

SERVICIOS DE SEGURIDAD.

Para proteger las comunicaciones de los usuarios a través de una red, es necesario dotar a las mismas con una serie de servicios, que se conocen como servicios de seguridad:

Autenticación de la entidad par: Este servicio verifica la fuente de los datos. La autenticación puede ser sólo de la entidad origen, de la entidad destino o de ambas a la vez.

Control de acceso: este servicio verifica que los recursos son utilizados por quien tiene derecho a hacerlo.

Confidencialidad de los datos: este servicio evita que se revelen, deliberada o accidentalmente, los datos de una comunicación.

Integridad de los datos: este servicio verifica que los datos de una comunicación no se alteren, esto es, que los datos recibidos por el receptor coincidan por los enviados por el emisor.

No repudio (irrenunciabilidad): este servicio proporciona la prueba, ante una tercera parte, de que cada una de las entidades han participado, efectivamente, en la comunicación. Puede ser de dos tipos:

Con prueba de origen o emisor: el destinatario tiene garantía de quien es el emisor concreto de los datos.

Con prueba de entrega o receptor: el emisor tiene prueba de que los datos de la comunicación han llegado íntegramente al destinatario correcto en un instante dado.

Mecanismos de seguridad

Para proporcionar los servicios de seguridad citados, es necesario incorporar en los niveles adecuados del modelo de referencia OSI los siguientes mecanismos de seguridad:

Cifrado: el cifrado puede hacerse mediante el uso de criptosistemas simétricos o asimétricos y puede aplicarse extremo a extremo o a cada enlace del sistema de comunicaciones.

El mecanismo de cifrado soporta el servicio de confidencialidad de los datos y puede complementar a otros mecanismos para conseguir diversos servicios de seguridad.

Firmado digital: la firma digital se puede definir como un conjunto de datos que se añaden a una unidad de datos de modo que protejan a ésta contra cualquier falsificación, permitiendo al receptor comprobar el origen y la integridad de los datos. Para ello, se cifra la unidad de datos junto con alguna componente secreta del firmante, y se obtiene un valor de control ligado al resultado cifrado.

El mecanismo de cifrado digital soporta los servicios de integridad de los datos, autenticación del emisor y no repudio con prueba de origen. Para que se pueda proporcionar el servicio de no repudio con prueba de entrega, hay que forzar al receptor para que envíe un acuse de recibo firmado digitalmente.

Control de acceso: se usa para autenticar las capacidades de una entidad para acceder a un recurso dado. El control de acceso se puede llevar a cabo en el origen o en un punto intermedio, y se encarga de asegurar que el emisor está autorizado a comunicarse con el receptor o a usar los recursos de comunicación.

El mecanismo de control de acceso soporta el servicio de control de acceso.

Integridad de datos: hay que distinguir entre la integridad de una unidad de datos individual y la integridad de una secuencia de unidades de datos. Para lograr integridad de una unidad de datos, el emisor añade datos suplementarios a la unidad de datos. Estos datos suplementarios se obtienen en función de la unidad de datos y, generalmente, se cifran. El receptor genera los mismos datos suplementarios a partir de la unidad original y los compara con los recibidos. Para proporcionar integridad a una secuencia de unidades de datos se requiere, adicionalmente, algún mecanismo de ordenación, tal como el uso de números de secuencia, un sello temporal o un encadenamiento criptográfico entre las unidades. El mecanismo de integridad de datos soporta el servicio de integridad de datos. intercambio de autenticación, que tiene dos grados:

Autenticación simple: el emisor envía su identificador y una contraseña al receptor, el cual los comprueba.

Autenticación fuerte: utiliza propiedades de los criptosistemas de clave pública. Un usuario se autentifica mediante su identificador y su clave privada. Su interlocutor debe verificar que aquel, efectivamente, posee la clave privada, para lo cual debe obtener, de algún modo, la clave pública del primero. Para ello deberá obtener su certificado. Un certificado es un documento firmado por una Autoridad de Certificación (una tercera parte de confianza) y válido durante el periodo de tiempo determinado, que asocia una clave pública a un usuario. El mecanismo de intercambio de autenticación soporta el servicio de autenticación de entidad par.

COMUNICACIONES SEGURAS SOBRE REDES INSEGURAS

Introducción

El crecimiento exponencial de los usuarios y organizaciones conectadas a Internet ha originado el tránsito a través de ella de informaciones de todo tipo, hasta complejas transacciones que requieren medidas específicas de seguridad que garanticen la confidencialidad, la integridad y la constatación del origen de los datos.

