Ética y Seguridad en la red

Fernando Tricas García
Dpto. de Informática e Ingeniería de Sistemas
Centro Politécnico Superior de la Universidad de Zaragoza
http://www.cps.unizar.es/ ftricas/
ftricas@unizar.es

1. Introducción

El mundo de la información y la comunicación ha cambiado: el modo en que adquirimos, almacenamos y diseminamos el conocimiento cada vez se parece menos a los modos usados tradicionalmente. El motivo fundamental es el tratamiento automatizado de la información que nos facilitan los computadores.

Sin embargo, y aunque los medios y sistemas utilizados están disponibles desde hace algún tiempo, todavía no llegamos a comprender completamente las consecuencias de su uso. Aún más, conforme su uso se extendiende, estamos viendo como la la situación se complica.

Estamos pasando muy rápidamente del uso de estas tecnologías por parte de comunidades restringidas con necesidades y capacidades muy específicas, a la generalización de su uso en aspectos muy diversos de la vida diaria, por parte de personas con muy diferentes intereses. Evidentemente, esto es así en la mayoría de los casos por los claros beneficios obtenidos. Pero ningún avance tiene sólo beneficios y ventajas: si adquirir, almacenar y diseminar información es cada vez más sencillo, también lo es hacer esas mismas cosas con fines diferentes a los iniciales.

Algunas de las facetas que pueden verse perjudicadas por estos avances son nuestra privacidad, y la seguridad de los datos almacenados por medios electrónicos: cuantos más datos nuestros estén informatizados, más posibilidades existen de que alguien que nosotros no hayamos previsto, pueda tener acceso a los mismos. No hace mucho, para obtener datos acerca de nosotros y de nuestros asuntos privados, un ladrón tenía que ir a nuestra casa o a nuestro centro de trabajo, y robar los documentos (o, al menos, copiarlos); ahora, basta con que sea suficientemente hábil para acceder a nuestro computador mientras nos conectamos a la red (para leer el correo electrónico, o charlar con los amigos en el IRC) y obtener la información sin que, tal vez, lleguemos ni siquiera a notarlo. Peor aún, puede ocurrir que nuestros datos sean obtenidos de los computadores de otros en los que, con nuestro conocimiento o sin él, están almacenados.

Aunque los motivos son muy variados, fundamentalmente podemos hablar de dos aspectos que inciden directamente en el problema: motivos técnicos (esen-

cialmente la forma en que se transmite y almacena la información) y motivos sociales/culturales (básicamente por el modo en que se usa la tecnología y por las personas que la usan).

En lo que sigue vamos a hablar de estos temas, tratando de dar una visión de cuáles pueden ser los principales problemas a los que nos podemos enfrentar y algunas ideas de autoprotección.

Comenzaremos con algunas definiciones; hablaremos sobre las formas de atacar nuestra seguridad (y la de otros) y la privacidad; tabién trataremos de dar algunas reglas de autoprotección; casi al final, hablaremos de como proteger la confidencialidad y, finalmente, daremos algunas indicaciones sobre donde buscar más información.

2. Definición de Privacidad

Seguramente está bastante claro, y todos tenemos una idea de a qué nos estamos refiriendo pero, ¿qué es la privacidad?. Antes de tratar de preservarla, seguramente conviene recordar su significado, aunque sólo sea para hacernos una idea de la complejidad del asunto. Por ejemplo, el diccionario ESPASA [**?**], entre otras da las siguientes definiciones:

> PRIVADO, DA adj: Que se ejecuta a la vista de pocos, familiar y domésticamente, sin formalidad ni ceremonia alguna || Particular y personal de cada uno.

En ese mismo diccionario, también aparece la definición de un término relacionado:

> INTIMIDAD: Parte personalísima, comúnmente reservada, de los asuntos, designios, o afecciones de un sujeto o de una familia.

Permítasenos citar también un texto extranjero, que se usa como referencia en el mundo anglosajón para asuntos lingüísticos. Del *Oxford English Dictionary*, ([**?**]), seleccionamos algunas definiciones:

> PRIVACY (from private) The state or quality of being private.
>
> The state or condition of being withdrawn from the society of others, or from public interest; seclusion. || The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; freedom from interference or intrusion. Also attrib. designating that which affords a privacy of this kind. 'one's right to privacy'.

Finalmente, la definición de la Wikipedia
(http://en.wikipedia.org/,
en inglés:
(http://en.wikipedia.org/wiki/Privacy):

> PRIVACY is the ability of an individual or group to stop information about themselves from becoming known to people other than those they choose to give the information to.

Y en nuestro idioma (http://es.wikipedia.org/wiki/Privacidad):

> La PRIVACIDAD es un ámbito de la vida de una persona que se desarrolla en un espacio privado, protegido por las leyes básicas de cualquier democracia.

Para una visión más completa sobre la privacidad, puede utilizarse, por ejemplo, [**?**], o [**?**]. Cualquier búsqueda sobre el tema en la red da suficientes referencias.

