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 vaya extendiéndose, es bastante probable que la situación se complique.

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 que pueda acceder a nuestro computador mientras nos conectamos con el modem (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.

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

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 [ESP], 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.

Finalmente, permítasenos citar también un texto extranjero, que se usa como referencia en el mundo anglosajón para asuntos lingüísticos. Del *Oxford English Dictionary*, ([oxf]), 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'.

Para una visión más completa sobre la privacidad, puede utilizarse, por ejemplo, [Gra99], o [Haf]. 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.

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. 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.

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.

  En un campo más profesional; una persona suficientemente hábil llama a una empresa y averigua el nombre de un 'jefe'; con ese nombre, hace una llamada a otra sucursal y averigua la localización de un cierto recurso; con esos dos datos, hace una tercera llamada y consigue que le proporcionen acceso a ese recurso: 'estoy de viaje, y no puedo hacer ...'.

- **Virus, troyanos, programas maliciosos:** Un virus es un programa de ordenador que puede infectar otros programas modificándolos para incluir

una copia de sí mismo según la definición que propuso Fred B. Cohen, quien en 1994 en su tesis doctoral. Habitualmente sólamente son destructivos (borrar ficheros, estropear el sistema), molestos (comportamientos anómalos, ralentización del sistema), ...

Un gusano es un programa que se reproduce, como los virus, pero que no necesita de otros programas para retransmitirse. Un troyano es un programa malicioso que se oculta en el interior de otro 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: 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 dóndepara 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 (aparentemente, esta sería la misión de Mydoom, como ejemplo de plena actualidad). 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 Napster 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.

Entre los peligros podemos destacar la existencia de programas espías ('spyware'). Se trata de programas que van desde la vigilancia de nuestras costumbres de navegación para hacer perfiles de usuario, a programas que pueden enviar nuestras claves, galletas ('cookies') del navegador, y otros datos.

También podemos nombrar a los programas re–marcadores ('dialers') que modifican la configuración de nuestro computador para que haga la conexión a través de números de tarificación especial, suponiendo una estafa y un grave perjuicio para la economía de los afectados.

3.1. El correo no solicitado: spam

Merece una mención especial el correo no solicitado, también conocido como spam. Aunque en la mayoría de los casos podemos considerarlo una siemple molestia (borrar unos cuantos mensajes que no nos interesan), en algunos casos puede suponer un compromiso, cuando menos a nuestra intimidad: puede utilizarse, con mensajes especialmente preparados, para averigura hábitos de lectura de correo, el tipo de conexión que utilizamos y mucha más información.

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.

  Navegador, herramientas, Windows Update (una vez al mes).

- 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 últimamente mediante reenvío automático utilizando la libreta de direcciones). Slammer (enero 2003) había infectado el 90 por ciento de los computadores vulnerables en diez minutos (ni siquiera era necesaria la intervención del usuario); como curiosidad, recordar que había solución para el problema que utilizaba el troyano para propagarse, con meses de antelación; el principal problema fue que las empresas no habían actualizado sus programas para utilizar versiones no vulnerables. Más recientemente, SoBig (agosto 2003) causó pérdidas de millones de dólares en USA. Esta misma semana, aún estamos bajo los efectos de Mydoom. Todavía se están evaluando las pérdidas ocasionadas, aunque aparentemente, las empresas estaban mejor preparadas.

- 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, mensajería instantánea, ...) 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 que sean seguros (.ps, .pdf, imágenes, ...). El .html también puede ser peligroso, teniendo en cuenta lo que puede contener.

- Nadie pide que envíemos nuestra clave por correo; al menos, debería verse como algo muy sospechoso.

- No pinchar en las direcciones que nos envían por correo electrónico (se han dado casos de estafa: el truco consiste en que nosotros vemos una dirección en el mensaje, pero cuando pinchamos vamos a otra diferente). Es mejor copiar y pegar, o ir directamente al sitio de nuestro banco (o cualquier otro servicio) y navegar normalmente allí; en caso de necesidad, copiar y pegar en el navegador, no pinchar).

- Si una dirección comienza con https, eso sólo garantiza que la información viaja por la red codificada, no dice nada acerca de la autenticidad del origen. Para asegurarnos, podemos pinchar en el candado que aparece en la

parte de abajo del navegador (o confirmar que deseamos verlo, si el navegador nos pregunta) para ver que, efectivamente, el certificado correspone al sitio web que nosotros esperamos.

- En caso de duda, utilizar medios tradicionales (visita a la sucursal, teléfono ...): mejor sufrir algunos inconvenientes que vernos implicados en una estafa 'electrónica'.

- Si utilizamos computadores compartidos, o de otras personas temporalmente, es una buena idea borrar el historial de navegación.

- 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, disquetes, cintas, CD-ROM.

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

- Utilizar de vez en cuando detectores de programas espía, como Spybot[1].

- Instalar (si utilizamos el módem para conectarnos) un programa que impida que podamos conectarnos con números de tarificación especial (o contactar con la compañía telefónica para que no podamos usarlos en absluto), como Checkdialer[2]

- Algunos consejos sobre las claves. En muchos sitios (y nuestro computador debería ser el primero de ellos) será necesario el uso de alguna clave para acceder a determinados servicios. A continuanción se exponen algunos consejos sobre como deberían ser.