Terminología

Se supone la existencia de un emisor y un receptor, los cuales quieren intercambiar mensajes. El posible enemigo que quiere interferir de algún modo en la comunicación se denomina intruso. Este intruso puede ser pasivo, si sólo escucha la comunicación, o activo si trata de alterar los mensajes.

Es aquí donde aparece la criptografía con objeto de proporcionar comunicaciones seguras sobre canales inseguros. Los mensajes sin transformar de ninguna manera se denominan texto en claro (también llamado, según una no muy adecuada traducción, texto plano).

El proceso mediante el cual la información contenida en el mensaje es ocultada se denomina cifrado. Un mensaje cifrado se denomina, obviamente, texto cifrado. El proceso mediante el que se revierte el proceso de ocultación, obteniendo el texto en claro a partir del texto cifrado se denomina descifrado.

La criptografía (que, etimológicamente, procede de la raíz griega *kruptoj*, *kriptós*, "oculto", y de *grafia*, y significa "escritura oculta") se puede definir como la disciplina que estudia los principios, métodos y medios de ocultar la información contenida en un mensaje. Es practicada por los criptógrafos.

Es decir, se trata de permitir que dos entidades, ya sean usuarios o aplicaciones, puedan enviarse mensajes por un canal que puede ser intervenido por una tercera entidad, de modo que sólo los destinatarios autorizados puedan leer los mensajes. Como paradigma de red insegura consideraremos Internet, que es, previsiblemente, la red de redes sobre la que se llevarán a cabo las transacciones comerciales del futuro.

Pero la criptografía no es en sí seguridad; simplemente es la herramienta utilizada por mecanismos más complejos para proporcionar no sólo confidencialidad, sino también otros servicios de seguridad, ya que, en el contexto de Internet, la confidencialidad es, a menudo, un factor secundario. Generalmente estaremos más interesados en el mantenimiento de la integridad de los mensajes y en los mecanismos de autenticación que, implícitamente, proporciona la criptografía. En efecto, un mensaje cifrado sólo puede ser descifrado si la clave que vamos a utilizar para ello pertenece a quien ha cifrado previamente el mensaje.

La criptografía no es una panacea, solo un instrumento. De hecho, no más del 15% de los "advisories" de los diferentes CERTs durante los últimos diez años describen vulnerabilidades que podrían haber sido evitadas si el uso de la criptografía hubiese sido generalizado.

La ciencia o arte que se ocupa del estudio sistemático de los métodos de descifrar informaciones cifradas se le denomina criptoanálisis, y es practicada por los criptoanalistas (ambas disciplinas, el criptoanálisis y la criptografía se engloban en una rama de las matemáticas conocida como criptología).

El texto en claro se representa como M (por message) o también por P (de plain text). M es simplemente un dato binario. El texto cifrado se designa por C (de ciphertext). No existe relación directa entre los tamaños de ambos mensajes. Unas veces su tamaño coincide. Otras, el del texto cifrado es mayor que el del texto en claro. Puede ocurrir, incluso, que texto cifrado sea de menor tamaño. Esto sucede cuando, además de las técnicas de cifrado, se emplean técnicas de compresión.

La función de cifrado, E, opera sobre M para producir C. En notación matemática:

$$E(M) = C$$

Inversamente, la función de descifrado, D, se aplica a C para producir M:

$$D(C) = M$$

En todo caso, debe cumplirse la siguiente igualdad:

$$D(E(M)) = M$$

Un algoritmo criptográfico es una función matemática utilizada para el cifrado y descifrado de mensajes. Generalmente, hay dos funciones relacionadas: una para el cifrado y otra para el descifrado

Tipos de ataques

Una comunicación, protegida o no mediante sistemas criptográficos, está sujeta a una gran variedad de ataques de los cuales es imposible dar una taxonomía completa. Los citados habitualmente son los siguientes:

Ataque sólo al criptograma: es el más desfavorable para el intruso o criptoanalista. En este caso, sólo tiene acceso al texto cifrado. El trabajo del intruso consiste en recuperar el texto en claro de tantos mensajes como sea posible. En tales condiciones, y aunque conociera el algo-

ritmo de cifrado, sólo puede intentar vulnerar dicho algoritmo, realizar un análisis estadístico de los criptogramas o probar todas las claves posibles del algoritmo. Este último caso, por motivos obvios se conoce como búsqueda exhaustiva o también como ataque basado en fuerza bruta.

Ataque mediante texto en claro conocido: en este ataque, más ventajoso para el atacante, éste se ha hecho con pares de texto en claro y su equivalente cifrado o ha adivinado, de algún modo, el contenido del mensaje (muchos mensajes cifrados, correspondientes a protocolos normalizados, reproducen la misma estructura o poseen las mismas palabras en los mismos sitios del mensaje). Estas parejas pueden ser usadas para llevar a cabo el criptoanálisis y averiguar la clave, lo cual será útil si se usa la misma clave para posteriores comunicaciones.