2.1. Privado vs. Público

En algunos foros, sobre todo a raíz de grandes catástrofes o amenazas del exterior, cuestionan el acceso a las herramientas que permiten la privacidad: ¿no estaremos ayudando a los 'malos' a que su trabajo sea más fácil?. Se trata de un problema delicado pero, como casi siempre, es muy probable que la solución no venga por la vía de las prohibiciones, puesto que la tecnología ya está disponible y su prohibición o hacer más difícil su acceso, no va a impedir la difusión, ni hará que desaparezcan las que ya están usando.

3. Ataques a la privacidad/seguridad

Es cierto que la mayoría de los usuarios de la red son como nosotros: esto es, personas que la utilizan para comunicarse con sus semejantes, sin demasiado interés en interceptar y recopilar información privada de otras personas. Esto puede inducirnos a una errónea sensación de seguridad: '¿quién puede estar interesado en mi persona?'. Si bien esto puede ser cierto para la mayoría de nosotros, no debemos perder de vista que aunque es muy posible que seamos personas poco relevantes o interesantes desde el punto de vista de la información que poseemos, por razón de nuestro trabajo o las actividades que desarrollemos podemos tener acceso a información de terceras personas (han sido tristemente famosos los casos de cientos de computadores infectados con troyanos y que fueron utilizadas para provocar ataques de denegación de servicio -realizando, por ejemplo, tantas peticiones a un servidor simultáneamente que deja de responder a las peticiones legítimas, de usuarios normales- llegando a poner en aprietos a redes tan importantes como las de Microsoft o Yahoo!).

También puede darse el caso de que seamos utilizados como simples medios para atacar a otros. Finalmente, no es menos cierto que en muchos casos los ataques no se hacen buscando información concreta, sino con fines destructivos (sin ni siquiera tener acceso real a la información) o como prueba de concepto (sería sencillo modificar uno de los últimos virus que se diseminaban utilizando la libreta de direcciones de algunos lectores de correo populares, para reenviar a la

dirección que se quisiera determinado fichero o conjunto de ficheros del sistema): en los medios de comunicación han recibido bastante difusión los virus y troyanos de difusión masiva, pero no hay datos fiables sobre la utilización de las técnicas mostradas en esos virus para la obtención de datos concretos de personas o empresas individuales. De lo que si que hay constancia es de actualmente hay mafias que controlan miles de máquinas de usuarios despistados y que alquilan sus servicios para diversos cometidos: desde enviar spam (publicidad no deseada) a robar datos de clientes bancarios (Phising y otras técnicas), pasando por los antedichos ataques de denegación de servicio.

Más adelante hablaremos de cómo preservar la confidencialidad de los datos, pero antes vamos a hablar un poco sobre los ataques que podemos sufrir.

- **Acceso físico a los recursos:** nada de lo que digamos en lo sucesivo tendrá la más mínima utilidad si el medio que utilizamos para el almacenamiento (computador, disquete, CD-ROM) puede ser accesible, y por lo tanto utilizable por terceros. Bien porque está ubicado en algún lugar de acceso común, bien porque el propio recurso es de uso común.

- **Técnicas de ingeniería social:** está uno charlando tranquilamente en un canal de IRC, o a través de una lista de correo y alguien, muy amablemente, nos informa de que nuestro computador tiene algún problema. Él se ofrece a ayudarnos, para lo que tenemos que ejecutar un programa que nos proporciona, o darle nuestra clave para que lo soluciones él por nosotros; un poco más tarde (o tal vez nunca) nos damos cuenta de que nos han tomado el pelo. Hay cientos de formas de hacer cosas como esa, y a diario se producen muchísimos ataques de este tipo; hay que ser extremadamente cuidadoso con lo que se hace en estos casos.

  Tambien entran dentro de esta categoría los mensajes que recibimos, aparentemente de nuestro banco, sugiriéndonos que pinchemos un enlace o que introduzcamos nuestros datos en la página que nos envían. O las cartas (correos electrónicos, claro) que nos invitan a instalar programas, abrir documentos, y otras muchas acciones.

  Aparentemente, se trata de avisos inofensivos (o incluso buenos para nosotros) y habitualmente se corresponden con amenazas a nuestra seguridad o la de nuestros datos.

- **Virus, troyanos, programas maliciosos:** desde los ya clásicos virus (cuyo efecto puede ser la destrucción del contenido almacenado, o efectos más o menos molestos en el uso de la máquina) a los troyanos (cuya misión puede ser desde la simple auto-replicación y por tanto, su propia supervivencia, al envío de información contenida en nuestra propia máquina, pasando por la instalación de programas 'durmientes' que esperan a las ordenes del que los instaló proporcionando acceso completo a nuestros recursos -quién sabe desde dónde- para ser utilizados, en algunos casos, en diversos ataques contra terceros; un ejemplo de estos últimos son los utilizados para ataques de denegación de servicio distribuida –DDOS:

Distributed Denial of Service– que se utilizan para colapsar un servidor o conjunto de servidores, y que se instalan y controlan mediante el uso del IRC). En cualquier caso, todos ellos comparten la forma de infección: casi siempre se trata de conseguir que ejecutemos el código malicioso en nuestro computador; una vez ejecutado, el daño está hecho. Las vías de entrada de la infección, sin embargo, son múltiples:

