Seguridad y Software Libre

Autor: José Angel de Bustos Pérez - jadebustos (arroba) augcyl (punto) org
Reedición - Este artículo fue publicado en Kriptópolis el 13/12/2002
Fecha de Publicación: 13 de Noviembre de 2005

Mucha gente utiliza software especial para proteger sus comunicaciones y evitar así intromisiones en su privacidad. Pero lamentablemente la educación de la mayoría de los usuarios de ordenadores deja mucho que desear en cuestiones de seguridad. ¿Cuál es el motivo?. Muy sencillo: para la mayoría de los usuarios, el ordenador es una mera herramienta de trabajo y sólo están interesados en encenderlo y despreocuparse de todo. Todo lo que quieren es utilizar un programa de ordenador y que dicho programa les solucione todos los problemas...

Por ejemplo, si quieren proteger sus comunicaciones se limitan a buscar en los foros o preguntar en grupos de news para encontrar un programa que les solucione su problema. Una vez encontrado, se limitan a instalarlo y utilizarlo sin preocuparse de adquirir unos ligeros conocimientos sobre la materia (por ejemplo, criptografía), resultando que muchas veces sus comunicaciones están mal protegidas. Esto es aún más peligroso que no proteger las comunicaciones, ya que cuando se sabe que éstas no son seguras se evita transmitir información "sensible", mientras que esa falsa sensación de seguridad invita sin duda a hacerlo.

Afortunadamente, hay usuarios que son más conscientes y van un paso más allá: se preocupan de adquirir una serie de conocimientos que les permitan utilizar el software que han elegido de forma segura y correcta. ¿Pero es eso suficiente para decir que el programa es seguro? La respuesta no puede ser más sencilla y directa: no.

Para que un programa informático sea seguro no basta con utilizarlo correctamente. Hace falta que esté libre de fallos, que no tenga puertas traseras y que no posea ninguna funcionalidad "no documentada".

Cuando adquirimos un software propietario rara vez se nos suministra el código fuente. Sin embargo, la mayoría de la gente no le da importancia a este hecho ya que, como ellos dicen, "¿Y qué me importa a mí que me den el código fuente si no tengo los conocimientos necesarios para leerlo?".

Sin embargo, la única forma de poder fiarnos de la seguridad de un programa informático es tener a nuestra disposición el código fuente, ya que de esta manera podemos ver cómo ha sido programado y si lo ha sido de forma correcta. Además, también podremos comprobar que en dicho programa no hay:

- Puertas traseras. No es necesario que el desarrollador las incluya. Hay veces en las que un intruso introduce una puerta trasera sin el

conocimiento del desarrollador; otras veces la competencia puede pagar a un programador descontento para que introduzca esa puerta trasera.
- Funcionalidades no documentadas. Un programa puede realizar ciertas tareas de las que no somos conscientes. Por ejemplo, un programa para cifrado de correo electrónico tendrá acceso a nuestras claves y podría haber sido programado para mandar esas claves a una determinada persona. O bien podría incluir información sobre nosotros y nuestras claves en las firmas digitales que utilicemos mediante la inclusión de canales subliminales.

La única forma de detectar todo esto es mediante la disponibilidad del código fuente, ya que encontrar un bug en un programa de ordenador no es tan sencillo como se piensa, a menos que se disponga del código fuente. La disponibilidad del código fuente nos da más seguridad en el sentido de transparencia: como el código fuente está disponible se puede auditar y comprobar así que está libre de puertas traseras y/o funcionalidades no documentadas, ya que en caso de tenerlas se descubrirían, y su hallazgo sería una auténtica vergüenza para la empresa que lo vende, pudiéndola llevar a la ruina.

Mucha gente argumenta lo siguiente:

- Como no tienen conocimientos suficientes, ni tiempo muchas veces, no pueden comprobar si dicho programa es seguro.

Pero hay gente que sí lo hace, y cuando se descubre algún fallo salta a la luz pública enseguida. De esta forma, todos los usuarios que lo utilizan son conscientes de esos fallos de seguridad y pueden obrar en consecuencia. En materia de seguridad, la falta de transparencia sólo perjudica a los usuarios, porque puede resultar mucho más difícil descubrir las vulnerabilidades del software que estén utilizando.

- La disponibilidad del código fuente no garantiza que el software que se utiliza haya sido generado a partir de ese código fuente.

Pero como el código fuente está disponible, quien tenga dudas puede compilarlo por sí mismo y quedarse más tranquilo.

- Al estar el código fuente disponible los intrusos tienen ventajas, ya que pueden descubrir antes los fallos y aprovecharse de ellos.