Ataque mediante texto en claro escogido: ataque mucho más eficaz que el anterior en el que el intruso es capaz, de algún modo, de conseguir que un texto elegido por él sea cifrado con la clave desconocida. Por tanto hay que diseñar el sistema criptográfico de modo que nunca un intruso pueda introducir mensajes propios.

Ataque adaptable mediante texto en claro escogido: caso especial del anterior en el que el intruso no sólo puede elegir el texto que quiere cifrar, sino que puede tomar decisiones sobre el texto que se cifra basadas en resultados anteriores.

Ataque mediante criptogramas escogidos: el atacante puede obtener el descifrado de diversos mensajes cifrados escogidos por él.

Aunque se pueden diseñar otros ataques criptoanalíticos, los citados son los más frecuentes. En el marco de una comunicación entre dos entidades, se puede hablar de los siguientes ataques, que pueden servir para implementar alguno de los anteriores:

Escucha pasiva (passive eavesdropping): el intruso simplemente escucha el tráfico que circula por el canal.

Tercero interpuesto (man-in-the-middle): el intruso, de alguna forma, se coloca entre los dos interlocutores y hace creer a cada uno de ellos que es su interlocutor.

Retransmisión ciega (replay): el intruso intercepta un mensaje legítimo, lo almacena (sin eliminarlo) y lo reenvía un tiempo después.

Cortado-y-pegado (cut-and-paste): dados dos mensajes cifrados con la misma clave, a veces es posible combinar partes de los dos para producir uno nuevo. El intruso no sabe lo que dice este nuevo mensaje, pero puede utilizarlo para confundir a los interlocutores legítimos e inducir a alguno de ellos a hacer algo beneficioso para el intruso.

Puesta a cero del reloj (time-resetting): en protocolos que utilizan de alguna forma la hora actual, el intruso puede tratar de confundirnos acerca de cuál es la verdadera hora.

Un poco de historia

Los usos más primitivos de la criptografía se encuentran documentados desde la época de Julio César (nos referimos al cifrado de César, aunque hay constancia también de su uso por persas y espartanos). Estos mecanismos de cifrado se basaban en técnicas de transposición de caracteres y fundamentan su eficacia en el secreto del algoritmo empleado para el cifrado. Algoritmos de este tipo son sólo de interés histórico.

Los algoritmos modernos usan una clave para controlar el cifrado y descifrado de los mensajes. Generalmente, el algoritmo de cifrado es públicamente conocido y sometido a escrutinio por parte de expertos y usuarios. Se acepta, por tanto, la denominada hipótesis de Kerckhoffs, que establece que la seguridad del cifrado debe residir, exclusivamente, en el secreto de la clave y no en el del mecanismo de cifrado.

Criptografía de clave simétrica

Las técnicas de clave única, secreta o simétrica tienen fundamentos de complejidad diversa, pero todas usan una misma clave k que es conocida por el remitente de los mensajes y por el receptor, y mediante la cual se cifra y descifra el mensaje que se quiere proteger (existe una variante según la cual la clave de descifrado puede obtenerse de la de cifrado utilizando unos recursos y en un tiempo razonables).

Los cifradores simétricos pueden dividirse en dos grupos:

Cifradores de flujo, los cuales cifran un único bit del texto en claro cada vez.

Cifradores de bloque, que toman un grupo de bits (un valor típico es 64 bits) y lo cifran como si se tratase de una unidad.

Las ventajas de la utilización criptografía de clave simétrica es la existencia de algoritmos muy rápidos y eficientes, especialmente si se implementan en hardware. Si k es lo bastante larga (típicamente se usan valores de 56 a 128 bits), es imposible reventarlas usando la fuerza bruta.

Criptografía de clave asimétrica

El principal inconveniente estriba en la necesidad de que todas las partes conozcan k . Esta clave es distribuida mediante una transacción separada y diferente a la transmisión del mensaje cifrado. Es aquí, precisamente, donde se halla el punto vulnerable del mecanismo: la distribución de la clave. Si la clave es interceptada se pone en peligro todo el mecanismo. La clave debe ser transmitida por un canal seguro para poder asegurar la eficacia del sistema criptográfico. Este canal es generalmente externo a Internet, ya que, en caso contrario, surgiría la pregunta "Si tenemos un canal seguro, ¿para qué necesitamos criptografía?".

La solución a este problema apareció en 1976. En ese año, Whitfield Diffie y Martin Hellman demostraron la posibilidad de construir sistemas criptográficos que no precisaban la transferencia de una clave secreta entre emisor y receptor, evitando así los problemas derivados de la búsqueda de canales seguros para tal transferencia. Se trataba de la "criptografía de clave asimétrica o pública".