- Virus tradicionales y troyanos: habitualmente están añadidos como parte del código de otros programas ejecutables normales que conseguimos en la red, o a través de otras personas (disquetes, etc.). La ejecución del programa conlleva la ejecución del código malicioso, y por tanto la infección. Hay variantes sobre esto, pero la idea siempre es bastante parecida. A las formas ya nombradas de infección se añaden algunas nuevas como pueden ser el intercambio de ficheros P2P (estilo eMule y similares), el IRC, etc, y los ficheros adjuntos envíados mediante correo electrónico.
- Ficheros de contenidos para aplicaciones ofimáticas con capacidades programables: los ficheros con .doc y .xls (entre otros) no sólo contienen textos, números y fórmulas, sino que también pueden contener miniprogramas perniciosos. No sólo estos: dadas las características de los programas que los manejan, un .doc con contenido peligroso puede renombrarse a .rtf (este último formato puede considerarse seguro, puesto que no admite las características de programación) cuando Word lo abra, se 'dará cuenta' de que es un .doc, y lo abrirá como tal, encontrándonos con los posibles problemas. No sólo podemos encontrar problemas con ficheros de estos tipos; no conviene olvidar que el sistema operativo de uso mayoritario (Windows), oculta la extensión de los ficheros en su configuración por defecto, eso puede ser aprovechado para introducirnos un virus de macro con el nombre LEEME.TXT.DOC. El sistema, ocultará 'amablemente' la extensión .DOC, nosotros lo abriremos, y cuando nos demos cuenta de lo que es, ya será tarde.
- Aplicaciones de visualización de datos con capacidades programables: es bastante habitual enviar mensajes escritos con marcas de .html de manera que los mensajes adquieren un aspecto visual más atractivo (todo es opinable, claro), pero también más peligroso. Dentro de las etiquetas en .html (inofensivas) puede integrarse código en diversos lenguajes de programación (java, javascript, Visual Basic Script, ...) que, si bien pueden utilizarse para mejorar el aspecto de lo enviado, también se pueden utilizar para forzar la ejecución de código malicioso.

4. Algunas reglas básicas de autoprotección (El arte de la prudencia)

A continuación relacionamos algunas normas de protección frente a infecciones, aunque la regla fundamental, como dice el título, debería ser la prudencia:

- Disponer de un antivirus (y utilizarlo para comprobar cualquier programa nuevo o fichero sospechoso, antes de ejecutarlo); como mínimo, debería ser actualizable (y actualizado) periódicamente siguiendo las normas del fabricante.
- Suscribirse a las listas de avisos de seguridad de los programas que utilicemos habitualmente (si las hay) y actualizarse cuando el fabricante proporcione modificaciones que afecten a dicha seguridad.
- Nunca ejecutar programas ni abrir ficheros en aplicaciones con capacidades de programación, que provengan de fuentes no confiables (los amigos no siempre lo son, recordemos los virus y troyanos transmitidos en los últimos tiempos mediante reenvío automático utilizando la libreta de direcciones). Incluso cuando vienen de conocidos, si son envíos que no esperábamos, haremos bien en preguntar sobre ellos, porque en algunos casos, los programas maliciosos son capaces de alterar la procedencia del mensaje para que parezca que viene de alguien conocido.
- Si su sistema operativo permite establecer perfiles de usuario, úselos. Eso le permitirá hacer su trabajo normal con un perfil sin permisos para borrar/modificar programas importantes de su sistema.
- Configurar adecuadamente los programas que interaccionan con el exterior (navegadores, lectores de correo, programas de IRC, ...) para que no ejecuten automáticamente programas desconocidos.
- Nadie necesita (ni nosotros tampoco) enviar documentos en formatos potencialmente peligrosos. Es más seguro y conveniente (ocupan menos espacio) enviar solamente texto, o cuando el aspecto es importante, formatos orientados a la visualización considerados seguros (.ps, .pdf, imagenes, ...). El .html también puede ser peligroso, teniendo en cuenta lo que puede contener.

  Salvo que estemos trabajando con alguien en la elaboración de un documento, no tiene mucho sentido mandarlo en Word, por ejemplo: sería como ir al médico a que nos cure una herida y que nos proporcionara alcohol, vendas y esparadrapo y un folleto explicando como hacernos la cura. No es la primera vez tampoco que alguien ha desvelado más datos de los que quería por utilizar un formato de esos en los que no se guarda sólo nuestra carta, sino la historia de cómo se ha realizado con, tal vez, alguna frase que borramos en su día, o datos que eliminamos después de pensar mejor sobre ellos.

- Estar preparados para lo peor: si surge un nuevo virus y recibimos un programa infectado antes de actualizar nuestro modernísimo antivirus, no estamos protegidos. Por lo tanto, es bueno hacer copias de seguridad frecuentes de nuestros datos importantes, de modo que aunque se produjera la destrucción de nuestros ficheros, siempre podamos recuperar una versión razonablemente reciente (lo de cuánto es razonable, deberemos decidirlo nosotros). Naturalmente, la copia debe realizarse en un medio de almacenamiento separado del propio computador (o que no se pueda alterar). Por ejemplo: otro disco duro, cintas, CD-ROM.

- Instalar y configurar adecuadamente un cortafuegos (*firewall*); su utilidad es permitir el acceso a través de puertos y protocolos autorizados por nosotros, de forma que cualquier intento de acceso extraño puede ser detectado y evitado.