  - Que contengan mezcladas letras, números y otras cosas
    Z-89ñ.qe2
  - Alrededors de 8 caracteres (o más)
  - No compartirlas.
    - Con los otros, cada uno su usuario y su clave.
    - Para varias cosas, una clave para cada sitio; al menos claves diferentes para recursos especialmente delicados.

[1] http://www.seguridadenlared.org/es/spybot.php
[2] http://www.hispasec.com/software/checkdialer

- Cambiarlas de vez en cuando
- No sirve de nada una clave muy buena, si está escrita en un papel al lado del recurso donde se usa

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, alguien puede 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.

5.1. La red

La red fue diseñada para que fuera robusta y fiable, no segura: los protocolos y mecanismos que se utilizan se preocupan más de ser resistentes a los fallos y problemas que de transmitir la información de forma segura. Ni siquiera tenemos control sobre el camino que seguirá la información. Cada dispositivo conectado a la red tiene una dirección que sirve como forma de referenciarlo y conocerlo por parte de los demás. Además, para que un mismo dispositivo pueda proporcionar varios servicios (web, correo electrónico, IRC, ...), se asignan diferentes

números a estos servicios (podemos hacer una analogía con los pisos, dentro de una casa; o los cajetines de correo, en las oficinas). Estos números se denominan puertos. De esta manera, una conexión habitualmente consiste en una dirección y un puerto, indicando el servicio al que se quiere acceder. Este sistema aporta robustez y flexibilidad, pero aumenta el 'núnero' de puertas que hay que vigilar. Una consecuencia inmediata es que, cuantos menos servicios proporcionemos, más sencillo será protegernos. La otra es que, si no proporcionamos un determinado servicio, el puerto correspondiente debería estar cerrado. La conclusión es clara: cerrar el máximo posible de entradas a nuestro computador y sólo abrir las que sean imprescindibles (que es, justamente, lo contrario de lo que se ha venido haciendo habitualmente hasta ahora, en las instalaciones por defecto de la mayoría de los sistemas).

Para cerrar los puertos, se utilizan los cortafuegos (*firewall*), que son programas capaces de controlar el acceso a los diferentes servicios. Muchos sitios disponen ya de un cortafuegos corporativo, que se interpone entre los puestos de trabajo y el exterior. Conviene recalcar que, además de este tipo de dispositivos, es aconsejable utilizar un cortafuegos personal que proteja cada máquina individualmente. No es infrecuente que, una vez que tenemos el problema dentro (de nada sirve el cortafuegos, si alguien -accidental o intencionadamente- se trae un troyano en un disquete), se contagie al resto de computadores del entorno por carecer de la protección adecuada.

A todo lo que venimos diciendo se añaden algunos problemas, cuando utilizamos redes inalámbricas (WiFi - Wireless Fidelity). Se trata de una tecnología muy exitosa, en la que las conexiones a la red se producen mediante ondas de radio, por lo que la información viaja por el aire. Es muy conveniente y cómoda, al evitarnos la necesidad de utilizar cables. Pero, como casi siempre en informática, su diseño y expansión no ha tenido en cuenta los condicionantes relativos a la seguridad de lo que se transmite. Algunos consejos relativos a la seguridad de estos sistemas serían:

- Tener cuidado con las claves (activarlas y gestionarlas adecuadamente)
- Utilizar control de acceso con autentificación bidireccional
- La configuración de la criptografía de las claves WEP debería ser lo más restrictiva posible (128 bits)
- Cuando sea posible, establecer una política de variación en las claves a lo largo del día
- Si es factible, controlar el radio de transmisión (si necesitamos red a 20 metros del punto de acceso, no ganamos nada -sólo más peligro- si ampliamos el alcance a más distancia).
- Estar atentos ... todo cambia muy rápido todavía, se trata de una tecnología que todavía está experimentando cambios y novedades.

5.2. 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. Esto 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.

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. 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[3].
- Sobre seguridad:
  - Criptonomicón[4], con textos accesibles y variados.
  - Campaña de seguridad de la Asociación de Internautas[5], recientemente asumida también por el Gobierno, con la creación del sitio Seguridad en la red[6]
  - Hispasec[7] 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.
- Sobre cifrado, confidencialidad:
  - Los códigos secretos [Sin]
  - Página con mucha información sobre PGP[8], 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)[9].
  - La versión libre (y gratuita) de PGP: The GNU Privacy Guard (GnuPG)[10]

7. 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.

[3] http://www.epic.org/
[4] http://www.iec.csic.es/criptonomicon/
[5] http://seguridad.internautas.org/
[6] http://www.seguridadenlared.org/
[7] http://www.hispasec.com/
[8] http://www.pgpi.org/
[9] http://www.pgp.com/
[10] http://www.gnupg.org/

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.

Referencias

[ESP] *ESPASA, Diccionario Enciclopédico Abreviado*. ESPASA.

[Gra99] Ian Graham. Putting privacy into context: An overview of the concept of privacy and of current technologies. 1999. http://www.utoronto.ca/ian/privacy/privacy.html.

[Haf] Katie Hafner. Do you know who's watching you? do you care?

[oxf] *Oxford English Dictionary*. Oxford University Press, second edition (electronic database version) edition. http://www.oed.com/.

[Sin] Simon Singh. *Los códigos secretos*. Debate. Pequeña Gran Historia.