PGP Pretty Good Privacy

PGP está basado en una tecnología de cifrado ampliamente aceptada conocida como criptografía de clave pública, en la cual dos claves complementarias llamadas par de claves, son usadas para mantener comunicaciones seguras. De ellas, una es una clave privada a la cual solamente usted tiene acceso, y la otra es una clave pública que se intercambia libremente con otros usuarios PGP. Ambas claves, privada y pública, son guardadas en archivos de claves, siendo accesibles desde la ventana PGPkeys. Es desde esta ventana que se realizan todas las funciones de administración de claves.

Para enviar a alguien un mensaje de correo electrónico privado, se usa una copia de la clave pública del destinatario para cifrar la información, de manera que el mensaje solamente podrá

ser descifrada usando la clave privada del destinatario. Al contrario, cuando alguien desea enviarnos correo cifrado usa una copia de nuestra clave pública para cifrar los datos, los cuales solamente será posible descifrar usando nuestra clave privada. También se puede usar PGP para cifrar o firmar archivos que son guardados en el equipo, para autenticar que no han sido alterados

También puede usarse la clave privada para firmar el correo electrónico dirigido a otros o para firmar archivos para autenticarlos. Los destinatarios pueden entonces usar una copia de su clave pública para asegurarse que fue realmente usted quien envió el mensaje de correo electrónico, y que no fue alterado mientras estaba en tránsito.

Cuando alguien nos envía un mensaje de correo electrónico con una firma digital, usamos una copia de la clave pública de esa persona para comprobar la firma digital y asegurarnos que nadie haya adulterado el contenido del mensaje.

Con el programa PGP se pueden crear y administrar fácilmente las claves y acceder a todas las funciones para cifrar y firmar, así como descifrar y verificar los mensajes de correo electrónico, archivos, y archivos adjuntos.

Creación de un par de claves

Antes de empezar a usar PGP, se necesita generar un par de claves. Un par de claves PGP está compuesto de una clave privada a la cual solamente usted tiene acceso, y una clave pública que se puede copiar y hacer disponible libremente a cualquiera con quien intercambie información.

Se crea un nuevo par de claves inmediatamente después de haber finalizado el procedimiento de instalación de PGP, o puede hacerse en cualquier momento abriendo la aplicación PGPkeys.

Intercambio de claves públicas con otros usuarios

Después de haber creado un par de claves, se puede empezar a intercambiar correspondencia con otros usuarios de PGP.

Será necesario contar con una copia de la clave pública de los otros usuarios, y ellos necesitarán una copia de la nuestra. Su clave pública es un simple bloque de texto, de modo que es fácil intercambiar claves con cualquiera.

Puede incluir su clave pública en un mensaje de correo electrónico, copiarla a un archivo, o publicarla en un servidor de claves público o corporativo donde cualquiera pueda obtener una copia cuando la necesite.

Validación de claves

Una vez obtenida una copia de la clave pública de alguien, puede agregarla a su archivo de claves públicas.

Deberíamos asegurarnos que la clave no ha sido alterada, y que realmente pertenece al usuario correcto. Para ello debe compararse la huella única (fingerprint) de la copia de la clave pública de esa persona, con la huella de la clave original de esa persona.

Cuando se esté seguro de tener una clave pública válida, se firma para indicar que su uso es seguro. Además, puede concederse al usuario de la clave un nivel de confianza que indica

cuánta confianza se tiene en esa persona para garantizar la autenticidad de la clave pública de otra persona.

Cifrado y firma de sus mensajes de correo electrónico y archivos

Después de haber generado el par de claves propio y haber intercambiado claves públicas, se puede empezar a cifrar y firmar mensajes de correo electrónico y archivos.

- * Si se usa una aplicación de correo electrónico soportada por los complementos (plug-in) PGP, se pueden cifrar y firmar los mensajes seleccionando las opciones apropiadas desde la barra de herramientas de la aplicación.
- * Si la aplicación de correo electrónico no está soportada por los plug-ins PGP, se puede copiar el mensaje al portapapeles y realizar desde allí las funciones apropiadas. También pueden cifrar y firmar archivos desde el Explorador de Windows antes de adjuntarlos al correo electrónico. El cifrado asegura que solamente usted y los destinatarios pueden descifrar el contenido de los archivos; la firma asegura que cualquier alteración será rápidamente advertida.

Descifrado y verificación de los mensajes de correo electrónico y archivos

Cuando nos envían correo electrónico cifrado, se descifra el contenido y se verifica cualquier firma agregada para asegurarse que los datos fueron originados por el presunto remitente y que no fueron alterados.