  La estrategia correcta sería: 'nada está permitido' y, a partir de allí, autorizar sólo lo que nos parezca necesario y/o conveniente (porque sepamos que es razonable y seguro).

5. Confidencialidad de los datos

Si logramos mantener nuestro computador libre de los problemas anteriormente mencionados, manteniéndonos libres de virus y otros programas maliciosos, ya tenemos una parte de la guerra ganada. En cualquier caso, no debemos olvidar que nuestro objetivo es comunicarnos con otras personas, que pueden no tener las cosas tan claras. Todavía más, hay que tener en cuenta cómo viaja la información por la red: Internet no fue diseñada para ser segura, sino fiable y robusta; esto es, cuando se conectan dos computadores, lo importante es que la conexión se produzca y la transmisión funcione correctamente. Por este motivo, de los múltiples caminos que pueden existir para interconectar dos computadores, no hay ninguno predeterminado, y cualquiera de ellos puede ser elegido para la transmisión. De este modo, la información se va transmitiendo entre pares de nodos intermedios, sobre los que a menudo no tenemos ningún conocimiento, ni mucho menos control. Los peligros a los que nos enfrentamos son los siguientes:

- Alguien puede 'escuchar' la comunicación entre los dos puntos, sin que seamos capaces de detectarlo.

- Alguien puede generar información, y transmitirla a otros haciéndose pasar por nosotros.

- Alguien puede interceptar nuestra comunicación, modificándola del modo que le parezca conveniente.

- Debido a los últimos dos peligros, podemos generar una información, transmitirla, y después negar haberlo hecho, alegando haber sido víctimas de alguno de los ataques señalados.

Para evitar estos problemas, se utiliza la criptografía, mediante la cual podemos dar cuenta de cada uno de los puntos anteriores.

Las redes inalámbricas (WiFi) que resuelven tantos problemas de comunicación de manera cómoda y conveniente son un ejemplo de como podemos simplificarle la vida a los 'malos': si no las usamos con los niveles de protección adecuados, estamos haciendo que un posible atacante ya no necesite ni siquiera acceder al cable para 'robarnos'. Bastará con que disponga de una antena y se coloque en las inmediaciones de donde estemos.

Respecto a estas redes, algunos consejos generales pueden ser:

- Cuidado con las claves: no teclear claves de sitios importantes, si no estamos seguros de que van a ir desde nuestro computador al servidor cifradas.
- Implantar un control de acceso con autentificación bidireccional (nosotros 'reconocemos' al punto de conexión y el punto de conexión nos 'identifica' a nosotros).
- Configuración WEP (Wired Equivalent Privacy) con 128 bits o, mejor, WPA (Wi-Fi Protected Access), en su versión 2 si es posible.
- También hay sistemas que permiten la variación en las claves a lo largo del día, de forma que si alguien robara la clave en algún momento, no le sería de utilidad en otro momento diferente.
- Control de radio de transmisión: puede ser interesante conocer (y, en algunos casos, tratar de limitar o redirigir) qué alcance tienen nuestros puntos de acceso y desde donde son visibles (esto es, desde qué lugares puede alguien conectarse).
- Estar atentos ... todo cambia muy rápido todavía

5.1. Breve historia de la criptografía

La criptografía es tan antigua como la escritura: siempre que ha habido comunicación entre dos personas, o grupos de personas, ha habido un tercero que podía estar interesado en interceptar y leer esa información sin permiso de los otros. Además, siempre que alguien esconde algo, hay personas interesadas en descubrirlo, así que ligado a la ciencia de esconder (la criptografía), se encuentra casi siempre la de descifrar (el criptoanálisis).

El primer cifrado que puede considerarse como tal (por tener evidencias no sólo del cifrado, sino también una metodología e instrucciones para llevarlo a cabo) se debe a Julio César: su método consistía en sustituir cada letra de un mensaje por su tercera siguiente en el alfabeto. Parece ser que también los griegos y egipcios utilizaban sistemas similares. Civilizaciones anteriores, como la Mesopotamia, India y China también utilizaban sus propios métodos.

Estos sistemas tan simples evolucionaron posteriormente a elegir una reordenación cualquiera (una permutación) del alfabeto, de forma que a cada letra se le hace corresponder otra, ya sin ningún patrón determinado (ss. XV-XVI).

Durante la I Guerra Mundial se utilizaron extensivamente las técnicas criptográficas, con no muy buen resultado, lo que impulsó al final de la guerra, el desarrollo de las primeras tecnologías electromecánicas. Un ejemplo de estos desarrollos es la máquina Enigma, utilizada por los alemanes para cifrar y descifrar sus mensajes.

Es un dato muy revelador saber que el cifrado de estas máquinas fue roto (descubierto) incluso sin disponer de ningún ejemplar de las mismas, por un mal uso por parte de algunos operadores: nuevamente descubrimos ejemplos de como los aspectos sociales relacionados con la tecnología también son importantes. No basta sólo con las máquinas, hace falta que las personas hagamos nuestra parte del trabajo adecuadamente.

