios: ella los usa.

2. Microsoft presenta a palladium como una medida de seguridad, y proclama que brindará protección contra virus, pero esta afirmación es evidentemente falsa. Una presentación de Microsoft Research en octubre de 2002 estableció que una de las especificaciones de palladium es que los sistemas operativos y aplicaciones existentes seguirán pudiéndose ejecutar, por lo tanto, los virus seguirán siendo capaces de hacer todas las cosas que hacen actualmente.

   Cuando Microsoft habla de "seguridad" con relación a palladium, no lo hace con el significado que normalmente asociamos a esa palabra: proteger a su computadora de cosas que usted no desea. Ellos se refieren a proteger su acceso a las copias de datos en su computadora de formas que otros no desean que se realice. Una diapositiva en la presentación enumeraba varios tipos de

secretos que palladium podría resguardar, incluyendo "secretos de terceras partes" y "secretos de usuario" -- pero poniendo "secretos de usuario" entre comillas, reconociendo que es un absurdo en el contexto de palladium.

La presentación hizo uso frecuente de otros términos que usualmente asociamos en el contexto de seguridad, tales como "ataque", "código malicioso", "engaño" ("spoofing", en inglés), así como también "confianza". Ninguno de esos términos tiene el significado usual. "Ataque" no significa alguien tratando de dañarlo a usted, sino usted intentando copiar música. "Código malicioso" significa código instalado por usted para hacer algo que otros no desean que su computadora haga. "Engaño" no significa alguien engañándolo, sino usted engañando a palladium. Y así sucesivamente.

3. Una declaración previa de los desarrolladores de palladium establecía la premisa básica que quien hubiera desarrollado o recolectado información debía tener control total sobre cómo usted la usa. Esto hubiera representado una vuelta revolucionaria de ideas pasadas acerca de éticas y del sistema legal, y creado un sistema de control sin precedentes. Los problemas específicos de esos sistemas no son accidentales; sino que resultan de metas básicas. Es la meta que debemos rechazar.

Este ensayo ha sido publicado en *Free Software, Free Society: The Selected Essays of Richard M. Stallman*

Traductor: 19 de enero de 2003 - Javier Smaldone javier@dc.exa.unrc.edu.ar

---