- * Si se usa una aplicación de correo electrónico soportada por los plug-in PGP, se descifran y verifican los mensajes seleccionando las opciones apropiadas.
- * Si no está soportada, se copia al portapapeles y se realizan las funciones apropiadas desde allí. Los archivos adjuntos, se descifran desde el Explorador de Windows. También pueden descifrarse archivos cifrados guardados en su equipo, y verificar archivos firmados para asegurarse que no han sido modificados.

Borrado irreversible de archivos

Cuando sea necesario borrar permanentemente un archivo, puede usarse la opción Tachar [Wipe] para asegurarse que el archivo sea irrecuperable. El archivo es entonces inmediatamente sobrescrito de modo que no pueda ser recuperado usando herramientas de recuperación de datos.

PGP for Personal Privacy

PGP soporta el uso de un tipo de clave: Diffie-Hellman/DSS.

La versión PGP Internacional tiene la opción de generar, usar y administrar claves tipo RSA compatible con versiones anteriores.

PGP funciona sobre los datos generados por otras aplicaciones. Por lo tanto, las funciones PGP apropiadas están diseñadas para estar inmediatamente disponibles para su uso según la tarea que usted esté realizando en un momento dado. Hay tres modos primarios de usar PGP:

- * Desde la barra de tareas del sistema.
- * Desde aplicaciones de correo electrónico soportadas.
- * Desde el menú del Explorador de archivos de Windows.

Uso de PGP/MIME

PGP/MIME es una norma para algunos de los complementos PGP que integran las funciones PGP directamente a las aplicaciones de correo electrónico populares. Si está usando una aplicación de correo electrónico que es soportada por uno de los complementos que ofrecen PGP/MIME, será capaz de cifrar y firmar, así como descifrar y autenticar automáticamente sus mensajes de correo electrónico y archivos adjuntos cuando se envía o recibe correo electrónico.

Sin embargo, antes de enviar correo electrónico PGP/MIME se debe verificar que los destinatarios estén usando una aplicación de correo electrónico que soporte esta norma, porque si no es así podrían tener dificultades para descifrar y autenticar sus mensajes.

Iconos de PGPkeys, definiciones

La siguiente tabla muestra todos los mini-iconos usados en la ventana PGPkeys, junto a una descripción de lo que representan.

ICONO	QUE REPRESENTA
	Un par de llaves amarillas representa su par de claves Diffie-Hellman/DSS, que consta de su clave privada y su clave pública.
	Una sola llave amarilla representa una clave pública Diffie-Hellman/DSS.
	Un par de llaves azules representa su par de claves RSA, que consta de su clave privada y su clave pública.
	Una sola llave azul representa una clave pública RSA.
	Cuando un par de llaves está atenuado, temporalmente no está disponible para cifrar y firmar. Usted puede inhabilitar una clave desde la ventana PGPkeys, para evitar confusiones con las claves que usa siempre en el cuadro de diálogo Selección de Claves.
	Una llave atravesada por una línea roja indica que la clave ha sido revocada. Los usuarios revocan sus claves cuando no son más válidas o han sido comprometidas de algún modo. Una llave atravesada por una X roja indica que la clave es inválida.

ICONO	QUE REPRESENTA
	Una llave con un reloj indica que la clave ha caducado. La fecha de caducidad de la clave es establecida cuando es creada la clave.
	Un diamante representa al dueño de la clave y lista los nombres de usuario y direcciones de correo electrónicos asociados con la clave.
	Una llave con un reloj indica que la clave ha caducado. La fecha de caducidad de la clave es establecida cuando es creada la clave.
	Un sobre representa al dueño de la clave y lista los nombres de usuario y direcciones de correo electrónico asociados con la clave.
	Un círculo vacío indica que la clave es inválida.
	Un círculo verde indica que la clave es válida. Un círculo rojo indica que la clave tiene asociada una Clave de Descifrado Adicional.
	Un diamante verde indica que usted posee la clave, y que tiene confianza implícita.
	Un lápiz o una estilográfica indica las firmas de los usuarios PGP que responden por la autenticidad de la clave. Una firma atravesada por una línea roja indica una firma revocada. Una firma atravesada por una X roja indica una firma mala o inválida. Una firma con una flecha azul próxima a ella indica que es exportable.
	Una pluma de ave indica la firma de los usuarios PGP que han garantizado la autenticidad de la clave. Una firma atravesada por una línea roja indica una firma revocada. Una firma atravesada por una X roja indica una firma mala o inválida.
	Una barra vacía indica una clave inválida, o desconfianza en el usuario.
	Una barra llena por la mitad indica una clave con validez marginal, o confianza marginal en el usuario.
	Una barra llena indica una clave con validez completa, o confianza completa en el usuario.
	Una barra con franjas indica una clave con validez implícita y confianza implícita en el usuario. Esta configuración está disponible solamente para los pares de claves creados por vd

Conceptos básicos acerca del sistema de claves publica y privada.