Todos los métodos comentados anteriormente pueden ser más o menos seguros, dependiendo de la complejidad del sistema, del tiempo y la información adicional de que disponga el atacante; en cualquier caso, todavía tienen los siguientes inconvenientes:

- Solamente dan cuenta del problema de la confidencialidad (primer punto de los comentados anteriormente): sirven para dificultar las escuchas, pero no sirven para afrontar ninguno de los otros tres problemas reseñados.
- Hacen falta dos claves por persona con la que nos queremos comunicar (la que nos dé él, y la que usamos para él).
- Para intercambiar las claves, es preciso un contacto personal, o bien, una comunicación a través de un medio seguro y no interceptable.

Como ventajas, cabe destacar su simplicidad y rapidez, que la hace fácil de usar en muchos contextos.

Afortunadamente, la criptografía actual tiene resueltos estos problemas, mediante la codificación basada en sistemas de clave pública. Cada persona tiene dos claves: una privada (esto es, sólo la conoce y maneja él) y una pública (esto es, accesible por quien la solicite). Estas claves (junto con el sistema de cifrado) satisfacen la siguiente propiedad: lo que se codifica utilizando una de ellas, se decodifica con la otra, de manera que utilizando las dos de modo consecutivo obtenemos el mensaje original.

- **Confidencialidad** Cuando queremos enviar un mensaje a una persona, lo codificamos con su clave pública. De esta forma sólo él puede descifrarlo, utilizando su clave privada.
- **Autenticidad** Sólo nosotros podemos codificar el mensaje con nuestra clave privada, y cualquiera puede leerlo con la pública. Esto sirve para garantizar el origen del mensaje. Habitualmente, en lugar de cifrar el texto del mensaje completo, se extrae un resumen del texto (mediante su adecuada transformación: nótese que no sirve cualquier resumen puesto que para mensajes diferentes deberíamos poder obtener resúmenes diferentes que imposibiliten la confusión) y es este resumen lo que se codifica y adjunta al final del mensaje. En este caso hablamos de **firma digital**.

- **Integridad** Si la forma de obtener el resumen del punto anterior es correcta, dos mensajes diferentes tendrán resúmenes diferentes. En consecuencia, un mensaje modificado tendría un resumen diferente del original.
- **No repudio** Cuando el mensaje lleva nuestra firma, o está cifrado con nuestra clave privada, sólo podemos haberlo generado nosotros.

Ahora, según el nivel de seguridad que necesitemos, podemos utilizar:

- La clave pública del receptor.
- Nuestra clave privada.
- Ambas.

Nótese que con este cifrado en dos partes, el secreto lo proporciona la clave del receptor (sólo él puede descifrarlo) y la autenticidad del mensaje la proporciona mi clave (sólo yo tengo mi clave privada). Las características más relevantes de este sistema son:

- La parte pública de mi clave es conocida por todo el mundo.
- La parte privada de mi clave no es transmitida por ningún medio, siendo mucho más sencillo conservarla secreta.
- El uso de la clave pública del receptor garantiza que sólo él podrá leerlo.
- El uso de mi clave privada garantiza que sólo yo he podido generarlo (salvo robo, claro).
- Para comunicarse con varias personas, sólo necesitamos una clave por cada una de ellas (la pública).

Como inconvenientes de este tipo de sistemas, podemos hablar de la lentitud (necesitan operaciones con números grandes, que son muy costosas), y la necesidad de autoridades de certificación, que acrediten cuál es la clave pública de una determinada persona o entidad.

6. Algunos datos más

Se habla con frecuencia de la cantidad de contenidos indeseables y de poca calidad que hay en la web. Está claro que es nuestro criterio el que debe ayudarnos a decidir eso y que la tarea de selección de los contenidos tiene más que ver con nuestro propio (buen) juicio que con lo que hay en la red. De hecho, textos y fotografías que a nosotros podrían parecernos perfectamente aceptables y adecuados, en otras culturas pueden no serlos, asi que no parece que la simple censura o prohibición vayan a solucionar el problema. Por supuesto, siempre habrá quien exceda todas las convenciones y ponga a disposición de otros contenidos ilegales; eso no debe impedir que nosotros seamos capaces de explorar la

parte de la red que nos resulte conveniente. También existen sistemas de filtrado que aseguran protegernos de contenidos indeseables, aunque habitualmente tienen dos inconvenientes:

- ¿Quién decide qué es inconveniente y en base a qué? Imaginen un filtro basado en palabras utilizado por un médico que estudia el cáncer de mama.
- La segunda, y mas grave es la falsa sensación de seguridad: nada (ni nadie) nos garantiza que uno de esos filtros vaya a controlar perfectamente todo lo que llega a nuestra pantalla (o a la de nuestros hijos) asi que, aunque pueden ayudarnos en el control, nada suplirá al que nosotros hagamos personalmente.

Entre los contenidos indeseables que pueden llegar a nuestro computador se encuentran los temidos virus, troyanos y, en general, programas maliciosos.