Cierto, pero hay algo más sobre este tema, que desde los sectores contrarios al software libre no se comenta. No sólo los intrusos los descubren, sino que también hay gente dedicada a la "caza" de bugs que descubre los fallos, los pone en conocimiento de los usuarios y los arregla, con lo cual los usuarios pueden obrar en consecuencia (por otro lado, al ser conscientes del fallo de seguridad y gracias a la disponibilidad del código fuente, es posible que cualquier persona con los conocientos adecuados pueda arreglar el fallo y

poner la versión ya reparada a disposición de los usuarios). Con software propietario, habría que esperar a que la empresa sacara el parche o Service Pack correspondiente y no hay que olvidar que esto lo hará cuando le salga económicamente rentable. Generalmente se espera a tener corregidos una determinada cantidad de errores y sólo entonces se libera el correspondiente Service Pack, en lugar de solucionar los fallos cuando se detectan. De este tipo de políticas también salimos perjudicados los usuarios.

Entonces, ¿qué motivos existen para no querer software libre?

Los motivos son claros y sencillos:

- Hay muchas empresas que se dedican a vender humo. Es decir venden software de mala calidad y la disponibilidad del código fuente daría a conocer, sin ninguna duda, la falta de calidad del software que venden.
- Habría una mayor competencia y las empresas que más éxito tendrían serían aquellas que mejores productos crearan, y no aquellas que desde posiciones de privilegio se aprovechan de ello.
- Hay empresas que se aprovechan de su posición predominante en el mercado y mediante el uso de formatos propietarios para el manejo de ficheros (información) los convierten en un estándar. Al ser los formatos propietarios, la mayoría de las veces no es posible crear programas que puedan trabajar con esos formatos (por no ser públicos), y de esta manera se elimina la competencia, lo que se traduce en peor calidad para el usuario. Mediante el software libre sería posible que varias empresas fabricaran sus propios procesadores de textos, hojas de cálculo, etc, y de esta forma los usuarios tendriamos la posibilidad para elegir entre varios productos, pudiendo así comunicarnos e intercambiar información con usuarios que utilizar un software diferente al nuestro.

¿Es más seguro el software libre que el propietario?

El software libre no es más seguro que el propietario, ni el propietario lo es más que el software libre. El que un determinado software sea seguro no depende de si se distribuye junto con su código fuente (una de las diferencias entre entre estos tipos de software). Un software es seguro cuando ha sido bien desarrollado y se utiliza de forma correcta, y esto es independiente de la forma bajo la que se distribuya. Sin embargo, el software libre es más transparente que el software propietario, ya que permite comprobar que fue desarrollado de forma correcta.

Otra de las ventajas del software libre es que está basado en estándares abiertos, es decir cualquier empresa puede crear un programa que maneje la información que genera en ese software. De ese modo no se produce una dependencia tecnológica hacía una determinada empresa. Siempre es el usuario quien elige el programa con el que manejará sus datos, pudiendo cambiar su elección cuando lo desee, ya que la información estará almacenada en formatos estándar, que pueden ser manejados por otros

programas diferentes al nuestro. Un ejemplo de esto son los ficheros jpg o png: cada usuario puede utilizar el programa que más le guste para ver las imágenes almacenadas en estos formatos, ya que son formatos públicos.

¿El software libre es gratuito?

Aunque la mayoría del software libre es gratuito, no tiene por qué ser así. Las licencias de software libre obligan a distribuir el software junto con su código fuente y permiten al usuario modificarlo y distribuirlo.

Para terminar este artículo quisiera hacerle recapacitar sobre algo:

Imagínese Ud. que va a comprar un coche y las condiciones de compra son:

1. Ud. sólo puede circular con su coche por la provincia en la que reside. Si quisiera circular por otra provincia diferente necesitaría pagar más dinero en concepto de licencia.
2. No podrá ceder ni alquilar su coche.
3. No podrá modificarlo de ninguna manera, no podrá ponerle otro radio-cassette, colgarle unos dados del retrovisor, cambiarle los neumáticos cuando estén gastados ... Para hacerlo tendrá que solicitarlo al vendedor y obviamente le cobrarán por ello, y al sólo poder hacer las modificaciones el vendedor ¿se imagina cómo serán las tarifas?
4. No podrá abrirlo/desmontarlo para estudiar su funcionamiento.

¿Compraría un coche en estas condiciones? Seguro que no. Entonces, ¿cuál es la razón de comprar software propietario bajo unas condiciones similares? Cuando compra un software propietario, si se molesta en leer la licencia que lo acompaña, verá que:

1. Sólo podrá instalar el software en un determinado número de equipos, requiriendo el pago adicional, en concepto de licencias, de más dinero si quisiera instalarlo en más equipos.
2. Ud. no puede ceder ni alquilar el software que acaba de comprar.
3. No puede modificarlo de ninguna manera. El único que puede hacerlo es el desarrollador y en las condiciones que considere oportunas (y siempre y cuando le salga rentable).
4. No podrá realizar ingeniería inversa para estudiar su comportamiento.

Como puede ver, el software libre ofrece más ventajas que la transparencia para los usuarios. Espero que este artículo les sirva para entender un poco más este mundillo y sobre todo para que sean conscientes de los peligros que existen a la hora de utilizar un determinado programa, sobre todo cuando no se sabe cómo está hecho.