CLAVES

Sin entrar en demasiados detalles, puede decirse que no es realmente el contenido del mensaje de correo electrónico el que es cifrado usando el esquema de cifrado de clave pública. En vez

de eso, los datos son cifrados usando un algoritmo de clave única mucho más rápido, y realmente es esta clave única la que está cifrada usando la clave pública del destinatario. El destinatario entonces usa su clave privada para descifrar esta clave, la cual le permite descifrar los datos.

El tamaño de la clave corresponde al número de bits usado para construir la clave digital. Cuanto más grande es este número, menor es la posibilidad que alguien pueda descubrirla, pero mayor el tiempo que tomará realizar los procesos de cifrado y descifrado.

Es necesario buscar un balance entre la conveniencia de realizar las funciones PGP en forma rápida con una clave más pequeña, y el mayor nivel de seguridad provisto por una clave más grande.

Una clave de 1024 bits es segura, a menos que intercambie información extremadamente sensible que interese lo suficiente como para que alguien esté dispuesto a montar un ataque criptográfico caro y lento.

Una vez creado el par de claves y después de haber distribuido la clave pública, probablemente se continuarán usando las mismas claves a partir de entonces.

Sin embargo, pueden crearse un par de claves especiales con el propósito de usarlas solamente por un tiempo limitado. En este caso, cuando la clave pública caduca no puede usarse más para cifrar correo, pero todavía puede ser usada por otros para verificar su firma digital.

Similarmente, cuando el par de claves caduca, todavía puede ser usado por usted para descifrar correo que le fue enviado antes que caducara su clave pública, pero no puede ser usado más para firmar correo a dirigido otros.

CONTRASEÑAS

Se debe elegir alguna contraseña que pueda recordarse con facilidad, pero que otros no puedan adivinar.

La frase de contraseña distingue entre letras mayúsculas y minúsculas.

Cuanto más larga la frase de contraseña y mayor la variedad de caracteres que contiene, más segura es. Las frases de contraseñas seguras incluyen letras mayúsculas y minúsculas, números, signos de puntuación y espacios pero son olvidadas más fácilmente.

Cifrar un archivo y luego encontrarse imposibilitado de descifrarlo es una lección dolorosa, que conduce a aprender cómo elegir una frase contraseña que pueda recordarse.

Una palabra de contraseña aislada es vulnerable a un "ataque de diccionario" que consiste en hacer que una PC pruebe todas las palabras del diccionario hasta encontrarla.

Para protegerse de este tipo de ataques, es ampliamente recomendada la creación de una palabra que incluya una combinación de letras mayúsculas y minúsculas, números, signos de puntuación y espacios. Esto resulta en una contraseña de una palabra más segura pero oscura, que no se recuerda fácilmente. No es recomendable usar una contraseña de una sola palabra.

Una frase de contraseña es menos vulnerable al ataque del diccionario.

Se efectúa fácilmente usando múltiples palabras en su contraseña, en vez de intentar impedir un ataque de diccionario insertando arbitrariamente en la palabra de contraseña caracteres raros, no alfabéticos, con el propósito de enmascararla, lo que puede hacerla demasiado fácil de olvidar, y llevar a una pérdida desastrosa de información cuando no pueden descifrarse los propios archivos.

Sin embargo, a menos que la frase de contraseña elegida se pueda memorizar fácilmente por mucho tiempo, es muy probable que no se recuerde totalmente.

Se debe elegir algo que ya se encuentre en la memoria.

No debe ser algo que usted haya repetido a otros recientemente, ni una frase famosa, porque lo que usted desea es que sea difícil atacarla o adivinarla con equipos sofisticados. Si ya está profundamente en su memoria, probablemente no la olvidará.

Por supuesto, si es lo suficientemente imprudente como para escribir la contraseña en un papel pegado al monitor o dentro del escritorio, no importa lo que elija.

PROTECCION DE LAS CLAVES

Una vez que haya generado un par de claves, es conveniente hacer una copia y ponerla en un lugar seguro para el caso que algo le suceda al original.

Las claves privadas y públicas son guardadas en archivos de claves separados, que se pueden copiar como cualquier archivo.

En forma predeterminada, el archivo de claves privadas (`secreting.skr`) y el archivo de claves públicas (`pubring.pkr`), son guardados junto a los demás archivos de PGP en el directorio que los contiene, pero pueden guardarse las copias de seguridad en otra ubicación.