En principio, cualquier programa 'extraño' (que viene del exterior) que ejecutemos es potencialmente peligroso; deberíamos tener muy buenas razones para descargar y ejecutar programas de los que no conozcamos perfectamente su procedencia. Esto es cierto incluso para programas que nos pueden parece útiles e interesantes (algunas empresas utilizan aplicaciones sencillas y atractivas para instalar programas indeseables). Siempre que instalemos programas, deberíamos hacerlo de fuentes reconocidas y, si es posible, que esté disponible el código fuente, como garantía de que no esconden nada 'feo' (aunque nosotros no sepamos leer ese código fuente ni interpretarlo, seguramente hay personas que pueden hacerlo por nosotros).

Pero ... ¿Qué es un virus? ¿Y un gusano? ¿Y un troyano? Vamos a dar a continuación algunas definiciones para situar estos términos que se escuchan con tanta frecuencia.

- Un virus es un programa de ordenador que puede infectar a otros programas modificándolos para incluir una copia de sí mismo.

  Fred B. Cohen, fue el primero que mostró como construir uno por lo que se le considera el primer autor de virus 'autodeclarado' en el 1984 en su tesis doctoral. Habitualmente se trata de programas destructivos, molestos, ...

- Un gusano es un programa que se reproduce, como los virus, pero que no necesita de otros programas para retransmitirse. Ellos mismos tienen los mecanismos adecuados para viajar por la red e infectar a los computadores.

- Finalmente, un troyano es un programa malicioso que se oculta en el interior de un programa de apariencia inocente. Cuando este último es ejecutado el Troyano realiza la acción o se oculta en la máquina del incauto que lo ha ejecutado. Frente a lo que puede sugerir la terminología habitualmente usada, conviene recordar que la historia nos dice que el caballo de Troya fue introducido en la ciudad y los troyanos fueron los atacados, justo al revés de como se usa el nombre en este ámbito.

La terminología de los programas maliciosos ('malware' en inglés) no acaba aquí y últimamente se oye hablar mucho de 'spyware' (programas espía). Se trata de programas que no afectan al funcionamiento de nuestro computador ni molestan en nuestra actividad diaria pero que se dedican a almacenar y enviar datos sobre nuestra navegación: desde qué sitios visitamos (y cuando) en los casos mas benignos a robar claves y otro tipo de información más importante. Sin olvidarnos de los marcadores telefónicos ('dialers') que sustituyen nuestra conexión habitual por una mucho más cara.

Hay muchas formas de infectarnos. La más tradicional que es como se propagan los virus es mediante la copia de programas que previamente estaban infectados. Pero también es posible, como decíamos arriba, a través de programas con efectos graciosos, pequeñas utilidades, felicitaciones, bromas, ... Incluso ha habido casos de falsos detectores de virus y de programas espía que descubrían los programas maliciosos ' de la competencia' pero no avisaban de los que pretendían ocultar. Además, las vías de llegada se han multiplicado: redes de intercambio de ficheros, IRC, mensajería instantántanea, correo electrónico, la web, ...

Hace un par de años fue bastante comentado el caso de MyDoom. Era un gusano (también conocido como Novarg, Shimgapi, Shimg, Mimail.R), que se propaga a través del correo electrónico (automáticamente y de KaZaa (una de las redes p2p, aprovechándose de las malas costumbres de algunos internautas). Comenzó su propagación el día 26 de enero de 2004 y todavía hoy se detectan variantes suyas en la red. Algunas de sus características son:

- Una de las formas de distribuirse era a través de adjuntos de correo, con alguna de las siguientes extensiones: .BAT, .CMD, .EXE, .PIF, .SCR y .ZIP
- El icono en Windows simula ser el de un fichero de texto (no fiarse de los iconos, mejor mirar la información sobre el archivo).
- La dirección de origen del correo es falsa.
- El asunto ('Subject:') del mensaje era variable, podíamos recibir uno de estos: "Error", "Status", "Mail Transaction Failed", "hello", "hi".
- También era capaz de generar el contenido del mensaje variable ...
- Entre sus efectos están:
  - Generar un fichero "Message" en el directorio temporal de Windows
  - Introducir "shimgapi.dll" y "taskmon.exe" en el directorio de sistema (system) de Windows.
  - Abre "Message" (con caracteres al azar) en el bloc de notas, con el objetivo de distraer al usuario y hacerle pensar que ese es todo el efecto de la infección (nuevamente ingeniería social).
  - Busca direccciones de correo y se auto-envía.

- Intenta reproducirse mediante Kazaa, con nombres 'sugerentes': winamp5, icq2004-final, activation_crack, strip-girl-2.0bdcom_patches, rootkitXP, office_crack, nuke2004
- Abre el puerto TCP 3127 (¿puerta trasera? -virtual, claro-)
- Es capaz de enviar hasta 1000 mensajes por minuto; en los momentos mas graves de la infección se estimó que 1 de cada 12 mensajes de correo estaba infectado. De esta forma, una máquina infectada envía muchísimo correo (y también lo recibe, claro).
- Se trataba de un ataque contra SCO que dejó de realizarse el 12 de febrero. Algunas variantes se han utilizado después para atacar a otros sitios, aunque se piensa que actualmente simplemente se está utilizando para acumular computadores infectados que puedan usarse para lo que decida el 'comprador'.

Entre los ataques similares anteriores cabe destacar SoBig, en agosto de 2003, que causó millones en pérdidas (se estimaba que 1 de cada 17 correos estaba infectado). Slammer, en enero de 2003 fue uno de los más rápidos, dejando fuera de juego a la red de cajeros del 'Bank of America' infectando a la mayoría de sus 13000 cajeros automáticos. De hecho, infectó el 90 % de los servidores vulnerables en los primeros 10 minutos.

Otro problema creciente es el 'Phising': consiste en engañar al usuario para que visite una web falsa, que emula a la de un banco o alguna entidad y hacerle proporcionar sus datos, para robárselos. El consejo aquí es claro: nunca fiarse de este tipo de mensajes o sugerencias. En caso de querer comprobar que todo va bien con nuestro banco, lo mejor es conectarnos directamente a su web (usando los favoritos, o tecleando la dirección). En temas de seguridad son muy importantes las (buenas) costumbres y no dejarse llevar por la urgencia de un aviso, o por las sugerencias de nadie.

De todas formas, la palabra que se ha puesto de moda últimamente es el 'Pharming': se trata de explotar un fallo en el servicio de gestión de nombres de internet (DNS), de forma que cuando nos conectamos a una dirección mediante el nombre `www.miBanco.com`, nos redirigirían a un sitio diferente del que queremos ir. Esto es así porque el mecanismo de internet se basa en direcciones IP que son números. Por ejemplo `www.uninet.edu` corresponde, en realidad, a la dirección IP `193.146.180.65`. El mecanismo de los nombres se ideó para que no tuviéramos que acordarnos de los números, sino de nombres que son más fáciles de recordar. La traducción la hacen unos computadores especializados en la gestión de nombres de dominio (los servidores de DNS).

Esencialmente hay dos formas de realizar este tipo de ataques:

- Una sería atacar a un servidor de nombres (para engañar a sus usuarios); contra este tipo de ataque poco podemos hacer, porque todos ocurre fuera de nuestro control. De esta forma alguien podría cuando

tratamos de consultar `www.uninet.edu` enviarnos a, pongamos, tt 123.231.123.231 y allí pone un sustituto de lo que esperábamos ver.

De todas formas, es difícil de realizar y no ocurren ataques de este tipo con demasiada frecuencia.

- La otra es mas frecuente, y sobre ella tenemos algo de control: consiste en modificar la información local de nuestro computador para hacerle ir a una dirección diferente de la que se debería cuando se conecta.

  Se trata de hacer que cuando nuestro computador vaya a conectarse a `www.uninet.edu`, no haga la consulta de la dirección al servidor de nombres, sino que utilice información local. Para eso existe un fichero, que en Windows suele estar en

  `C:\Windows\system32\drivers\etc\hosts`

  y en Linux y otros sistemas tipo Unix en

  `/etc/hosts`

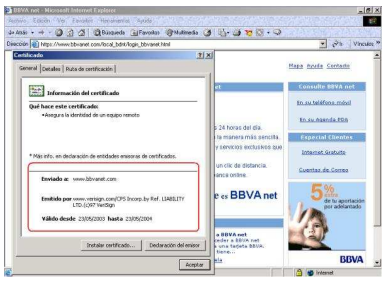
  Si añadimos una línea que asocie una dirección IP a un nombre, cuando tratemos de usar ese nombre, el computador no consultará al servidor de nombres sino que utilizará directamente la que haya allí. Creo que ya vamos viendo donde está el problema: asi como decíamos que atacar a los servidores de nombres era bastante complicado, modificar ficheros en las máquinas de los usuarios no lo es tanto.

  Sin embargo, contra esto si que podemos tomar algunas medidas:

  - Tener la máquina tan 'limpia' como sea posible: el antivirus, el cortafuegos, todas las herramientas de seguridad harán que sea más difícil que los programas maliciosos nos afecten.
  - Proteger el fichero `hosts`: comprobar manualmente que no tiene información extraña (debería ser un fichero muy corto, con muy pocas líneas). Si es posible, cambiarlo para que su forma de acceso sea de sólo lectura.
  - Ante la más mínima sospecha de que algo ha ido mal, preguntar: los bancos tienen números de teléfono a los que podemos llamar para asegurarnos de que no ha pasado nada raro.

En todo caso, cuando nos conectemos a un sitio web en el que vayamos a gastar o gestionar nuestro dinero (un banco, compras en la red, etc.) deberíamos ser prudentes y, como mínimo, comprobar:

- Que la conexión se hace cifrada (utilizando **https**). Pero cuidado, esto sólo garantiza que la conexión es cifrada, no que sea 'la buena'. Hay que hacer más comprobaciones:
  - Comprobar que la dirección coincide con lo que esperamos (nunca pinchar en direcciones que nos envíen, acceder como normalmente; si es imprescindible: copiar y pegar, la dirección, **nunca** pinchar).



  - Comprobar el certificado de autoridad (esa información se puede comprobar pinchando en el cerrojo amarillo -que debería estar cerrado- para ver que efectivamente la dirección corresponde con la que queríamos conectarnos).
- En caso de duda ... teléfono, visita a la sucursal...

Algunas medidas más que podemos aplicar, sobre todo si nos conectamos desde computadores compartidos con otros pueden ser borrar el historial (el navegador almacena los sitios que hemos visitado) después de navegar.