PGP crea copias de seguridad de las claves públicas y privadas cuando las genera estas claves. Estas copias son llamadas `pubring.pkr.bak` y `secreting.skr.bak`.

Además de hacer copias de seguridad, se debe ser especialmente cuidadoso acerca de dónde guardan.

Aún cuando la clave privada está protegida por una contraseña que solamente usted debería conocer, es posible que alguien pudiera descubrir la contraseña y usar su clave privada para descifrar sus mensajes de correo electrónico o firmar con su firma digital.

Por ejemplo, alguien podría interceptar la contraseña desde otro equipo conectado en red, o capturarla de las emisiones de radiofrecuencia que emite el equipo.

Para prevenir que alguien que pudiera haber obtenido su contraseña use su clave privada, debería guardarla en un disquete, o solamente en el propio equipo.

DISTRIBUCION DE LA CLAVE PUBLICA

Después de crear las claves, es necesario hacerlas disponibles a otros para que puedan enviarnos correo electrónico cifrado y verifiquen nuestra firma digital. Existen tres opciones para distribuir la clave pública:

- * Colocarla en un servidor de claves públicas. El mejor método para hacer disponible su clave pública es ubicarla en un servidor de claves públicas donde cualquiera pueda accederla. De este modo, la gente puede enviarle mensajes de correo electrónico cifrado sin tener que pedirle explícitamente una copia de su clave. También le libera a usted y otros de tener que mantener un gran número de claves públicas que usted raramente usa. Hay un número de servidores de claves públicas en todo el mundo, incluyendo aquellos ofrecidos por Network Associates, Inc., en los que usted puede hacer disponible su clave para que cualquiera acceda a ella

* Incluirlo en un mensaje de correo electrónico.

Cuando envía a alguien su clave pública, asegúrese de firmar el mensaje de correo electrónico. De ese modo el destinatario puede verificar su firma y asegurarse que nadie haya modificado la información a lo largo del recorrido. La clave pública se compone básicamente de un bloque de texto, así que resulta bastante fácil hacerla disponible a través de un servidor de claves público, incluirla en un mensaje de correo electrónico o exportarla/copiarla a un archivo. El destinatario puede entonces usar el método más conveniente para añadir su clave pública, a su propio archivo de claves públicas.

```
mQENAjMCpkOAAAEIALQiOUPrbStLJY-
fU7GGOX1QwrEkunvibLB8csCdfen9qPzKgUZolEg-
BTE6RstgNyYEPQjMXmIYOzUBvRuag6WJdIJPJ8/AFWVOUACYUbxq8Vro4b4RnMD
7bjvy68MalGVV07vC2+jx0yx9FeOx1M4BUrYvxfzLt9B8eP85CEjfcYAgCOCC/6CW8iZ
WUlvwwpNtVuirDjdF6TCKmQ/K3gdbmU-
wHByxSo2PlnG9jva+4vhUOKk71wQx4k/1Tv68hKlqieGqnLonNWvQrPK2yv2BOKQ4W
aF2xx25b5CeI7uNJDIEhp996nf2jnzG7xkhdv3amXNODO2Gs4m3gTXWWEABRG0Ik1
pY2hhZUugSi4gSWFubmFtaWNvIDxtama!cGdwLmNvbT6JARUDBRAzX1b1Gs4m3gT
XWWE-
BASP1B/4xAf+8HfUSRbq6XMxMvMVYNdVHgW+2bW9AG4JKwM/T8hmSq+Lj8VMpO
MN1XzmXVjxQ5Ln2HSgNACXtsA+sqCVd7xsXjJIG72i+bioOjtS4xQJHVsQ+mOmBY
Hlc67gobUSGO3iuqjDrJrB3P1+4CwtFPTcE6mkfIYoKor20GAppJVbrpEAm3Fjs20+gD
UC9NvogKzvOE1XOCO6RQmZM7BMT3kdZe44UOp/JsxTBExzpARxBCgKVXcQ08VX
FlbA/+oDdJ8EqLd/OckGunw312Nfd+fvGv5MKdva+JdsJzOK75xH3YHmQrpB/QUP8g
MB/nnnhcLP2x1JbW/NcxXV0V9riQEVawUQMwQn4TP6oFK2L9UbAQEK7gf+IKstvUha
BL9BRbF9RbMje9bdiHCeT8KRx0A912/+IZG2ckY2rypBP7A3mPOTfs6MQWD9/A4fb5l
ocld833GiOljEvv/Uu2VBCZbZTR74PwuHjc6n2dsMvq01T6rqL4SidCxwskaAvEaf9qKK
GbWapJF1G3gzl2dgsVKh26pAohD9NTvo13xj4aEL2xATvcbjglhxqw4Yk0YjHDci3Tyel
Ep-
keJ5qjwEMX8HTnJRsvjX1pMI/IOEaZmrODk4AFbstRHwH2PbhRRkJtZg8CZn3F5Wxz
kWaFjwM3aeTLt+Y2qtEwjnErct6OIZA8Je/IDoktv19XoOn20EWxjiOw+HlKA1QMFEDM
OF4dleYS4x61m3QEBEjOD/lbJLL3Kuek9rOK/fwUdIRx/TZyVBUo3JCpiOEZVF7VhZo3
GOW-
MuNYNSwmSoMMGs+gyB8qOWsPlidnugL4XpGlicvNLBP7Fbuw4iUN8coxXFOQP16R
Q60SUuf9r/SX3Qdcu39HhlzzzZVLYks+6AvxtdMOuOttzqpcgAd+3R9mWWm
=pz/6
-----END PGP PUBLIC KEY BLOCK-----
```