6.1. Más medidas

Mantener actualizado el sistema operativo y los programas: todos los fabricantes proporcionan mejoras de seguridad cuando se descubren problemas en sus programas: es nuestra tarea instalar esas actualizaciones y mantener nuestro equipo a salvo.

Por ejemplo, Microsoft proporciona actualizciones para sus productos todos los segundos martes de cada mes. Se puede acceder con nuestro navegador a las actualizaciones (lamentablemente, sólo con Explorer) en

http://windowsupdate.microsoft.com/.

También podemos programar para que las actualizaciones se hagan automáticamente, como explican en

http://support.microsoft.com/default.aspx?scid=kb;es;327838.

El peligro de los automatismos en estas cosas es que nos olvidemos de ellos y cuando por alguna razón fallen, no nos demos cuenta de que no se están realizando.

A pesar de que tengamos un sistema muy seguro, y tengamos mucho cuidado y todo el mundo a nuestro alrededor lo tenga, las desgracias ocurren. No existe una política de seguridad perfecta, ni existe el escudo de protección 'anti–todo': todo lo que hemos dicho hasta ahora debería complementarse con la realización de copias de seguridad, tan frecuentes como requiera nuestro uso del computador (obviamente, no es lo mismo alguien que lo utiliza ocasionalmente para escribir cartas y navegar por internet que alguien que lo utiliza profesionalmente, para gestionar datos de clientes, pacientes, ...). Hoy en día es muy sencillo gestionar las copias de seguridad porque casi todos los equipos incluyen una grabadora

de CD's o DVD's que nos permiten almacenar los datos por si nos ocurre una desgracia.

Para terminar, podríamos resumir casi todo lo dicho en las siguientes reglas:

- **Regla 1:** Hasta lo que parece inofensivo, puede ser peligroso.
- **Regla 2:** Cuanto menos automático, mejor.
- **Regla 3:** En caso de duda, preguntar.

Puede parecer un contrasentido que pidamos menos automatismos a una máquina automática, pero lo cierto es que con la simple precaución de obligarle a 'pedir permiso' para llevar a cabo ciertas acciones podemos ahorrarnos muchos dolores de cabeza.

La tercera regla también tiene su explicación: una computadora es una máquina compleja y contiene muchos programas que también tienen un grado de complejidad alto. Es muy difícil y costoso estar al día de todos los problemas que pueden surgir. En cualquier sitio donde haya un número grande de computadoras seguramente habrá personal especializado en administrarlas: es importante pedirles consejo y confiar en su criterio, igual que cuando nos ponemos enfermos consultamos al médico o a otros expertos dependiendo del problema que tengamos que solucionar.

7. Para saber más

Aquí proporcionamos algunos enlaces a sitios que contienen información relevante sobre privacidad y seguridad.

- Sobre privacidad: epic.org, Electronic Privacy Information Center[1].
- Sobre seguridad:
  - Criptonomicón[2], con textos accesibles y variados.
  - Campaña de seguridad de la Asociación de Internautas y Red.es[3],
  - Hispasec[4] contenido variado, en algunas ocasiones bastante técnico. Es interesante su servicio *una al día* que envía por correo electrónico una noticia diaria sobre temas de seguridad, privacidad, sociedad, virus.
  - Alerta-Antivirus[5] que da avisos de seguridad, sobre todo en cuanto a virus y otros programas maliciosos. Además facilitan documentos para usuarios, herramientas, ...

[1] http://www.epic.org/
[2] http://www.iec.csic.es/criptonomicon/
[3] http://www.seguridadenlared.org/
[4] http://www.hispasec.com/
[5] http://alerta-antivirus.red.es/

- Libro: Defiende tu PC, de Sacha Fuentes[6] Es un manual de 119 páginas con bastante información. Se puede comprar o descargarlo directamente de la red.

- Sobre cifrado, confidencialidad:

  - Página con mucha información sobre PGP[7], programa para el uso de cifrado de clave pública.
  - La página de la empresa propietaria de la versión comercial del programa PGP (Pretty Good Privacy)[8].
  - La versión libre (y gratuita) de PGP: The GNU Privacy Guard (GnuPG)

8. Conclusiones

La red es un magnífico medio de comunicación: permite poner en contacto a gente muy diversa y lejana geográficamente. Su diseño fué pensado para la fiabilidad y robustez, no para la seguridad. Se han explicado algunos de los problemas que pueden aparecer, y como convivir con ellos en nuestro uso diario de la red. La idea principal es que debemos ser cuidadosos y prudentes; nuestro comportamiento en la red no debería ser muy diferente al que tenemos en la vida diaria: esto es, no dar más información de la que damos normalmente (incluso menos), ni permitir el acceso a desconocidos en nuestro computador.

La informática nos permite en ocasiones hacer cosas de manera muy sencilla; en algunas ocasiones, esa sencillez tiene un precio: igual que nosotros tenemos que trabajar poco para llevar a cabo determinadas tareas, el atacante también lo tiene todo más fácil.

La seguridad es un proceso, no basta con instalar un antivirus y un cortafuegos: hay que permanecer atento y tratar de estar informado sobre nuevos problemas que van apareciendo.

[6] http://www.defiendetupc.com/
[7] http://www.pgpi.org/
[8] http://www.pgp.com/