*Exportarla o copiarla a un archivo de texto.

Cuando se intercambian claves públicas, algunas veces es difícil de saber si la clave realmente pertenece a esa persona. PGP proporciona un conjunto de salvaguardas que permiten verificar la autenticidad de una clave y certificar que la clave pertenece a un usuario en particular. El programa PGP alerta si se intenta usar una clave que no es válida, y también en forma predefinida alerta cuando se está por usar una clave de validez marginal.

Una de las mayores vulnerabilidades del sistema de cifrado por clave pública, es la habilidad de algunos fisgones para montar un ataque "hombre del medio" [man-in-the-middle], reemplazando la clave pública de una persona por una que les pertenezca. De ese modo pueden interceptar cualquier mensaje de correo electrónico cifrado dirigido a esa persona, descifrarlo usando su propia clave, cifrarlo de nuevo con la clave real de esa persona, y luego enviarlo como si nada hubiera sucedido. En realidad, esto podría hacerse automáticamente a través de un sofisticado programa de computadora que se ubica en el medio y descifra toda la correspondencia dirigida a usted.

Basado en este escenario, quienes intercambian mensajes de correo electrónico necesitan una manera para determinar si realmente tienen copias legítimas de las claves de los demás.

La mejor manera de estar completamente seguro que una clave pública realmente pertenece a una persona en particular es que la copie en un disquete y la entregue en mano.

Sin embargo, raramente se estará lo suficientemente cerca de alguien como para entregarle un disquete en mano, y generalmente se intercambiarán claves públicas a través de mensajes de correo electrónico o se obtendrán de un servidor de claves público.

Aún cuando estos métodos de intercambiar claves a prueba de modificaciones son algo menos seguros, todavía se puede determinar si una clave realmente pertenece a una persona en particular verificando su huella, una serie única de números generados cuando la clave es creada.

Se puede estar absolutamente seguro de tener una copia válida de la clave pública de una persona comparando la huella de su copia de la clave con la huella de la clave original. Para encontrar la huella de una clave, se selecciona la clave en la ventana PGPkeys, y luego desde el menú Claves se elige Propiedades de la Clave.

El modo más eficaz de verificar la huella de la clave de una persona es llamarla por teléfono y pedirle que lea la huella. El segundo mejor modo es el impreso. Muchas personas han impreso la huella de su clave en sus tarjetas personales y de negocios, pero el único modo de asegurar que la tarjeta es legítima es que le haya sido entregada por su titular.

Una vez que se está absolutamente convencido de tener una copia legítima de la clave pública de una persona, se firma.

Al firmarla con su clave privada, usted certifica que está seguro que la clave pertenece al pretendido usuario.

En forma predeterminada, las firmas que se realizan sobre otras claves no serán exportadas, lo cual significa que solamente se aplican a la clave cuando están en el archivo de claves propio.

Los usuarios de PGP a menudo hacen firmar sus claves públicas por otros usuarios de confianza para que atestigüen su autenticidad. Por ejemplo, usted podría enviar a un colega de confianza una copia de su clave pública con una petición de que la certifique y la devuelva, de modo que se pueda incluir esa firma cuando publique su clave en un servidor de claves público.

Usando PGP, cuando una persona obtiene una copia de una clave pública, no tiene que verificar la autenticidad de la clave por sí misma, sino basarse en lo mucho que confía en las personas que firmaron dicha clave. PGP proporciona las maneras para establecer este nivel de validez para cada una de las claves públicas que se agreguen a su archivo de claves públicas y muestra el nivel de confianza en la validez asociada con cada clave en la ventana PGPkeys.

Esto significa que cuando se obtiene una clave firmada por un presentador de confianza, puede estar medianamente seguro de que la clave pertenece al pretendido usuario.